

On the Hardness of 4-to-1 Games with Perfect Completeness

Yumou Fei*

Dor Minzer[†]Shuo Wang[‡]

Abstract

We prove that for all $\varepsilon > 0$, there exists a positive integer k such that given a 4-to-1 game Ψ with alphabet size at most k , it is **NP**-hard to distinguish between the case that $\text{val}(\Psi) = 1$ and the case that $\text{val}(\Psi) \leq \varepsilon$. This confirms the 4-to-1 Games Conjecture from [Khot, *CCC 2002*]. Previously, the best known result, due to [Dinur, Khot, Kindler, Minzer, Safra], established the almost-perfect completeness version (but applied to the stricter problem of 2-to-1 games). Using results from the literature, we get the following implications:

- (1) For all $k \in \mathbb{N}$, given a 3-colorable graph G , it is **NP**-hard to find a proper k -coloring.
- (2) For all $\delta > 0$, given a 2-colorable 3-uniform hypergraph G , it is **NP**-hard to find in it an independent set containing at least δ fraction of the vertices.

Our proof is a three-step construction that builds on the two-step framework of [Dinur, Khot, Kindler, Minzer, Safra]. In the outer-PCP step, we use quadratic equations to gain perfect completeness. We then construct a new middle PCP that performs low-rank tests while preserving a key covering property. Finally, we construct a new inner PCP based on a tensor product of the standard Grassmann encoding with its low-rank variant due to [Golowich, FOCS 2023].

*Department of EECS, Massachusetts Institute of Technology. Supported by NSF CCF award 2310818 and NSF DMS award 2022448.

[†]Department of Mathematics, Massachusetts Institute of Technology. Supported by NSF CCF award 2227876 and NSF CAREER award 2239160.

[‡]Department of Mathematics, Massachusetts Institute of Technology. Supported by NSF award 2239160.

Contents

1	Introduction	4
1.1	Label-Cover, Unique Games and d -to-1 Games	4
1.2	Main Result	5
1.2.1	Implications	6
1.3	Our Techniques	7
2	Proof Overview	8
2.1	The Imperfect Completeness Construction	8
2.1.1	The Outer PCP	8
2.1.2	The Inner PCP	9
2.1.3	On the Non-Standard Notion of Soundness	10
2.1.4	Difficulties in Achieving Perfect Completeness	11
2.2	Our Techniques	11
2.2.1	A First Attempt: the Quadratic Grassmann Encoding	11
2.2.2	Variations on the Quadratic Grassmann Encoding	13
2.2.3	A Second Attempt: Three-Step Construction	14
2.2.4	Our Outer PCP	15
2.2.5	Our Middle PCP	16
2.2.6	Our Inner PCP	18
3	Preliminaries	21
3.1	General Notations	21
3.2	Sub-4-to-1 Games	22
3.3	Technical Ingredients from Prior Work	22
3.3.1	Approximate Coloring of Hypergraphs	22
3.3.2	Grassmann Agreement Test	23
3.3.3	List Decoding Bounds	24
3.4	Proof Organization	25
3.5	Parameter Relations	25
4	The Outer PCP	26
4.1	Preparation: Tripled Sets	26
4.1.1	Thinning, and Thinning with Advice	27
4.2	Preparation: The NAE Predicate	28
4.2.1	Linear Functionals vs. Bilinear Forms	29
4.3	The Equation vs. Variable Game	31
4.4	From Joint Satisfaction to Bilinear Forms	34
5	The Middle PCP	37
5.1	Preparation: Thinning with Subspaces	37
5.2	The Local Tensor Check Game	39
5.3	Soundness Analysis	40
5.3.1	Preparing for Grassmann Decoding	41
5.3.2	Invoking the Grassmann Decoding Theorem	42
5.3.3	Deriving Strategy for the Outer PCP	44
5.4	Lazy Parallel Repetition	47

6	The Inner PCP	48
6.1	Preparation: Tripled Packets	48
6.1.1	Thinning of Tripled Packets	50
6.2	Preparation: Low-Rank Grassmann	51
6.2.1	Construction from Hadamard Code	51
6.2.2	Mixed-Type Advice Sequences	53
6.2.3	Zoom-out Probabilities	55
6.2.4	Mixed-Type Grassmann Graph	57
6.2.5	Extension of Agreement	59
6.3	The 4-to-1 Game Construction	61
6.4	Soundness Analysis	64
6.4.1	Notation Setup	65
6.4.2	Covering Property of Mixed-Type Subspaces	66
6.4.3	Alice's Existence of Decoding	69
6.4.4	Bob's Existence of Decoding	71
6.4.5	Sending Bob's Decoding back to Alice	75
6.4.6	Consistency of Decodings	77
6.4.7	Deriving Strategy for the Middle PCP	82
7	Acknowledgments	86
A	Basic Linear Algebra	91
B	From Sub-4-to-1 to Exact 4-to-1 Games	94
C	Approximate Coloring of Hypergraphs	96
D	Grassmann Decoding Theorems	103
D.1	The Expansion Theorem	103
D.2	From Expansion to Decoding	104
E	Linearity Testing and List Decoding Bounds	107
F	Covering Properties	110
F.1	Covering in the Outer PCP	110
F.2	Covering in the Middle PCP	113
F.3	Covering in the Inner PCP	114

1 Introduction

The PCP Theorem [FGL⁺96, AS98, ALM⁺98] is a fundamental result in theoretical computer science with many consequences. Most relevant to the current paper are the applications in the area of hardness of approximation, in which the PCP theorem often serves as the starting point for reductions. The combination of Fourier analysis with the long-code (or, in some cases, other error correcting codes) has proven itself to be a very successful recipe, leading to many strong hardness of approximation results [Fei98, Hås01, DS05, Zuc07]. However, this paradigm appears to be incapable of establishing optimal results for many other problems, and below are a few notable examples:

- (1) The Max-Cut problem: given a graph $G = (V, E)$, the goal is to partition the vertex set into two sides A, B so as to maximize the number of edges crossing between A and B . A polynomial time algorithm due to [GW95] achieves the approximation ratio $\alpha_{GW} \approx 0.878$, and the best known **NP**-hardness result [TSSW00] has ratio $\frac{16}{17} + \varepsilon$, for any $\varepsilon > 0$.
- (2) The Vertex-Cover problem: given a graph $G = (V, E)$, the goal is to find the smallest set of vertices $A \subseteq V$ that touches all edges of E . Known polynomial time algorithms achieve approximation ratio 2, and the best known **NP**-hardness result [KMS25, DKK⁺25, DKK⁺21, KMS23] has ratio $\sqrt{2} - \varepsilon$, for any $\varepsilon > 0$.
- (3) The 3-coloring problem: given a graph $G = (V, E)$ promised to be 3-colorable, the goal is to find a proper k -coloring of the vertices of G with k as small as possible. Polynomial time algorithms for this problem have been studied extensively over the years [Wig83, KMS98, BK97, ACC06, Chl07, KT17, KTY24, BHL26], and the state-of-the-art algorithm achieves $k = |V|^{0.2-\varepsilon}$ for a small explicit $\varepsilon > 0$. The **NP**-hardness of this problem has also been studied [KLS00, GK04, BBKO21], and the state-of-the-art **NP**-hardness result is for $k = 5$.

To make progress on these problems, Khot [Kho02b] introduced the Unique-Games Conjecture and the d -to-1 Games conjectures, which we present next.

1.1 Label-Cover, Unique Games and d -to-1 Games

It is convenient to discuss PCPs in the language of the label-cover problem, defined as follows.

Definition 1.1. An instance Ψ of the label-cover problem consists of a bipartite graph $G = (L \sqcup R, E)$,¹ alphabets Σ_L, Σ_R , and a collection of constraints $\{\Phi_e \subseteq \Sigma_L \times \Sigma_R\}_{e \in E}$. For any given positive integers d and d' , a constraint $\Phi_e \subseteq \Sigma_L \times \Sigma_R$ is called a d -to- d' constraint if there is a partition $\Sigma_L = \Sigma_{L,1} \sqcup \dots \sqcup \Sigma_{L,t}$ into sets of size d and a partition $\Sigma_R = \Sigma_{R,1} \sqcup \dots \sqcup \Sigma_{R,t}$ into sets of size d' such that

$$\Phi_e = \bigcup_{i=1}^t \Sigma_{L,i} \times \Sigma_{R,i}.$$

Given a label-cover instance Ψ and assignments $A_L: L \rightarrow \Sigma_L, A_R: R \rightarrow \Sigma_R$, we define

$$\text{val}_\Psi(A_L, A_R) = \frac{|\{e = (u, v) \in E \mid (A_L(u), A_R(v)) \in \Phi_e\}|}{|E|},$$

that is, the fraction of constraints that are satisfied by A_L, A_R . We define the value of Ψ as

$$\text{val}(\Psi) = \max_{A_L, A_R} \text{val}_\Psi(A_L, A_R).$$

¹We always allow parallel edges, so E is a multi-set.

For parameters $0 < s < c \leq 1$, an input to the promise problem $\text{GapLC}(c, s)$ is a label cover instance Ψ that either has $\text{val}(\Psi) \geq c$ or $\text{val}(\Psi) \leq s$, and the goal is to distinguish between the two cases. The basic PCP theorem [FGL⁺96, AS98, ALM⁺98] combined with the parallel repetition theorem [Raz98] gives:

Theorem 1.2. *For all $\varepsilon > 0$, there exists a positive integer r such that $\text{GapLC}_r(1, \varepsilon)$ is **NP-hard**. Here GapLC_r is the GapLC problem in which both alphabets have size at most r .*

Khot conjectured that versions of Theorem 1.2 continue to hold even when the constraints are d -to-1 for a small d . Towards presenting these conjectures, we make the following definition.

Definition 1.3. Let d and d' be positive integers. An instance Ψ of label-cover is called a d -to- d' game if all of its constraints are d -to- d' . In the case that $d = d' = 1$, Ψ is called a unique-game. We write $\text{GapUG}_r(c, s)$ for the restriction of $\text{GapLC}_r(c, s)$ to unique-game instances, and $\text{Gap-}d\text{-to-}d'_r(c, s)$ for its restriction to d -to- d' game instances.

It is easy to see that one cannot hope for Theorem 1.2 to hold for unique-games, and Khot [Kho02b] conjectured that allowing for imperfect completeness remedies that:

Conjecture 1.4. *For any $\varepsilon > 0$, there exists $r \in \mathbb{N}^+$, such that $\text{GapUG}_r(1 - \varepsilon, \varepsilon)$ is **NP-hard**.*

For $d \geq 2$ and $d' = 1$, he conjectured that the assertion of Theorem 1.2 should hold as is. More precisely:

Conjecture 1.5. *For any $\varepsilon > 0$ and any integer $d \geq 2$, there exists a positive integer r such that $\text{Gap-}d\text{-to-}1_r(1, \varepsilon)$ is **NP-hard**.*

These conjectures, and especially Conjecture 1.4, have been shown to have remarkable implications, see for example [KR08, KKMO07, Rag08, KV15] and [Kho10b, Kho10a, Tre12, Kho14] for surveys, and significant effort has gone into studying them. On the algorithmic front, connections with semi-definite programming, sum-of-squares algorithms and graph expansion have led to the development of very powerful techniques and a number of algorithms for unique-games with non-trivial guarantees [CMM06, AKK⁺08, ABS15]. On the hardness front, a line of work [KMS25, DKK⁺25, DKK⁺21, KMS23] (with contributions from [BKS19, KMMS25]) established the imperfect completeness version of Conjecture 1.5, showing that for all $\varepsilon > 0$, there is $r \in \mathbb{N}^+$ such that $\text{Gap-2-to-1}_r(1 - \varepsilon, \varepsilon)$ is **NP-hard**. This implies that for all $\varepsilon > 0$ there exists $r \in \mathbb{N}^+$ such that $\text{GapUG}_r(1/2, \varepsilon)$ is **NP-hard**, which to date is the best evidence towards Conjecture 1.4.

The difference between Conjecture 1.5 and its imperfect completeness version is significant in a number of ways:

- (1) **Implications:** there are a number of hardness of approximation results that crucially rely on perfect completeness, most prominently graph coloring problems.
- (2) **Techniques:** the approach taken by [KMS25, DKK⁺25, DKK⁺21, KMS23] inherently incurs imperfect completeness. Currently, constructions of low-soundness PCPs with perfect completeness follow composition of PCPs, for example [MR10, DH13, DHK15], which at the very least require constructions that already have perfect completeness and small soundness (with perhaps a large alphabet which is then reduced), or from parallel repetition [Raz98, Hol09, Rao11], which inherently increases the d -parameter rapidly.

1.2 Main Result

Our main result is that Conjecture 1.5 holds for $d = 4$ and $d' = 1$.

Theorem 1.6. *For all $\varepsilon > 0$, there exists $r \in \mathbb{N}^+$, such that $\text{Gap-4-to-1}_r(1, \varepsilon)$ is **NP-hard**.*

1.2.1 Implications

We now discuss some implications of [Theorem 1.6](#). Using known connections between d -to-1 games and graph coloring/independent sets [[DMR09](#), [KOWŻ23](#), [GS20](#)], we get the following results.

Corollary 1.7. *For any integer $k \geq 3$, given a graph G , it is **NP**-hard to distinguish between the following two cases:*

- (1) **Yes case:** G is 3-colorable.
- (2) **No case:** G is not k -colorable.

Previously, [Corollary 1.7](#) was known [[BBKO21](#)] for $k = 5$, or in the case the condition in the yes-case only required a proper 3-coloring of $1 - \varepsilon$ fraction of the vertices [[HMS23](#)].

Remark 1.8. Under slightly super-polynomial time reductions, our techniques give versions of [Corollary 1.7](#) for k growing with the instance size, but at a very slow rate. Namely, assuming **NP** has no algorithms running in time $n^{t(n)}$, we get that there are no polynomial time algorithms that color a given 3-colorable graph with $O(\log \cdots \log t(n))$ colors, where the number of logs is finite (probably at most 10, say).

In the next corollary, the condition in the completeness case is weaker, but the condition in the soundness case is stronger:

Corollary 1.9. *For all $\delta > 0$, given a graph G , it is **NP**-hard to distinguish between the following two cases:*

- (1) **Yes case:** G is 8-colorable.
- (2) **No case:** G has no independent set of relative size at least δ .

Using [[KS14](#)], we get the following result for hypergraphs:

Corollary 1.10. *For all $\delta > 0$, given a 3-uniform hypergraph G , it is **NP**-hard to distinguish between the following two cases:*

- (1) **Yes case:** G is 2-colorable.
- (2) **No case:** G has no independent set of relative size at least δ .

Using the results of [[HMRW14](#)], [Corollaries 1.7](#) and [1.9](#) show hardness results for low-rank matrix completion. An instance in the (k, r, ε, c) -completion problem is a matrix $A \in (\mathbb{R} \cup \{\perp\})^{n \times n}$, such that there exists $M \in \mathbb{R}^{n \times n}$ satisfying:

- (1) $|M(i, j)| \leq c$ and M has rank at most r .
- (2) Letting $\Omega \subseteq [n] \times [n]$ be the set of (i, j) such that $A(i, j) \neq \perp$, we have that $|\Omega| \geq 0.9n^2$ and for each $(i, j) \in \Omega$ we have $M(i, j) = A(i, j)$.

The goal is to find a matrix $B \in \mathbb{R}^{n \times n}$ of rank at most k , such that $|B(i, j)| \leq c$ for all (i, j) and

$$\sum_{(i,j) \in \Omega} |A(i, j) - B(i, j)|^2 \leq \varepsilon n.$$

Applying [[HMRW14](#), Theorem 1.8] on [Corollary 1.7](#) gives:

Corollary 1.11. *For all $k > 3$ and $c > 1$, the $(k, 3, 0, c)$ -completion problem is **NP**-hard.*

Applying [[HMRW14](#), Theorem 1.9] on [Corollary 1.9](#) gives:

Corollary 1.12. *For all $k > 8$ and $c > 1$, the $(k, 8, \varepsilon, c)$ -completion problem is **NP**-hard for all $0 < \varepsilon < \frac{1}{(2ck)^2}$.*

1.3 Our Techniques

In this section we give a brief account of the components that go into the proof of [Theorem 1.6](#). We refer the reader to [Section 2](#) for a more thorough description.

For 2-to-1 games with almost-perfect completeness, the proof of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#) combines the following two components:

- (1) An outer PCP with completeness close to 1, vanishing soundness, and a feature called the “covering property” (originally appearing in [\[KS13\]](#)). This game is very far from being a 2-to-1 game, and to turn it into a 2-to-1 game it is composed with an appropriate inner PCP. The goal of the covering property is to facilitate the composition step.
- (2) An inner PCP with perfect completeness and a non-standard notion of soundness. The inner PCP is based on the Grassmann graph, the Grassmann encoding and the Grassmann agreement test. The Grassmann agreement test can be viewed as a local tester for the Grassmann code, but it turns out not to be sound in the traditional error correcting codes sense. Instead, it satisfies a weaker notion of soundness, which we refer to as non-standard soundness.

The outer PCP and inner PCP are then composed, and the covering property of the outer PCP is used in the soundness analysis of the composed PCP (even though the inner PCP only satisfies a non-standard notion of soundness).

The outer PCP construction of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#) is based on the hardness of approximation result of [\[Hås01\]](#) for solving linear equations, which inherently has imperfect completeness, and this propagates throughout their construction. To remedy that, a key difficulty is to come up with an outer PCP that has perfect completeness and simultaneously admits (some version of) the covering property.

We start our outer PCP construction based on hardness of solving a system of quadratic equations (which has perfect completeness). However, the Grassmann agreement test (which is still basically the only tool we have to achieve d -to-1-ness in the inner PCP) is inherently a “linear” test and cannot incorporate quadratic equations. In order for quadratic equations to be accommodated in a d -to-1 way, we add a layer of construction called the “middle PCP” between the outer and inner PCPs. In the middle PCP, we carry out a low-rank test that allows us to convert the quadratic equations into linear ones.

However, this linearization of quadratic equations destroys the covering property that is essential for composing with a Grassmann-based inner PCP. To remedy that, we have to come up with another two key ideas:

- (1) We do a “lazy parallel repetition” in the middle PCP. This creates room for covering properties while preserving the soundness.
- (2) The covering property we get from lazy parallel repetition is still not sufficient for composing with the Grassmann agreement test of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#). As a workaround, we base our inner PCP on a combination of standard Grassmann graphs over matrix spaces $\mathbb{F}_2^{n \times n}$ with a sparser version of them, known as the low-rank Grassmann graph over $\mathbb{F}_2^{n \times n}$, recently defined by [\[Gol23\]](#).

Statement of AI use: the mathematical ideas and the overall approach presented in this paper are due to the authors. ChatGPT 5.6, 6 and 6.1 were used for polishing and proofreading.

2 Proof Overview

In this section we give an overview of the proof of [Theorem 1.6](#). It will be useful to first discuss the construction of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#) which achieves imperfect completeness. We then discuss why it fails to have perfect completeness, and then in [Section 2.2](#) we explain preliminary attempts at fixing that, building towards our construction.

2.1 The Imperfect Completeness Construction

In this section we explain the components that go into the construction of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#).

2.1.1 The Outer PCP

It will often be easier for us to describe label-cover instances in the equivalent, active language of 2-prover-1-round games, which we introduce next. In a 2-prover-1-round game, a verifier samples a challenge $e = (u, v)$, sends u to a prover named Alice, sends v to a prover named Bob. Upon receiving their challenges, they respond with labels (they are not allowed to communicate once they get their challenges), and based on their responses the verifier decides to accept or reject. The value of the game is the maximum, over all strategies of Alice and Bob, of the probability that the verifier accepts. Identifying the individual challenges the players receive as vertices of a bipartite graph, pairs of challenges the verifier may sample with its edges, and the verifier's acceptance criteria with the constraints, one gets the equivalence. It is easy to see that the value of a game is exactly the value of the resulting label cover instance.

With this in mind, the reduction of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#) starts with the result of [\[Hås01\]](#) regarding the approximability of $3\text{Lin}_{\mathbb{F}_2}$.

Definition 2.1. An instance of the $3\text{Lin}_{\mathbb{F}_2}$ problem consists of a set of variables $\mathcal{V}$ and a set of equations $\mathcal{E}$, where each $e \in \mathcal{E}$ is a linear equation over $\mathbb{F}_2$ containing 3 distinct variables.

Håstad proved that for all $\varepsilon > 0$, $\text{Gap}3\text{Lin}_{\mathbb{F}_2}(1 - \varepsilon, 1/2 + \varepsilon)$ is **NP**-hard, and the reduction of [\[KMS25, DKK⁺25, DKK⁺21, KMS23\]](#) starts off with (some regularized version of) this problem. More specifically, they use the parallel repetition theorem to prove **NP**-hardness for a certain type of label-cover instance $\Psi_{q,\beta,k} = \Psi_{q,\beta,k}(\mathcal{V}, \mathcal{E})$, which we present below in the active 2-prover-1-round game view, and refer to as the β -smooth k -fold repeated game. For technical reasons, this game contains an additional feature called “advice”, which we encourage the reader to ignore in a first reading.

1. **Alice's challenge:** the verifier samples equations $e_1, \dots, e_k$ from $\mathcal{E}$ uniformly and independently, and sets E to be the set of all variables that appear in them.
2. **Bob's challenge:** for each $i \in \{1, \dots, k\}$ independently, with probability $1 - \beta$, the verifier takes E'_i to be the set of variables in e_i , and with probability β the verifier chooses E'_i to consist of a single uniformly chosen variable from e_i . The verifier sets $E' = E'_1 \cup \dots \cup E'_k$.
3. **Advice:** the verifier chooses $b^{(1)}, \dots, b^{(q)} \in \mathbb{F}_2^{E'}$ uniformly, and then takes $a^{(1)}, \dots, a^{(q)} \in \mathbb{F}_2^E$ where $a^{(i)}$ is obtained from $b^{(i)}$ by filling the missing coordinates with 0's. We write $B = (b^{(1)}, \dots, b^{(q)})$ and $A = (a^{(1)}, \dots, a^{(q)})$.
4. **Acceptance criteria:** the verifier sends (E, A) to Alice, and (E', B) to Bob. They respond with vectors $x \in \mathbb{F}_2^E$ and $y \in \mathbb{F}_2^{E'}$ respectively, and the verifier accepts if and only if x satisfies all of the equations $e_1, \dots, e_k$ and $x|_{E'} = y$.

The works [KMS25, DKK+25, DKK+21, KMS23] prove that for all $\varepsilon > 0$, it is **NP**-hard to distinguish between the case that $\text{val}(\Psi_{q,\beta,k}) \geq 1 - \varepsilon$, and the case that $\text{val}(\Psi_{q,\beta,k}) \leq 2^{-\Omega_q(\beta k)}$. Here and throughout, one should think of q as an absolute constant, and of β as slightly larger than $1/k$, say $\beta = k^{-3/4}$. The game $\Psi_{q,\beta,k}$ has several useful features in the context of 2-to-1 Games:

- (1) **Simplicity of the constraints:** the constraints of $\Psi_{q,\beta,k}$ can all be seen to be linear equations in the responses of the provers. This is because the starting point, the $3\text{Lin}_{\mathbb{F}_2}$, consisted of linear constraints, and on top of that we have the consistency constraints between the responses of Alice and Bob, which are also linear.
- (2) **The covering property:** for a fixed E , the spaces $\mathbb{F}_2^{E'}$ living on Bob's side cover Alice's space $\mathbb{F}_2^E$ almost perfectly. For example, fixing E , taking E' randomly as described above conditioned on E , then $y \in \mathbb{F}_2^{E'}$ and lifting it to $x \in \mathbb{F}_2^E$ by filling in the missing coordinates with 0's, we have that the distribution of x is statistically close to the uniform distribution over $\mathbb{F}_2^E$ (this property first appeared in [KS13] in a somewhat different context).

The relevance of these properties will become clear in the next part, the inner PCP.

2.1.2 The Inner PCP

The 2-prover 1-round game $\Psi_{q,\beta,k}$ constructed in Section 2.1.1 is far from 2-to-1, because given a Bob-answer $y \in \mathbb{F}_2^{E'}$, there are many possible Alice-answers $x \in \mathbb{F}_2^E$ consistent with it. In order to make it a 2-to-1 game, in a single query we can ask the provers only for a smaller piece of information.

For each possible question (E, A) to Alice, we ask her to prepare her answer in “Grassmann encoding,” and instead of requesting a full answer $x \in \mathbb{F}_2^E$, we ask her to return only the information in one location of the Grassmann encoding of x .

The Grassmann encoding scheme is based on the Grassmann graph $\text{Gr}(\mathbb{F}_2^E, \ell)$, whose vertices are the ℓ -dimensional linear subspaces of $\mathbb{F}_2^E$. Two vertices L and L' are adjacent if and only if $\dim(L \cap L') = \ell - 1$. By a slight abuse of notation, we also use $\text{Gr}(\mathbb{F}_2^E, \ell)$ to denote the vertex set of this graph. The Grassmann encoding of a vector $x \in \mathbb{F}_2^E$ stores, at each location $L \in \text{Gr}(\mathbb{F}_2^E, \ell)$, the local linear function

$$F[L] : L \rightarrow \mathbb{F}_2 \text{ defined by } z \mapsto \langle z, x \rangle.$$

Similarly, we ask Bob to prepare his answer $y \in \mathbb{F}_2^{E'}$ in Grassmann encoding, where each location $L' \in \text{Gr}(\mathbb{F}_2^{E'}, \ell - 1)$ stores the local function

$$G[L'] : L' \rightarrow \mathbb{F}_2 \text{ defined by } z \mapsto \langle z, y \rangle.$$

The final 2-to-1 game is the composition of the outer PCP with the Grassmann graph gadget. In the composed PCP, upon choosing (E, A) and (E', B) as in $\Psi_{q,\beta,k}$, the verifier chooses a space L' from $\text{Gr}(\mathbb{F}_2^{E'}, \ell - 1)$ and a space $L \in \text{Gr}(\mathbb{F}_2^E, \ell)$ containing L' . The subspace $L \subseteq \mathbb{F}_2^E$ will be regarded as a subspace of Alice's space $\mathbb{F}_2^E$ by appending 0's in the missing coordinates. The verifier then sends (E, A, L) to Alice and (E', B, L') to Bob, expecting to get linear functions $F[E, A, L] : L \rightarrow \mathbb{F}_2$ and $G[E', B, L'] : L' \rightarrow \mathbb{F}_2$. The verifier accepts only if $G[E', B, L']$ agrees with the restriction $F[E, A, L]|_{L'}$. This is essentially a 2-to-1 game because for any possible choice of $G[E', B, L']$, there are at most two choices of $F[E, A, L]$ consistent with it.

Covering property and consistency: consider a question (E, A) for Alice in the outer PCP (think of ℓ as much smaller than k), and the Grassmann graph $\text{Gr}(\mathbb{F}_2^E, \ell)$. The covering property above asserts that if we sample E' as in the outer PCP and a vertex in the graph $\text{Gr}(\mathbb{F}_2^{E'}, \ell)$, lifting it to $\text{Gr}(\mathbb{F}_2^E, \ell)$ yields a nearly uniform vertex in the latter graph. This implies that if Alice's assignment $F[E, A, \cdot]$ has agreement ε' with an actual Grassmann codeword F , then with decent probability over E' , Bob's assignment $G[E', B, \cdot]$ agrees with the projection of F to $\mathbb{F}_2^{E'}$. In short, the covering property ensures the consistency between decodings of assignments of the provers holds.

The linear equations side conditions: recall that in the outer PCP we want to ensure that Alice's response $x \in \mathbb{F}_2^E$ satisfies a collection of k linear equations. Note that these equations correspond to requiring that the function $z \mapsto \langle z, x \rangle$ attains specific values on k inputs. More precisely, letting the equations be $e_1, \dots, e_k$, letting $s^{(i)} \in \mathbb{F}_2^E$ be the indicator vector of the variables appearing in e_i , and letting $t_i \in \mathbb{F}_2$ be the constant term of the equation e_i , we want to ensure that $\langle s^{(i)}, x \rangle = t_i$. To do so, we define the space $N_E = \text{span}(s^{(1)}, \dots, s^{(k)})$, and request Alice to give assignment $F[E, A, L + N_E]: (L + N_E) \rightarrow \mathbb{F}_2$ (instead of just $L \rightarrow \mathbb{F}_2$). The verifier then checks consistency between Alice and Bob similarly to the above, and additionally that $F[E, A, L + N_E]|_{N_E} = g_E$, where the linear function $g_E: N_E \rightarrow \mathbb{F}_2$ is defined by $g_E(s^{(i)}) = t_i$.

2.1.3 On the Non-Standard Notion of Soundness

One would wish that the Grassmann gadget in the inner PCP has the following type of soundness: suppose $F[L]$ is a linear map $L \rightarrow \mathbb{F}_2$ for each $L \in \text{Gr}(\mathbb{F}_2^E, \ell)$, such that

$$\mathbb{P}_{L_1, L_2 \in \text{Gr}(\mathbb{F}_2^E, \ell)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \mid \dim(L_1 \cap L_2) = \ell - 1 \right] \geq \delta \quad (2.1)$$

for some constant $\delta \in (0, 1)$, then there exists a linear function $f: \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^E, \ell)} \left[F[L] = f|_L \right] \geq \delta'$$

for some $\delta' \in (0, 1)$. However, this conclusion cannot be made, as we next explain. Take $\varepsilon > 0$ to be a small constant, and take a random set $X \subseteq \mathbb{F}_2^E \setminus \{0\}$ of size $2^{-\ell\varepsilon} \cdot 2^{|E|}$. For each $x \in X$ choose a random linear function $f_x: \mathbb{F}_2^E \rightarrow \mathbb{F}_2$, and set a table F on ℓ -dimensional subspaces L as follows:

- If L contains a unique point $x \in X$, define $F[L] = f_x|_L$.
- Otherwise, choose $F[L]$ as a random linear function on L .

Using the inclusion-exclusion formula, one can prove that for a random edge $\{L_1, L_2\}$ in the Grassmann graph, with probability at least $\Omega(\varepsilon)$ there is $x \in X$ such that $L_1 \cap X = L_2 \cap X = \{x\}$, and F satisfies such constraints. Thus, F passes the Grassmann test Equation (2.1) with $\delta = \Omega(\varepsilon)$. However, it only agrees on $o(1)$ locations with any given codeword from the Grassmann code.

This example tells us that while there might be no linear function that agrees with F globally, it may be possible to extract a linear function by focusing on certain substructures inside the Grassmann graph. Indeed, it turns out that what can be concluded from Equation (2.1) is something of this form: for at least $\exp(-O(\ell^2))$ fraction of $Q \in \text{Gr}(\mathbb{F}_2^E, q)$, where q depends only on δ , there exists $W \in \text{Gr}(\mathbb{F}_2^E, |E| - q)$ and a linear function $f: W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^E, \ell)} \left[F[L] \equiv f|_L \mid Q \subseteq L \subseteq W \right] \geq \delta'. \quad (2.2)$$

We refer to the spaces Q and W in Equation (2.2) as zoom-ins and zoom-outs, respectively, and encourage the reader to ignore W (it will be irrelevant for the majority of the discussion). In words, Equation (2.2) asserts that if F passes the Grassmann test with noticeable probability, then inside non-trivial fraction of zoom-ins of constant dimension q , it does have a global linear structure.

The proof of [KMS25, DKK⁺25, DKK⁺21, KMS23] has to deal with this non-standard notion of soundness, and this is the purpose of the advice feature in the game $\Psi_{q,\beta,k}$. More precisely, given Alice and Bob’s tables of assignments F and G for the composed PCP, one needs to be able to derive a strategy for the original game $\Psi_{q,\beta,k}$. However, the strategy that one can derive using Equation (2.2) heavily depends on the choice of what zoom-in Q is used. The advice feature allows the two provers in $\Psi_{q,\beta,k}$ to use (essentially) the same Q for decoding — namely the span of their advice vectors — which guarantees consistency between their answers.

2.1.4 Difficulties in Achieving Perfect Completeness

The construction for 2-to-1 games with imperfect completeness can be illustrated using Figure 1.

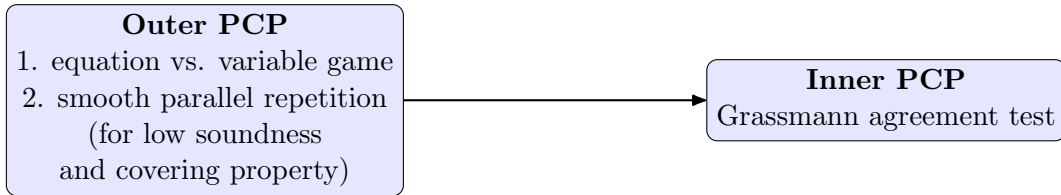


Figure 1: The imperfect-completeness construction of [KMS25, DKK⁺25, DKK⁺21, KMS23]

The above construction loses perfect completeness right from the start: it uses the $3\text{Lin}_{\mathbb{F}_2}$ problem, which inherently has imperfect completeness. Moreover, in some sense this seems necessary: the Grassmann encoding presented above only allows for linear checks in the encoded string $x \in \mathbb{F}_2^n$.

Thus, to achieve perfect completeness it is necessary to come up with an encoding scheme which is more powerful than the Grassmann encoding, in the sense that it allows for non-linear checks on the encoded string $x \in \mathbb{F}_2^E$. By itself this is not a hard task; for example, the long-code would work. However, the key difficulty is that one additionally needs the encoding scheme to satisfy a covering property, and then build an outer PCP with a suitable advice feature.

2.2 Our Techniques

In this section we discuss the new ideas that go into our construction.

2.2.1 A First Attempt: the Quadratic Grassmann Encoding

We begin by outlining a natural first attempt at a reduction achieving perfect completeness. It starts with the problem of quadratic equations, $3\text{QS}_{\mathbb{F}_2}$, defined as follows.

Definition 2.2. An instance of the $3\text{QS}_{\mathbb{F}_2}$ problem consists of a set of variables $\mathcal{V}$ and a set of equations $\mathcal{E}$, where each $e \in \mathcal{E}$ is a quadratic equation over $\mathbb{F}_2$ containing 3 distinct variables.

Using standard results, it can be proved that there is $s < 1$ such that $\text{Gap}3\text{QS}_{\mathbb{F}_2}[1, s]$ is **NP**-hard. Starting with an instance $(\mathcal{V}, \mathcal{E})$ of $3\text{QS}_{\mathbb{F}_2}$, one can construct the β -smooth k -fold repeated game corresponding to it, $\Psi_{\beta,k} = \Psi_{\beta,k}(\mathcal{V}, \mathcal{E})$ in the same way as in Section 2.1.1 (we ignore the advice for now). The main question is how to compose it with a Grassmann-style encoding so as to get to a d -to-1 Game.

In the game $\Psi_{\beta,k}$, the verifier performs two types of checks: consistency between the responses of Alice and Bob, and quadratic equations in the response of Alice. The Grassmann encoding is compatible with the former type of checks, but not with the latter type of checks, in the sense that we do not know how to incorporate checking quadratic equations on the encoded message into the Grassmann encoding itself. Instead, it is natural to consider the *quadratic Grassmann encoding*.

Let $x \in \mathbb{F}_2^E$ represent Alice's response in the game $\Psi_{\beta,k}$. In the quadratic Grassmann encoding, one considers the functions over $\mathbb{F}_2^{E \times E}$ defined by $z \mapsto \langle z, x \otimes x \rangle$, and takes its Grassmann encoding QF of x , which assigns to each ℓ -dimensional subspace $L \subseteq \mathbb{F}_2^{E \times E}$ the linear function

$$QF[L] : L \rightarrow \mathbb{F}_2 \text{ defined by } z \mapsto \langle z, x \otimes x \rangle.$$

The main benefit of the quadratic Grassmann encoding is that it indeed allows us to test quadratic equations as side conditions, as we explain next.

The quadratic-equation side conditions: Given a legitimate quadratic Grassmann codeword QF , it is possible to incorporate with it checks of quadratic equations on the encoded message. Indeed, suppose that $e_1, \dots, e_k$ are quadratic equations over E , let $s^{(1)}, \dots, s^{(k)} \in \mathbb{F}_2^{E \times E}$ be the indicator vectors of the pairs that appear in $e_1, \dots, e_k$ respectively, and let $t_1, \dots, t_k$ be the constant terms. Then the equation e_i can be written as $\langle s^{(i)}, x \otimes x \rangle = t_i$ for each $i \in \{1, \dots, k\}$. As before, this can be folded into the encoding by defining $N_E = \text{span}(s^{(1)}, \dots, s^{(k)})$, asking for the table to assign values to the sum $L + N_E$ (instead of to just L), and requiring that their projection onto N_E completely agrees with the linear function $g : N_E \rightarrow \mathbb{F}_2$ defined by $g(s^{(i)}) = t_i$. This way of incorporating quadratic side conditions will work for all of the constructions we present below, so for simplicity of presentation they will be omitted henceforth.

On the other hand, the quadratic Grassmann encoding has 2 very significant drawbacks:

- (1) **Codeword testing:** Even ignoring the issue of non-standard-type soundness, the Grassmann agreement test from [Section 2.1.2](#) is not actually a tester for the quadratic Grassmann code. Namely, if a table G that assigns each ℓ -dimensional subspace $L \subseteq \mathbb{F}_2^{E \times E}$ a linear function $G[L] : L \rightarrow \mathbb{F}_2$ passes it with non-negligible probability, then at best we will be able to argue that it has significant agreement with the Grassmann encoding of an arbitrary $x' \in \mathbb{F}_2^{E \times E}$, i.e., not necessarily of rank 1. We need an additional feature that will guarantee that x' has rank 1 (or at the very least small rank) and is symmetric.
- (2) **The covering property:** The covering property does not hold for the quadratic Grassmann encoding. Namely, fixing a question for Alice E and looking at typical possible questions E' for Bob (conditioned on E), the (lifting of the) spaces $\mathbb{F}_2^{E' \times E'}$ do not cover $\mathbb{F}_2^{E \times E}$. Indeed, the number of such typical questions for Bob is roughly $\binom{3k}{2\beta k}$, and the size of Bob's space is roughly $2^{(3-2\beta)^2 k^2}$, so in total they can cover at most

$$\binom{3k}{2\beta k} 2^{(3-2\beta)^2 k^2} \leq 2^{O(\beta k \log(1/\beta))} 2^{9k^2 - 8\beta k^2} = o(2^{9k^2})$$

points in $\mathbb{F}_2^{E \times E}$, which is a tiny fraction.

The first issue, namely ensuring that the encoded message has a low rank, is significantly easier to handle, and to do so we incorporate tensor tests. More precisely, instead of asking for the value of the Grassmann encoding at a subspace $L \subseteq \mathbb{F}_2^{E \times E}$, we will also take a random subspace $U \subseteq \mathbb{F}_2^E$ of dimension ℓ , and then ask for the value at the subspace $L + U \otimes U$, requiring that the projection

onto $U \otimes U$ is of rank at most 1. This yields the following 4-to-4 Grassmann agreement + tensor test. Upon receiving a table F assigning linear functions to spaces $L + U \otimes U$ as above, do the following:

1. Sample $L_1, L_2 \subseteq \mathbb{F}_2^{E \times E}$ of dimension ℓ intersecting at dimension $\ell - 1$, and $U_1, U_2 \subseteq \mathbb{F}_2^E$ of dimension ℓ intersecting at dimension $\ell - 1$.
2. Query $F[L_1 + U_1 \otimes U_1]$ and $F[L_2 + U_2 \otimes U_2]$. Accept if they agree on

$$L_1 \cap L_2 + (U_1 \cap U_2) \otimes (U_1 \cap U_2),$$

and their respective projections onto $U_1 \otimes U_1$ and $U_2 \otimes U_2$ are symmetric and of rank at most 1.

Given the (non-standard) soundness of the basic Grassmann agreement test, one can analyze the Grassmann agreement + tensor test and show that it satisfies a similar (non-standard) notion of soundness. Also, this test is 4-to-4: given a linear function on L_1 , there are at most 2 linear functions on L_2 that agree with it, and given a symmetric rank-1 functional on $U_1 \otimes U_1$, there are at most 2 symmetric rank-1 linear functions on $U_2 \otimes U_2$ agreeing with it.

Ensuring symmetry is more straightforward. To do that, define for distinct points $i, j \in E$ the matrix $M_{i,j} \in \mathbb{F}_2^{E \times E}$ which is 1 only at locations (i, j) and (j, i) , and set $N_{\text{sym}} = \text{span}(\{M_{i,j} \mid i \neq j\})$. Then, $x' \in \mathbb{F}_2^{E \times E}$ is symmetric if and only if the function $z \mapsto \langle z, x' \rangle$ vanishes on N_{sym} . Thus, instead of requesting an assignment on $L + U \otimes U$, the verifier requests an assignment on $L + U \otimes U + N_{\text{sym}}$, and checks that its projection on N_{sym} vanishes.

The second issue, namely the fact that the covering property fails, is substantially more difficult to handle, and in the next section we begin the discussion about it.

2.2.2 Variations on the Quadratic Grassmann Encoding

From now on, it will be convenient for us to think of points from $\mathbb{F}_2^{E \times E}$ and $\mathbb{F}_2^{E' \times E'}$ as matrices. The covering property fails for the quadratic Grassmann encoding because if, letting Bob's question be denoted by E' , we have $i \in E \setminus E'$, then i -th row and column will always be 0 in liftings from $\mathbb{F}_2^{E' \times E'}$ to $\mathbb{F}_2^{E \times E}$. On the other hand, typical matrices from $\mathbb{F}_2^{E \times E}$ do not contain fully-0 rows. This raises the question of whether we can replace the structure of $E \times E$ with a sparser structure that circumvents this atypical behaviour of liftings. Moreover, requiring a response from the provers for each pair of variables in their respective variable sets is not necessary, as the quadratic equations we wish to check only require access to $\Theta(k)$ pairs (out of the $\binom{k}{2}$ many ones that exist).

This view motivates the following general recipe: can we find a graph H with vertex set E and edge set $\mathcal{E}$, such that we can restrict the quadratic Grassmann encoding to $\mathbb{F}_2^{\mathcal{E}}$ in a meaningful way? The quadratic Grassmann encoding discussed above corresponds to choosing H to be a complete graph, but there are many other options for H . Below are a few simple choices we tried:

- (1) Expander graphs: One can try to take H to be an arbitrary sparse expander graph. It can be shown that if the degree of H is small then now the covering property will hold. Unfortunately, an arbitrary expander graph does not support any form of tensor tests.
- (2) Cliques in a sparse high-dimensional expander: one can take a sparse high-dimensional expander $X = (X(0), \dots, X(k))$, where $X(0)$ is the vertex set, and for each i , $X(i) \subseteq \binom{X(0)}{i+1}$, and take H to be the graph underlying it. Because the degree of X is constant, the covering property holds. Also, we can perform local type of tensor tests: if $K \in X(k)$ is a $(k+1)$ -face,

then K is a clique in X , so we can choose a subspace $U \subseteq \mathbb{F}_2^{X(0)}$ fully supported in K , and have access to all of the entries in $U \otimes U$.

This observation initially seems very promising, but it has one serious issue. We can only afford to perform such a local tensor test for a single clique (or perhaps $O(1)$ -many cliques if we are fine with increasing the value of d for which we are proving [Conjecture 1.5](#)). Unfortunately, these localized tensor tests do not actually guarantee that the encoded function has a small rank, and Alice and Bob can use a cheating strategy in the following way. When Alice receives a space of the type $L + U \otimes U$, she extracts from it a rank-1 vector, and takes any element v in its support. Then it is highly likely that v belongs to K , and because X has constant degree, the neighbourhood $N(v)$ of v has constant size. Thus, Alice can choose a linear function on $\mathbb{F}_2^{X(1)}$ which is rank-1 on $\mathbb{F}_2^{X(1) \cap (N(v) \times N(v))}$ but otherwise arbitrary, and responds according to it. Bob proceeds in the same way, where they agree beforehand on what is the rank-1 function they will use, and what the arbitrary function they will use on the rest of the space.

We remark that another attempt at implementing tensor tests via high-dimensional expanders is based on coboundary-type expansion, and we have not explored this thoroughly.

In summary, the attempts above suggest that there are meaningful variants of the quadratic Grassmann encoding that enjoy the covering property, but they come at the cost of, at best, being able to ensure small rank locally. This type of guarantee seems insufficient, at least with an outer PCP along the lines of [Section 2.1.1](#).

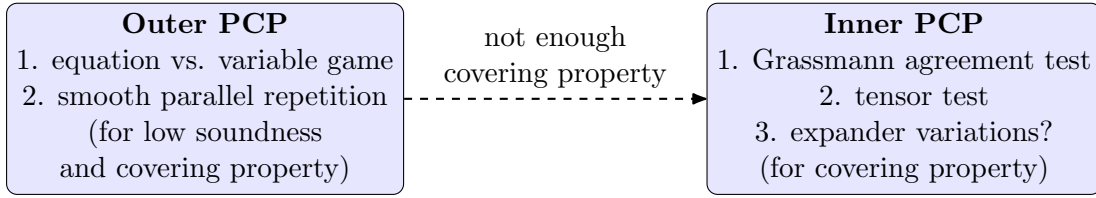


Figure 2: Our failed attempt for perfect completeness

2.2.3 A Second Attempt: Three-Step Construction

So far, the described attempts to create covering property for a quadratic-Grassmann-based inner PCP are not successful. In particular, it seems that the idea of “sparsifying” the quadratic-Grassmann encoding conflicts with tensor test. To address this conflict, we separate the tensor test from the inner PCP and name it the “middle PCP” (see [Figure 3](#)). Notice that the tensor test (proposed in [Section 2.2.1](#)) is a Grassmann structure over $\mathbb{F}_2^E$, instead of over $\mathbb{F}_2^{E \times E}$. Therefore, the tensor test by itself is compatible with the covering property provided by the smooth parallel repetition in the outer PCP. We only have to create more covering property for the inner PCP (which now consists only of a Grassmann agreement test) *after* incorporating tensor tests into the middle PCP. This will be provided by a “lazy parallel repetition” on the level of the middle PCP (see [Figure 3](#)).

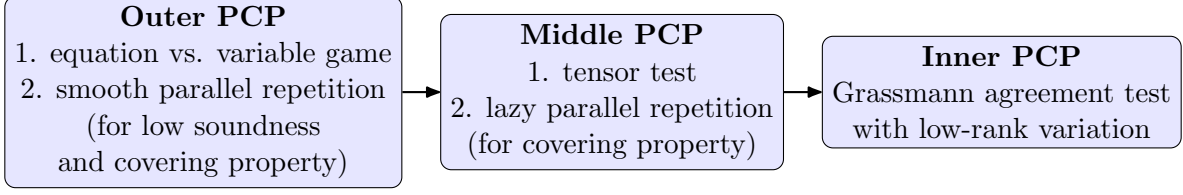


Figure 3: Our construction for perfect completeness

2.2.4 Our Outer PCP

Besides using quadratic equations to replace linear ones, the main difference between our outer PCP and the one in [Section 2.1.1](#) is that we need to establish a stronger soundness condition. This is because the tensor tests we ultimately perform will only guarantee that the decoded assignment has low rank (as opposed to rank-1).

Given a collection of quadratic equations $(\mathcal{V}, \mathcal{E})$ over $\mathbb{F}_2$ and a solution $x \in \mathbb{F}_2^{\mathcal{V}}$, one can consider the rank-1 (or 0) matrix $x \otimes x \in \mathbb{F}_2^{\mathcal{V} \times \mathcal{V}}$ and view it as an assignment to $(\mathcal{V}, \mathcal{E})$. This proposes a broader set of solutions given by low-rank matrices, motivating the following definition:

Definition 2.3. Let e be a quadratic equation over $\mathcal{V}$ described by $\langle x, Ax \rangle = b$ for a matrix $A \in \mathbb{F}_2^{\mathcal{V} \times \mathcal{V}}$, and let $x^{(1)}, \dots, x^{(r)} \in \mathbb{F}_2^{\mathcal{V}}$ be assignments. We say that $x^{(1)}, \dots, x^{(r)}$ jointly satisfy e if

$$\sum_{i=1}^r \sum_{u,v \in \mathcal{V}} A_{uv} x_u^{(i)} x_v^{(i)} = b.$$

We remark that [\[KS17\]](#) use the same notion, which they refer to as “superposition complexity”. With this definition in mind, the starting point of our reduction is the following result.²

Theorem 2.4. *For all $r \in \mathbb{N}^+$, there exists $\varepsilon > 0$ such that the following holds. Given an instance $\Psi = \Psi(\mathcal{V}, \mathcal{E})$ of $3\text{QS}_{\mathbb{F}_2}$, it is **NP**-hard to distinguish between the following two cases:*

- (1) **Yes case:** $\text{val}(\Psi) = 1$.
- (2) **No case:** for all $x^{(1)}, \dots, x^{(r)} \in \mathbb{F}_2^{\mathcal{V}}$, we have that $x^{(1)}, \dots, x^{(r)}$ jointly satisfy at most $1 - \varepsilon$ fraction of the equations in $\mathcal{E}$.

As in [Section 2.1.1](#), we can view the instances in [Theorem 2.4](#) as an equation vs. variable game, and then apply a β -smooth k -fold parallel repetition to get a game $\Psi_{q,\beta,k}$.

The soundness condition in [Theorem 2.4](#) translates to a variant of $\Psi_{q,\beta,k}$ where we ask the provers to return r vectors. In particular, upon receiving a question (E, A) , Alice needs to return $x^{(1)}, \dots, x^{(r)} \in \mathbb{F}_2^E$ that jointly satisfy all the equations in E . It turns out that one can modify this game into a different game where we ask the provers to return low-rank symmetric matrices. In particular, Alice now needs to return a symmetric matrix $X \in \mathbb{F}_2^{E \times E}$ that satisfies the equations in E , in the sense that for each e in E described by $\langle x, Ax \rangle = b$, we have

$$\sum_{u,v \in E} A_{uv} X_{uv} = b.$$

In [Section 4.4](#), we will show that this conversion from joint satisfaction to low-rank-matrix answers does not affect the soundness by too much.

²A more formal version of [Theorem 2.4](#) is stated in [Theorem 3.4](#).

For the purpose of composing with the middle and inner PCPs, we view an Alice-answer $X \in \mathbb{F}_2^{E \times E}$ as a symmetric bilinear map $f_X : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ defined by

$$f_X(x \otimes y) = \sum_{u,v \in E} X_{uv} x_u y_v \quad \text{for all } x, y \in \mathbb{F}_2^E.$$

Similarly, Bob should return a bilinear map $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$.

2.2.5 Our Middle PCP

In the outer PCP described in [Section 2.2.4](#), the verifier (roughly speaking) carries out the following (cf. [Section 2.1.1](#)):

1. Sample (E, A) and send it to Alice. Sample (E', B) and send it to Bob.
2. Receive from Alice a symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ of rank at most r , and from Bob a symmetric bilinear map $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$.
3. Accept if the restriction of f to $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$ is identical to g .

Local tensor check: the first goal of the middle PCP is to replace the global rank check “rank(f) $\leq r$ ” with a local tensor check. We move to the game Ψ_{mid} where the verifier carries out the following:

1. Sample (E, A) and (E', B) as in the outer PCP game $\Psi_{q,\beta,k}$.
2. Sample a subspace $U \in \text{Gr}(\mathbb{F}_2^{E'}, \ell_2)$ and a subspace $U' \in \text{Gr}(\mathbb{F}_2^{E'}, \ell_2 + 1)$ containing U . The subspace $U \subseteq \mathbb{F}_2^{E'}$ will be regarded as a subspace of Alice’s space $\mathbb{F}_2^E$ by appending 0’s in the missing coordinates.
3. Send (E, A, U) to Alice and (E', B, U') to Bob.
4. Receive from Alice a symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ such that rank($f|_{U \otimes U}$) ≤ 1 , and from Bob a symmetric bilinear map $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$.
5. Accept if the restriction of f to $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$ is identical to g .

In words, we have replaced the global rank check on Alice’s response with a local rank check, that verifies that the rank of f on $U \otimes U$ is at most 1, where U is a (nearly uniformly chosen) ℓ_2 -dimensional subspace given to Alice.

The completeness of this transformation is clear, but the soundness is much less so. Indeed, because we provide U to Alice, she knows where the rank test will be performed, and therefore she can potentially use that information to cheat. Nevertheless, we show that for all $\delta > 0$, if we fix r, q, ℓ_2 appropriately and let k be sufficiently large, then in the “no case” of [Theorem 2.4](#) we have $\text{val}(\Psi_{\text{mid}}) \leq \delta$. The intuition here is as follows:

- (1) If Alice did not use any cheating strategy, but her $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ was of rank more than r , then the probability that $f|_{U \otimes U}$ has rank at most 1 approaches 0 as ℓ_2 goes to infinity.
- (2) The type of cheating strategies Alice may use is limited. To see that, fix strategies F, G for Alice and Bob that achieve value at least s , fix the question of Bob, and sample two questions for Alice that only differ on the tensor test, say (E, A, U_1) and (E, A, U_2) . Using the Cauchy-Schwarz inequality, we get that with probability at least s^2 , Alice and Bob win both of these

challenges. In that case, Alice's functions $F[E, A, U_1]$, $F[E, A, U_2]$ have to agree with Bob's function, which is the same in both scenarios (his challenge has not changed). In particular, in that scenario we must have that

$$F[E, A, U_1]|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = F[E, A, U_2]|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}}.$$

In words, fixing (E, A) , we get that Alice's responses (as a function of the tensor test U she receives) must pass a sort of Grassmann agreement test. If that test had the standard notion of soundness, it would mean that Alice's responses have to basically follow an honest strategy, and a version of the argument from the first item will further guarantee that this honest strategy uses a low-rank function.

- (3) Using the non-standard notion of soundness (which we know to hold), the discussion in [Section 2.1.3](#) implies that after an appropriate zoom-in (and zoom-out, which we ignore for now), Alice's responses do behave like an honest strategy, and one can argue as in the first item. The implementation of the zoom-ins in the soundness analysis of Ψ_{mid} uses the advice A .

Lazy parallel repetition: next, we wish to turn the check that $f|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = g$ from Ψ_{mid} into a 2-to-1 test, and towards this end we intend to use the Grassmann encoding. A naive approach would have been to apply the Grassmann encoding directly on Alice's space $\mathbb{F}_2^E \otimes \mathbb{F}_2^E = \mathbb{F}_2^{E \times E}$ and on Bob's space $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} = \mathbb{F}_2^{E' \times E'}$, but as discussed in [Section 2.2.1](#) this fails due to the lack of the covering property. Our solution for this issue is to first hide the actual challenge within a large collection of trivial challenges, in an operation that we refer to as lazy repetition (we remark that it has appeared in PCP literature previously, see [\[Kho02a\]](#)). In the terminology of [Section 2.2.2](#), this amounts to taking a graph H which is a union of a large number of cliques (with no edges between them at all).

To describe the operation, fix a parameter t thought of as much larger than any of the previously mentioned parameters. Consider the game Ψ_{lazy} where the verifier carries out the following:

1. Sample $c \in [t]$, and sample challenges (E_c, A_c, U_c) , (E'_c, B_c, U'_c) as in Ψ_{mid} . We refer to c as the critical index.
2. For each $j \in [t] \setminus \{c\}$, sample an Alice-challenge (E_j, A_j, U_j) from Ψ_{mid} independently. We discard the obtained A_j and instead let A_j be a sequence of uniformly sampled vectors

$$a^{(1)}, \dots, a^{(q')} \in \mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j}.$$

Let $E'_j = E_j$, $B_j = A_j$ and $U'_j = U_j$.

3. We use calligraphic fonts to denote a sequence of objects. For instance, write $\mathcal{E} = (E_1, \dots, E_t)$ and $\mathcal{U}' = (U'_1, \dots, U'_t)$. Similarly define sequences $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{U}$. Let $\mathcal{V}(\mathcal{E}) = \bigoplus_{j=1}^t (\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j})$ and $\mathcal{V}(\mathcal{E}') = \bigoplus_{j=1}^t (\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j})$.
4. Send $(\mathcal{E}, \mathcal{A}, \mathcal{U})$ to Alice and $(\mathcal{E}', \mathcal{B}, \mathcal{U}')$ to Bob.
5. Alice must return a linear map $f : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ such that for each $j \in [t]$, the restriction of f to $\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j}$ is symmetric and satisfies all equations in E_j , and $\text{rank}(f|_{U_j \otimes U_j}) \leq 1$. Bob must return a linear map $g : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$.
6. Accept if $f|_{\mathcal{V}(\mathcal{E}')} = g$.

Lazy repetition is easily seen to preserve perfect completeness. It also does not worsen the soundness, because Alice and Bob still have to answer the questions (E_c, A_c, U_c) and (E'_c, B_c, U'_c) planted in the critical index, independent of what they do in the non-critical indices.

The main benefit of the lazy repetition is that it improves the covering property. More precisely, consider a random $x \in \mathcal{V}(\mathcal{E})$ obtained by the following process:

1. Sample c and $\mathcal{E}'$ as in Ψ_{lazy} .
2. Sample $y \in \mathcal{V}(\mathcal{E}')$, and lift to $x \in \mathcal{V}(\mathcal{E})$ by appending 0's in missing coordinates (which only happens in the critical index).

Then, provided that t is sufficiently large compared to k , the distribution of x is close to uniform in $\mathcal{V}(\mathcal{E})$. The intuition here comes from the following basic fact:

Claim 2.5. *Suppose that $(\Omega, \mathbb{P})$ is a discrete probability space, and $\Gamma \subseteq \Omega$ is an event such that $p = \mathbb{P}(\Gamma) > 0$. Then for each t , the following two distributions are $O_p(1/\sqrt{t})$ -close in statistical distance:*

- (1) *Sample $x_1, \dots, x_t \sim \mathbb{P}$ independently.*
- (2) *Sample $c \in [t]$, sample $x_c \sim \mathbb{P}$ conditioned on $x_c \in \Gamma$, and for $j \neq c$ sample $x_j \sim \mathbb{P}$ independently.*

In summary, the game Ψ_{lazy} has perfect completeness, small soundness, local tensor tests and the covering property. It can actually be composed with an appropriate version of the Grassmann graph but this is still not straightforward. In the next section we discuss why a naïve composition with the standard Grassmann encoding still fails, and explain how we circumvent this issue by taking an appropriate variant of the Grassmann encoding.

2.2.6 Our Inner PCP

A natural attempt at composing Ψ_{lazy} with the Grassmann encoding is to encode the functions $f: \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ and $g: \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$ via the Grassmann encoding, and then check consistency via the Grassmann test. While this test does satisfy the same notion of non-standard soundness as discussed in [Section 2.1.3](#), we do not know how to implement suitable advice vectors to facilitate the zoom-in coordination. Indeed, the Grassmann encoding via $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$ would require uniformly random advice vectors in $\mathcal{V}(\mathcal{E})$, and specifying a vector

$$x \in \mathcal{V}(\mathcal{E}) = \bigoplus_{j=1}^t \left(\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \right)$$

would require $|E_j|^2$ bits of information for each index j . However, although the advice $\mathcal{A} = (A_1, \dots, A_t)$ available in Ψ_{lazy} does provide quadratic-in- k amount of information for each non-critical index j via

$$A_j = (a^{(j,1)}, \dots, a^{(j,q')}) \in \left(\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \right)^{q'},$$

the advice available for the critical index $c \in [t]$ is

$$A_c = (a^{(1)}, \dots, a^{(q)}) \in \left(\mathbb{F}_2^{E_c} \right)^q,$$

which contains only $O_q(k)$ bits of information. Therefore, it is of interest to have a Grassmann-type structure on $\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$ with only $\exp(O_q(k))$ different zoom-in possibilities.

The low-rank Grassmann encoding: the idea is to consider not all, but only a special type of subspaces in $\text{Gr}(\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}, \ell_1)$. We only allow subspaces that consist of low-rank vectors in $\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$. By the rank-1 decomposition, any vector in $\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$ of rank at most s can be specified by $O(s|E_c|)$ bits of information.

In order to systematically construct linear subspaces consisting of low-rank vectors, we use the Hadamard code (the same idea has appeared in [Gol23]). Given a positive integer ℓ , let $\text{Had}_\ell \in \mathbb{F}_2^{2^\ell \times (2^\ell - 1)}$ be the $\{0, 1\}$ -Hadamard matrix with the first column (the all-0 column) deleted. For any $\mathbb{F}_2$ -vector space V and vectors $x^{(1)}, \dots, x^{(2^\ell - 1)} \in V$, let

$$\text{Lspan}(x^{(1)}, \dots, x^{(2^\ell - 1)}) = \left\{ \sum_{j=1}^{2^\ell - 1} \text{Had}_\ell(i, j) x^{(j)} \mid i \in \{1, 2, \dots, 2^\ell\} \right\}.$$

In words, for each row in Had_ℓ , the set $\text{Lspan}(x^{(1)}, \dots, x^{(2^\ell - 1)})$ contains a vector which is the linear combination of $x^{(1)}, \dots, x^{(2^\ell - 1)}$ with the coefficients given by that row. Because any linear combination of rows in Had_ℓ is a row in Had_ℓ , it follows that $\text{Lspan}(x^{(1)}, \dots, x^{(2^\ell - 1)})$ is always a linear subspace, and if $x^{(1)}, \dots, x^{(2^\ell - 1)}$ are linearly independent then that subspace has dimension exactly ℓ .

The upshot is that if $x^{(1)}, \dots, x^{(2^\ell - 1)} \in \mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$ are rank-1 vectors, then all vectors in the space $\text{Lspan}(x^{(1)}, \dots, x^{(2^\ell - 1)})$ have ranks at most $2^{\ell-1}$. For the sake of reference, we present the following definition of [Gol23]:³

Definition 2.6 ([Gol23, Definition 17]). Suppose V is an $\mathbb{F}_2$ -vector space of dimension at least 2^ℓ . We define $\text{LGr}(V, \ell)$, called *the low-rank Grassmann graph*, to be the subgraph of the Grassmann graph $\text{Gr}(V \otimes V, \ell)$ induced by the vertex set

$$\left\{ \text{Lspan}(u^{(1)} \otimes v^{(1)}, \dots, u^{(2^\ell - 1)} \otimes v^{(2^\ell - 1)}) \mid \begin{array}{l} u^{(1)}, \dots, u^{(2^\ell - 1)} \in V \text{ linearly independent} \\ v^{(1)}, \dots, v^{(2^\ell - 1)} \in V \text{ linearly independent} \end{array} \right\}.$$

Composing with middle PCP: we can now make Ψ_{lazy} into a 4-to-1 game by using the low-rank Grassmann encoding for the critical block $\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$, and using the ordinary Grassmann encoding for the non-critical blocks $\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j}$ where $j \in [t] \setminus \{c\}$. We define Ψ_{final} to be the game where the verifier carries out the following:

1. Sample the critical index $c \in [t]$, and sample $\mathcal{E}, \mathcal{E}', \mathcal{U}, \mathcal{U}'$ as in Ψ_{lazy} .
2. For each $i \in \{1, 2, \dots, 2^{\ell_1+1} - 1\}$, sample

$$x^{(i)} = x^{(i,1)} + \dots + x^{(i,t)} \in \mathcal{V}(\mathcal{E}'),$$

where $x^{(i,c)}$ is a uniformly random rank-1 vector in $\mathbb{F}_2^{E'_c} \otimes \mathbb{F}_2^{E'_c}$, while $x^{(i,j)}$ is a uniformly random vector in $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$ for each $j \in [t] \setminus \{c\}$.

3. Define the linear subspace $L' = \text{Lspan}(x^{(1)}, \dots, x^{(2^{\ell_1+1}-1)}) \subseteq \mathcal{V}(\mathcal{E}')$. If $\dim L' < \ell_1 + 1$, give up on asking questions and accept immediately. Otherwise, let L be a uniformly random subspace of L' with dimension ℓ_1 . We regard $L \subseteq \mathcal{V}(\mathcal{E}')$ as a subspace of $\mathcal{V}(\mathcal{E})$ by appending 0's in the missing coordinates (which only happens in the critical index).

³Definition 2.6 will not be used explicitly in this paper.

4. Send the challenge $(\mathcal{E}, \mathcal{U}, L)$ to Alice and $(\mathcal{E}', \mathcal{U}', L')$ to Bob.
5. Alice must return a linear map $f : \left(L + \bigoplus_{j=1}^t U_j \otimes U_j\right) \rightarrow \mathbb{F}_2$ such that $\text{rank}(f|_{U_j \otimes U_j}) \leq 1$ for each $j \in [t]$. Bob must return a linear map $g : \left(L' + \bigoplus_{j=1}^t U'_j \otimes U'_j\right) \rightarrow \mathbb{F}_2$ such that $\text{rank}(g|_{U'_j \otimes U'_j}) \leq 1$ for each $j \in [t]$.
6. Accept if the restriction of g to $\left(L + \bigoplus_{j=1}^t U_j \otimes U_j\right)$ is identical to f .

The game Ψ_{final} is our final composed PCP (modulo incorporating the side conditions checking satisfiability of the chosen quadratic equations, and the side conditions checking symmetry; this is done by adding the spaces N_{E_j} and N_{sym} as discussed in [Section 2.2.1](#)).

It is easy to see that in Ψ_{final} , for any response of Alice, there are at most 4 possible answers of Bob that can make the verifier accept. This is due to the following facts:

- Since $\dim L' = 1 + \dim L$, any linear function on L has two linear extensions to L' .
- For each $j \in [t] \setminus \{c\}$, we have $U_j = U'_j$. For the critical index c , we have $\dim U'_c = 1 + \dim U_c$, and hence any symmetric bilinear function on $U_c \otimes U_c$ of rank at most 1 has two symmetric bilinear extensions to $U'_c \otimes U'_c$ of rank at most 1.

The completeness of Ψ_{final} is clear by using the Grassmann encoding on the strategies of the provers from Ψ_{lazy} . For soundness, we show that a strategy for Ψ_{final} achieving value at least ε can be used to construct a strategy for Ψ_{lazy} achieving value at least $\Omega_\varepsilon(1)$. This argument is more elaborate, and we only give a high-level overview.

First, we describe a high-level overview where we pretend there was no need for zoom-outs in [Equation \(2.2\)](#). We show that for noticeable fraction of the partial challenges $(\mathcal{E}, \mathcal{U})$ for Alice, the table $L \mapsto F[\mathcal{E}, \mathcal{U}, L]$ passes the standard Grassmann test ([Equation \(2.1\)](#)) over $\mathcal{V}(\mathcal{E})$ with noticeable probability. Applying [Equation \(2.2\)](#), we know that Alice can use the advice $\mathcal{A}$ in Ψ_{lazy} as the zoom-in and thus decodes a global linear function g on $\mathcal{V}(\mathcal{E})$ which has rank at most 1 on $U_j \otimes U_j$ for each j . We argue that for noticeable fraction of the challenges $(\mathcal{E}', \mathcal{U}')$ of Bob (conditioned on $\mathcal{E}, \mathcal{U}, \mathcal{A}$), the restriction $g|_{\mathcal{V}(\mathcal{E}')}$ is a global linear function for Bob that has noticeable agreement with his table $L' \mapsto G[\mathcal{E}', \mathcal{U}', L']$ under the same zoom in (constructed from his advice). Together, this shows that for a fixed successful advice, each one of Alice and Bob only has constantly many global linear functions that have noticeable agreement with their table, and there is at least one pair of choices between them which is consistent. Thus, if each one of them chooses a random such global linear function, they will produce a satisfactory answer to Ψ_{lazy} with constant probability.

The need for zoom-outs in [Equation \(2.2\)](#) complicates matters considerably, as the number of “successful” zoom-outs could be rather large. This issue was already handled in [\[DKK⁺21\]](#), and we will make use of some ideas from there. However, the fact that we use the low-rank Grassmann encoding introduces further difficulties. In [\[DKK⁺21\]](#) it is shown that if Bob’s table has many zoom-outs of codimension w that admit a global linear function with noticeable agreement, then there is also a zoom-out of codimension $w - 1$ that admits a global linear function with noticeable agreement. While this may be possible in our case, it requires extra features from the low-rank Grassmann graph which we do not establish. Instead, we show how to stitch together global linear functions from many different Bob-questions $(\mathcal{E}', \mathcal{U}')$ to a function of Alice, on which we can apply the result of [\[DKK⁺21\]](#) (since Alice’s space has the standard Grassmann graph structure).

3 Preliminaries

In this section we set up basic notations and tools that will be used throughout the paper.

3.1 General Notations

In this subsection we summarize the general notational conventions used throughout the paper. Additional notation will be introduced as needed, typically within dedicated “Notation” environments.

Linear algebra. Given a finite dimensional $\mathbb{F}_2$ -vector space V and a linear subspace $W \subseteq V$, the codimension of W with respect to V is denoted by $\text{codim}_V(W) = \dim V - \dim W$. Given a finite dimensional $\mathbb{F}_2$ -vector space V , we let V^* denote the dual space of V , which consists of all linear functionals $f : V \rightarrow \mathbb{F}_2$. For any finite-dimensional $\mathbb{F}_2$ -vector spaces V_1, V_2 and any bilinear form $f : V_1 \otimes V_2 \rightarrow \mathbb{F}_2$, we define the linear map $T_f : V_1 \rightarrow V_2^*$ by letting $T_f(x)$ be the functional $y \mapsto f(x \otimes y)$.

As indicated in [Sections 2.2.4](#) and [2.2.5](#) of the proof overview, bilinear forms will play an important role in our construction and analysis of 4-to-1 games. More linear algebraic preliminaries about bilinear forms can be found in [Appendix A](#).

Grassmann graph. Given a finite dimensional $\mathbb{F}_2$ -vector space V and a positive integer $\ell \leq \dim V$, the Grassmann graph $\text{Gr}(V, \ell)$ has as vertices all ℓ -dimensional subspaces $L \subseteq V$, and two vertices are adjacent if they intersect in dimension $\ell - 1$. By a slight abuse of notation, we also use $\text{Gr}(V, \ell)$ to denote the vertex set of this graph. We denote by $\mathcal{G}(V, \ell)$ the uniform distribution over the edges of $\text{Gr}(V, \ell)$. For any nonnegative integer $b \leq \ell$ (such that $b \geq 2\ell - \dim V$), we use $\mathcal{G}(V, \ell, b)$ to denote the uniform distribution over the set

$$\{(L_1, L_2) \mid L_1, L_2 \in \text{Gr}(V, \ell) \text{ such that } \dim(L_1 \cap L_2) = b\},$$

i.e. pairs of ℓ -dimensional subspaces of V with an intersection of dimension b .

Probability. For a finite set Λ , we write $\mathbb{E}_{x \in \Lambda}[\cdot]$ and $\mathbb{P}_{x \in \Lambda}[\cdot]$ to denote expectation and probability, respectively, when x is drawn uniformly at random from Λ . If x is sampled according to a specific distribution $\mathcal{D}$ over Λ , we write $x \sim \mathcal{D}$ in place of $x \in \Lambda$ in the subscripts.

Assignment tables. In a 2-prover 1-round game, we often organize a prover’s strategy as an *assignment table* $F[\cdot]$, where for each possible question Q from the verifier, the entry $F[Q]$ takes value from an alphabet of answers. It is often convenient to allow partial assignment tables, where each entry $F[Q]$ is allowed to take a special nullity value outside of the prescribed alphabet. We usually denote such a nullity value by the symbol `nil`. Whenever a `nil` entry is tested for agreement with other entries or objects, we always assume the test rejects (i.e. reports a disagreement). For instance, if L_1 and L_2 are linear subspaces of a vector space V , the entry $F[L_1]$ takes value in $(L_1)^* \cup \{\text{nil}\}$ and $F[L_2]$ takes value in $(L_2)^* \cup \{\text{nil}\}$, then the statement

$$\left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right]$$

evaluates to “false” whenever either of $F[L_1]$ or $F[L_2]$ is `nil`.

Empty sequences. A sequence of objects $a^{(1)}, \dots, a^{(q)}$ is denoted by $(a^{(1)}, \dots, a^{(q)})$. If $q = 0$, the sequence is empty and is denoted by the symbol **empty**.

3.2 Sub-4-to-1 Games

In order to prove the main theorem ([Theorem 1.6](#)), it is convenient to work with a slight relaxation of the 4-to-1 requirement:

Definition 3.1. In the setting and notation of [Definition 1.1](#), a constraint $\Phi_e \subseteq \Sigma_L \times \Sigma_R$ is called a sub- d -to- d' constraint if there is a partition $\Sigma_L = \Sigma_{L,1} \sqcup \dots \sqcup \Sigma_{L,t}$ into sets of size d and a partition $\Sigma_R = \Sigma_{R,1} \sqcup \dots \sqcup \Sigma_{R,t}$ into sets of size d' such that

$$\Phi_e = \bigcup_{i=1}^t \Gamma_{L,i} \times \Gamma_{R,i}, \quad \text{for some subsets } \Gamma_{L,i} \subseteq \Sigma_{L,i} \text{ and } \Gamma_{R,i} \subseteq \Sigma_{R,i}.$$

The notion of sub- d -to- d' constraints motivates the following definition parallel to [Definition 1.3](#).

Definition 3.2. Let d, d' and r be positive integers. An instance Ψ of label-cover is called a sub- d -to- d' game if all of its constraints are sub- d -to- d' . For parameters $0 < s < c \leq 1$, we write $\text{GapS-}d\text{-to-}d'_r(c, s)$ for the restriction of $\text{GapLC}_r(c, s)$ to sub- d -to- d' game instances.

Accordingly, we have the following slight weakening of [Theorem 1.6](#).

Theorem 3.3. *For any $\delta \in (0, 1)$, there exists a positive integer N such that $\text{GapS-4-to-1}_N(1, \delta)$ is NP-hard.*

Although [Theorem 3.3](#) is a relaxation of [Theorem 1.6](#), we will show in [Appendix B](#) that [Theorem 3.3](#) actually implies [Theorem 1.6](#). The main body of this paper ([Sections 4 to 6](#)) will be devoted to proving [Theorem 3.3](#).

3.3 Technical Ingredients from Prior Work

In this subsection, we record the main technical ingredients of this paper that are imported from prior works.

3.3.1 Approximate Coloring of Hypergraphs

As discussed in [Section 2.2.4](#), our construction starts from the hardness of approximating satisfiable $3\text{QS}_{\mathbb{F}_2}$ instances. However, limitations of the tensor tests used in our middle PCP require us to start from an NP-hard gap problem in which the “yes” and “no” cases impose conditions on *different* constraint satisfaction instances. Specifically, the soundness condition in [Theorem 2.4](#) must assert that, even after the alphabet of the $3\text{QS}_{\mathbb{F}_2}$ instance is suitably enlarged (from $\mathbb{F}_2$ to $(\mathbb{F}_2)^r$, roughly speaking), the resulting $3\text{QS}_{(\mathbb{F}_2)^r}$ instance still has small value.⁴

Fortunately, the desired starting point in [Theorem 2.4](#) is essentially implicit in the result of [\[DRS05\]](#) on the hardness of coloring 2-colorable 3-uniform hypergraphs.⁵ Although their result is stated with the no-case condition that the hypergraph H is not c -colorable, a closer inspection of their argument yields the statement below.

⁴This formulation is characteristic of promise constraint satisfaction problems (PCSPs); see, for example, [\[KO22\]](#).

⁵In [Section 4.2](#), we will explain why 2-coloring a 3-uniform hypergraph can be viewed as solving a $3\text{QS}_{\mathbb{F}_2}$ instance.

Theorem 3.4 ([DRS05]). *For every fixed positive integer $c \geq 2$, there exists a constant $\varepsilon \geq \exp(-\exp(O(c^3)))$ such that given a 3-uniform hypergraph H , it is **NP**-hard to distinguish between the following cases:*

- (1) *Yes case: H is 2-colorable.*
- (2) *No case: in every c -coloring of H , at least ε fraction of the edges are monochromatic.*

Since **Theorem 3.4** differs slightly from the result proved in [DRS05], we provide a proof in **Appendix C**. Our proof is a minor adaptation of their argument, which in turn uses the PCP theorem [FGL⁺96, AS98, ALM⁺98] and parallel repetition [Raz98].

3.3.2 Grassmann Agreement Test

The main analytical/combinatorial tool used in this paper is the (non-standard) soundness of the Grassmann agreement test, informally stated in **Equation (2.2)**. Under the notation specified in **Section 3.1**, given a table $F[\cdot]$ that assigns to each ℓ -dimensional subspace $L \subseteq \mathbb{F}_2^n$ either a linear function $F[L]: L \rightarrow \mathbb{F}_2$ or the nullity element **nil**, the passing probability of the Grassmann test is

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right],$$

where the event does not hold if either $F[L_1]$ or $F[L_2]$ are **nil**. The following result is due to [KMS23, EKL23], but we use a slightly different formulation which we derive directly from their results.

Theorem 3.5 ([KMS23, EKL23]). *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right] \geq 2^{-q+5}. \quad (3.1)$$

Then for at least $2^{-q-\ell^2}$ fraction of subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, there exist a subspace $W \in \text{Gr}(\mathbb{F}_2^n, n-q)$ containing Q and a linear map $f: W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \subseteq W \right] \geq 2^{-Cq^2}.$$

A derivation of **Theorem 3.5** from the formulation of [EKL23] will be presented in **Appendix D**.

We also need the following simpler result, which concerns not a table of local linear functions, but a table where every entry takes value from the same abstract alphabet. The following result asserts that if the “Grassmann equality test” passes with noticeable probability, then after zoom-ins and zoom-outs the entries take a certain constant value noticeably often.

Theorem 3.6. *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose Σ is a finite set and $F[\cdot]$ is a table where $F[L] \in \Sigma \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[F[L_1] = F[L_2] \neq \mathbf{nil} \right] \geq 2^{-q+4}. \quad (3.2)$$

Then for at least $2^{-q-\ell^2}$ fraction of subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, there exist an element $\sigma \in \Sigma$ and a subspace $W \in \text{Gr}(\mathbb{F}_2^n, n-q)$ containing Q such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = \sigma \mid Q \subseteq L \subseteq W \right] \geq 2^{-Cq^2}.$$

Proof. Deferred to [Appendix D](#). □

3.3.3 List Decoding Bounds

When we use [Theorem 3.5](#) we will often need to argue that given a zoom-in Q , the number of possible decodings (f, W) is not too large. In this section we precisely define this notion and state the bounds we will use, established by [\[DKK+25\]](#).

Definition 3.7 ([\[DKK+25\]](#)). Let n, ℓ, q, w be nonnegative integers such that $n - w \geq \ell \geq q + 1$. Fix parameters $\tau_0, \tau_1, \dots, \tau_w \in (0, 1)$ and write $\vec{\tau} = (\tau_0, \dots, \tau_w)$. Fix an $\mathbb{F}_2$ -vector space V of dimension n and a subspace $Q \in \text{Gr}(V, q)$. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\text{nil}\}$ for each $L \in \text{Gr}(V, \ell)$. For a linear subspace $W \subseteq V$ with $\text{codim } W \leq w$ and a linear functional $f : W \rightarrow \mathbb{F}_2$, we say that the pair (f, W) is $\vec{\tau}$ -occurring in $F[\cdot]$ modulo Q if $Q \subseteq W$ and

$$\mathbb{P}_{L \in \text{Gr}(W, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \right] \geq \tau_i, \quad \text{where } i = n - \dim W.$$

It is not possible to give a bound on the number of $\vec{\tau}$ -occurring pairs that is independent of n , simply because the number of zoom-outs W can be very large. We have to restrict our attention to pairs (f, W) that “cannot be extended,” as defined below.

Definition 3.8. In the setting and notation of [Definition 3.7](#), we say that (f, W) is $\vec{\tau}$ -maximal in $F[\cdot]$ modulo Q if

- (1) (f, W) is $\vec{\tau}$ -occurring in $F[\cdot]$ modulo Q , but
- (2) for any linear subspace $W' \subseteq V$ that properly contains W and any extended linear functional $f' : W' \rightarrow \mathbb{F}_2$, $f'|_W = f$, the pair (f', W') is not $\vec{\tau}$ -occurring in $F[\cdot]$ modulo Q .

The set of all $\vec{\tau}$ -maximal pairs will be denoted by $\text{LIST}_Q^{\vec{\tau}}(F)$.

We use the following bound on the size of maximal pairs proved by [\[DKK+25\]](#).

Lemma 3.9 ([\[DKK+25\]](#)). *There is an absolute constant $C \geq 40$ such that the following holds. Let n, ℓ, q, w be nonnegative integers such that $n - w \geq 2\ell \geq C(q + 1)$. Suppose $\vec{\tau} = (\tau_0, \dots, \tau_w)$ is a vector such that*

$$\tau_0 \geq 2^{-\ell/C} \quad \text{and} \quad \tau_{i-1} \leq C^{-1} \tau_i^C \text{ for each } i \in [w].$$

Then for any subspace $Q \in \text{Gr}(\mathbb{F}_2^n, q)$ and any table $F[\cdot]$ where $F[L] \in L^ \cup \{\text{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$ we have*

$$|\text{LIST}_Q^{\vec{\tau}}(F)| \leq \exp(C(w + 1)^2 \ell).$$

The original statement of the above lemma in [\[DKK+25\]](#) does not allow for **nil** entries in the table. In [Appendix E](#), we will explain how to adapt their arguments to tables with **nil** entries.

In a part of the analysis of our inner PCP, we are not able to use [Lemma 3.9](#) as a black box, and we will instead draw from the proof of [Lemma 3.9](#). A useful component of the proof by [\[DKK+25\]](#) is the notion of *sunflower* of zoom-outs, defined as follows.

Definition 3.10. Let V be a vector space over $\mathbb{F}_2$, and let $W_1, \dots, W_m \subseteq V$ be subspaces of co-dimension w . We say that $(V, W_1, \dots, W_m)$ forms a sunflower if $\text{codim}_V(W_i \cap W_j) = 2w$ for each pair of distinct indices $i, j \in [m]$.

In words, a sunflower is a collection of subspaces $W_1, \dots, W_m$ living inside a space V that have as small as possible pairwise intersections. The following result from [DKK⁺25] asserts that any sufficiently large collection of zoom-outs of constant codimension contains a large sunflower structure.

Lemma 3.11 ([DKK⁺25, Corollary 3.14]). *Let V be a finite dimensional $\mathbb{F}_2$ -vector space, and let $W_1, \dots, W_N \subseteq V$ be a list of subspaces of codimension w . Let m be a positive integer such that $(m \cdot 2^w)^{w+1} \leq N$. Then, there exists a subspace $W \subseteq V$ containing m of the W_i 's, say, $W_1, \dots, W_m$, such that $(W, W_1, \dots, W_m)$ forms a sunflower.*

3.4 Proof Organization

The proof of Theorem 3.3 spans Sections 4 to 6, during which we construct a sequence of five 2-prover 1-round games; see Figure 4.

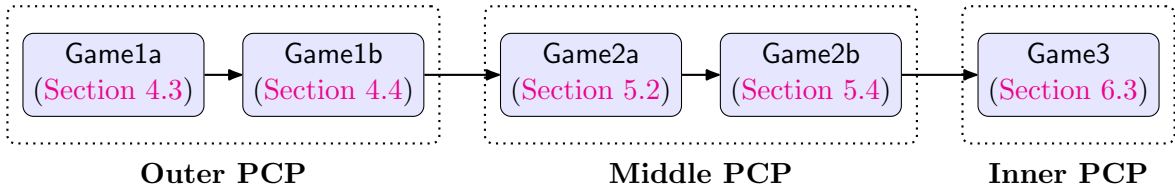


Figure 4: Proof organization

For each version label $xx \in \{1a, 1b, 2a, 2b, 3\}$, we will prove completeness and soundness guarantees of the following form:

- (1) Completeness: if H is 2-colorable, then $\text{val}(\text{Game}_{xx}[H]) = 1$.
- (2) Soundness: if every c -coloring of H makes at least ε fraction of the edges monochromatic, then $\text{val}(\text{Game}_{xx}[H])$ is small.

Completeness is straightforward and can be proved independently for each game, without invoking the completeness of preceding games. Most of the work lies in establishing soundness: for each game after the first, the soundness proof relies on that of its predecessor in the sequence. The final construction $\text{Game}_3[H]$ is a sub-4-to-1 game, whose completeness and soundness yield Theorem 3.3.

3.5 Parameter Relations

During the course of our construction of 4-to-1 games, there will be many parameters on different scales (they are all constant with respect to the size of the starting hardness instance in Theorem 3.4). We summarize the relations between these constants in the following condition.

Condition 3.12. Let $k, q_0, q_1, q_2, t, r, \ell_1, \ell_2, s$ be positive integers, let $\delta, \beta, \varepsilon \in (0, 1)$, and let $\vec{\tau} = (\tau_0, \tau_1, \dots, \tau_{2q_0})$ be a vector such that for a sufficiently large absolute constant $C > 0$, the conditions in Table 1 hold.

Parameter	Requirement	First appears in	Why require this
$\delta \in (0, 1/2)$		inner PCP	
$q_0 \in \mathbb{N}^+$	$q_0 \geq C \log_2(1/\delta)$	inner PCP	inner PCP
$\tau_{2q_0} \in (0, 1)$	$\tau_{2q_0} \leq \exp(-q_0^C)$	inner PCP	inner PCP
$\tau_{2q_0-1}, \dots, \tau_0 \in (0, 1)$	$\tau_{i-1} \leq C^{-1} \tau_i^C, \forall i \in [2q_0]$	inner PCP	inner PCP
$\ell_1 \in \mathbb{N}^+$	$\ell_1 \geq C \log_2(1/\tau_0)$	inner PCP	inner PCP
$s \in \mathbb{N}^+$	$s = 3\ell_1$	inner PCP	inner PCP
$q_1 \in \mathbb{N}^+$	$q_1 = 2s(2^{2\ell_1} - 2^{2\ell_1 - q_0})$	outer PCP	inner PCP
$q_2 \in \mathbb{N}^+$	$q_2 \geq C\ell_1^2$	outer PCP	inner PCP
$\ell_2 \in \mathbb{N}^+$	$\ell_2 \geq Cq_2^2$	middle PCP	middle PCP
$r \in \mathbb{N}^+$	$r = 2q_2 + 1$	outer PCP	middle PCP
$\varepsilon \in (0, 1)$	$\varepsilon \leq \exp(-\exp(\exp(Cr)))$	outer PCP	outer PCP
$k \in \mathbb{N}^+$	$k \geq \varepsilon^{-C} \exp(\exp(\ell_2))$	outer PCP	outer PCP
$\beta \in (0, 1)$	$\beta = k^{-3/4}$	outer PCP	outer PCP
$t \in \mathbb{N}^+$	$t \geq \exp(k^C)$	middle PCP	inner PCP

Table 1: Parameter relations

Condition 3.12 is meant to be a consistent setting of parameters that we can invoke in [Sections 4](#) to [6](#). Whenever the condition is invoked, the absolute constant $C > 0$ can be different from previous invocations. More precisely, a statement of the form

$$\left[\text{Assume **Condition 3.12**. Then [XX] holds.} \right]$$

should be interpreted as

$$\left[\text{There exists an absolute constant } C > 0 \text{ such that the conditions in [Table 1](#) imply [XX].} \right]$$

4 The Outer PCP

In this section, we formally construct and analyze our outer PCP, following the outline in [Section 2.2.4](#). We first introduce the necessary framework in [Sections 4.1](#) and [4.2](#) before turning to the actual construction in [Sections 4.3](#) and [4.4](#).

4.1 Preparation: Tripled Sets

As discussed in [Sections 2.1.1](#) and [2.2.4](#), Alice's challenge in the outer PCP consists of a set E of variables together with an advice sequence. The variables in E are naturally grouped into triples, each consisting of the three distinct variables appearing in an equation of the $3\text{QS}_{\mathbb{F}_2}$ instance. We call such a set E a *tripled set*, formally defined as follows.

Definition 4.1. A *tripled set* is a finite set E equipped with a partition into subsets of size 3. We refer to the parts of this implicit partition as the *triples* of E , and we write $\text{Triples}(E)$ for the collection of its triples.

As discussed in [Sections 2.1.1](#) and [2.2.4](#), our outer PCP construction applies (smooth) parallel repetition to a $3\text{QS}_{\mathbb{F}_2}$ instance. Since the $3\text{QS}_{\mathbb{F}_2}$ instance provided by [Theorem 3.4](#) is represented by a 3-uniform hypergraph H , k -fold parallel repetition yields a 2-prover 1-round game played on the vertex-disjoint union of k copies of H .

Definition 4.2. Let H be a 3-uniform hypergraph with vertex set $\mathcal{V}(H)$ and edge set $\mathcal{E}(H)$. Given a positive integer k , we let $H^{\sqcup k}$ denote the k -fold vertex-disjoint union of H . More explicitly, the vertex set of $H^{\sqcup k}$ is $[k] \times \mathcal{V}(H)$, and we denote $\mathcal{V}(H, k) = [k] \times \mathcal{V}(H)$; the edge set of $H^{\sqcup k}$ is $\bigcup_{i=1}^k \mathcal{E}_i(H, k)$, where

$$\mathcal{E}_i(H, k) = \{ \{ (i, v_1), (i, v_2), (i, v_3) \} \mid \{v_1, v_2, v_3\} \in \mathcal{E}(H) \}.$$

We let $\mathcal{E}(H, k)$ be the collection of all vertex subsets $E \subseteq [k] \times \mathcal{V}(H)$ that result from picking one edge from each $\mathcal{E}_i(H, k)$. That is, it consists of E of the form

$$E = \{v_{i,j} \mid i \in [k], j \in [3]\} \quad \text{such that} \quad \{v_{i,1}, v_{i,2}, v_{i,3}\} \in \mathcal{E}_i(H, k) \text{ for all } i \in [k], \quad (4.1)$$

and we view it naturally as a tripled set, with $\text{Triples}(E) = \{ \{v_{i,1}, v_{i,2}, v_{i,3}\} \mid i \in [k] \}$.

In words, viewing the set of hyperedges in H as the challenges that a verifier samples, the edges in $H^{\sqcup k}$ are naturally viewed as the challenges that the verifier chooses in the k -fold repeated game.

Remark 4.3. For a tripled set E of the form (4.1), the k triples of E are naturally ordered. For each $i \in [k]$, we will call $\{v_{i,1}, v_{i,2}, v_{i,3}\}$ the i -th triple of E .

4.1.1 Thinning, and Thinning with Advice

We next introduce notation to formalize the smoothness in our application of parallel repetition. The following definition captures the structure of the challenges in each coordinate: with probability $1 - \beta$, the two players receive identical challenges; otherwise, Alice receives the full challenge, while Bob receives only a single variable from it.

Definition 4.4. Let E be a tripled set and let $\beta \in [0, 1]$. We write $E' \sim \text{Thin}_\beta(E)$ for the random subset $E' \subseteq E$ obtained as follows. Independently for each triple $T \in \text{Triples}(E)$, we include all elements of T in E' with probability $1 - \beta$, and include a uniformly random element of T in E' with probability β . We stress that the output E' itself is only a set, not a tripled set.

In the outer PCP construction, each prover will receive *two* advice sequences A_{in} and A_{mid} , the latter supplying the Grassmann-type zoom-ins needed in the middle PCP, while the former is reserved for zoom-ins in the inner PCP. The next definition formalizes the process by which the verifier samples the two advice sequences.

Definition 4.5. Let E be a tripled set. Fix nonnegative integers q_1, q_2 and a parameter $\beta \in [0, 1]$. We let $\mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$ denote the output distribution of the following process:

1. Sample a β -thinning $E' \sim \text{Thin}_\beta(E)$.
2. Sample $q = q_1 + q_2$ vectors $a^{(1)}, \dots, a^{(q)} \in \mathbb{F}_2^{E'}$ independently and uniformly at random. We denote $A_{\text{in}} = (a^{(1)}, \dots, a^{(q_1)})$ and $A_{\text{mid}} = (a^{(q_1+1)}, \dots, a^{(q_1+q_2)})$.

3. Output the tuple $(E', A_{\text{in}}, A_{\text{mid}})$.

Remark 4.6. For a subset E' of a finite set E , we always view $\mathbb{F}_2^{E'}$ as a linear subspace of the ambient space $\mathbb{F}_2^E$. In particular, the vectors $a^{(1)}, \dots, a^{(q)}$ in [Definition 4.5](#) are viewed also as elements of the vector space $\mathbb{F}_2^E$.

In the outer PCP, Alice will see a tripled set E and the two advice sequences A_{in} and A_{mid} , but not the β -thinning E' which is only sent to Bob. The next proposition states that, even conditioned on A_{in} and A_{mid} , the distribution of E' is still nicely structured. In particular, it is independent over the triples of E .

Proposition 4.7. Let E be a tripled set. Fix nonnegative integers q_1, q_2 and a parameter $\beta \in [0, 1)$. Fix arbitrary tuples

$$A_1 \in (\mathbb{F}_2^E)^{q_1} \quad \text{and} \quad A_2 \in (\mathbb{F}_2^E)^{q_2}.$$

Sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$. Then the resulting marginal distribution of E' is independent over triples of E . Furthermore, each triple of E is entirely included in E' with conditional probability at least $1 - 4^{q_1+q_2}\beta$.

Proof. Deferred to [Appendix F.1](#). □

As emphasized throughout the proof overview, “covering properties” are crucial in our construction of 4-to-1 games, and they will appear many times (in different forms) throughout [Sections 4](#) to [6](#). They are important primarily for Grassmann encodings, and a job of our outer PCP construction is to prepare a strong enough “covering property” for the Grassmann-based tensor tests in the middle PCP to work. On the most basic level, we need that the distribution of vectors sampled uniformly from $\mathbb{F}_2^{E'}$ (where E' is a random β -thinning), once lifted to $\mathbb{F}_2^E$ as discussed in [Remark 4.6](#), is close to uniform over $\mathbb{F}_2^E$. The next proposition (essentially from [\[DKK⁺25\]](#)) proves that this is the case if $\beta = o(|E|^{-1/2})$.

Proposition 4.8. Let E be a tripled set. Fix nonnegative integers q_1, q_2 and a parameter $\beta \in [0, 4^{-q_1-q_2})$. Fix an arbitrary tuple $A_1 \in (\mathbb{F}_2^E)^{q_1}$. Sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\}$. Then the resulting marginal distribution of A_{mid} has total variation distance at most $4^{q_1+q_2}\beta\sqrt{|E|/3}$ to the uniform distribution over $(\mathbb{F}_2^E)^{q_2}$.

Proof. Deferred to [Appendix F.1](#). □

We remark that although we include [Proposition 4.8](#) here in [Section 4](#), it will not be used until [Section 5](#).

4.2 Preparation: The NAE Predicate

The reason that 2-colorability of a 3-uniform hypergraph can be viewed as a system of quadratic equations is that the ternary not-all-equal predicate on a Boolean alphabet is a “quadratic” constraint:

Definition 4.9. We define a function $\text{NAE}_3 : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2$ defined by

$$\text{NAE}_3(x_1, x_2, x_3) = x_1 + x_2 + x_3 + x_1x_2 + x_2x_3 + x_3x_1.$$

We note that $\text{NAE}_3(x_1, x_2, x_3) = 1$ if and only if x_1, x_2, x_3 are not all equal.

As discussed in [Section 2.2.4](#), we will use the notion of “joint NAE-satisfaction”, which we formalize below. Here we assume that an assignment to the variables in E is presented as a linear functional $f : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$.

Definition 4.10. Let E be a tripled set and let r be a positive integer. Given r linear functionals $f^{(1)}, \dots, f^{(r)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$, let $a^{(1)}, \dots, a^{(r)} \in \mathbb{F}_2^E$ be the unique vectors such that

$$f^{(i)}(x) = \sum_{v \in E} a_v^{(i)} x_v \quad \text{for all } i \in [r] \text{ and } x \in \mathbb{F}_2^E.$$

If we have

$$\sum_{i=1}^r \text{NAE}_3(a_{v_1}^{(i)}, a_{v_2}^{(i)}, a_{v_3}^{(i)}) = 1 \quad \text{for all } \{v_1, v_2, v_3\} \in \text{Triples}(E),$$

then the linear functionals $f^{(1)}, \dots, f^{(r)}$ are said to be *jointly NAE-satisfying*. In the case $r = 1$, then the functional $f^{(1)}$ is simply said to be *NAE-satisfying*.

We can now translate the “2-colorability” of a 3-uniform hypergraph H into the language of NAE-satisfaction. For the sake of future reference, the following proposition is stated for the k -fold disjoint union $H^{\sqcup k}$.

Proposition 4.11. Suppose H is a 2-colorable 3-uniform hypergraph and k is a positive integer. Then there exists a linear functional $f : \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$ such that for any $E \in \mathcal{E}(H, k)$, the restriction $f|_{\mathbb{F}_2^E}$ is NAE-satisfying.

Proof. Since H is 2-colorable, so is the k -fold vertex-disjoint union $H^{\sqcup k}$. Let $\varphi : \mathcal{V}(H, k) \rightarrow \mathbb{F}_2$ be a proper 2-coloring of $H^{\sqcup k}$. Let $f : \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$ be the linear functional defined by

$$f(x) = \sum_{v \in \mathcal{V}(H,k)} \varphi(v) x_v \quad \text{for all } x \in \mathbb{F}_2^{\mathcal{V}(H,k)}.$$

For any $E \in \mathcal{E}(H, k)$ and any $\{v_1, v_2, v_3\} \in \text{Triples}(E)$, since $\{v_1, v_2, v_3\}$ is an edge of $H^{\sqcup k}$, by definition we know that $\varphi(v_1), \varphi(v_2), \varphi(v_3)$ are not all equal. Therefore, it follows from [Definition 4.10](#) that $f|_{\mathbb{F}_2^E}$ is NAE-satisfying. $\square$

4.2.1 Linear Functionals vs. Bilinear Forms

In later stages of the outer PCP construction, an assignment to variables in E will be presented as a symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$. The NAE-satisfaction notion generalizes to bilinear maps as follows.

Definition 4.12. Let E be a tripled set. Given a symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$, let $X \in \mathbb{F}_2^{E \times E}$ be the unique matrix such that

$$f(x \otimes y) = \sum_{u, v \in E} X_{uv} x_u y_v \quad \text{for all } x, y \in \mathbb{F}_2^E.$$

If we have

$$X_{v_1 v_1} + X_{v_2 v_2} + X_{v_3 v_3} + X_{v_1 v_2} + X_{v_2 v_3} + X_{v_3 v_1} = 1 \quad \text{for all } \{v_1, v_2, v_3\} \in \text{Triples}(E),$$

then the bilinear map f is said to be NAE-satisfying.

In [Section 4.4](#), we will need to decode from a low-rank symmetric bilinear map a collection of linear functionals. This process is essentially the standard “rank-1 decomposition” in linear algebra, which we formalize below.

Definition 4.13. Let V be a finite-dimensional $\mathbb{F}_2$ -vector space and let r be a positive integer. Given a symmetric bilinear map $f : V \otimes V \rightarrow \mathbb{F}_2$ and r linear functionals $f^{(1)}, \dots, f^{(r)} : V \rightarrow \mathbb{F}_2$, we say that $(f^{(1)}, \dots, f^{(r)})$ is a *tensor decomposition* of f if the following conditions hold:

- (1) For each $i \in [r]$, we have $f^{(i)} \in \text{image}(T_f)$. In other words, there exists a vector $x^{(i)} \in V$ such that $f^{(i)}(y) = f(x^{(i)} \otimes y)$ for each $y \in V$.
- (2) For each $x, y \in V$, we have

$$f(x \otimes y) = \sum_{i=1}^r f^{(i)}(x) f^{(i)}(y). \quad (4.2)$$

The following two propositions show that the NAE-satisfaction of symmetric bilinear maps is interchangeable with the joint-NAE-satisfaction of its tensor decompositions.

Proposition 4.14. Let E be a tripled set and let r be a positive integer. Suppose $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ is an NAE-satisfying symmetric bilinear map. Then any tensor decomposition $(f^{(1)}, \dots, f^{(r)})$ of f is jointly NAE-satisfying.

Proof. Let $a^{(1)}, \dots, a^{(r)} \in \mathbb{F}_2^E$ be the unique vectors such that

$$f^{(i)}(x) = \sum_{v \in E} a_v^{(i)} x_v \quad \text{for all } i \in [r] \text{ and } x \in \mathbb{F}_2^E.$$

Let $X \in \mathbb{F}_2^{E \times E}$ be the matrix defined by

$$X_{uv} = \sum_{i=1}^r a_u^{(i)} a_v^{(i)} \quad \text{for all } u, v \in E.$$

Plugging the expansion of $f^{(i)}$ into (4.2) and changing the order of summation, we get that

$$f(x \otimes y) = \sum_{u, v \in E} X_{uv} x_u y_v \quad \text{for all } x, y \in \mathbb{F}_2^E.$$

Since f is NAE-satisfying, for each triple $\{v_1, v_2, v_3\} \in \text{Triples}(E)$ we must have

$$X_{v_1 v_1} + X_{v_2 v_2} + X_{v_3 v_3} + X_{v_1 v_2} + X_{v_2 v_3} + X_{v_3 v_1} = 1,$$

and hence

$$\sum_{i=1}^r \left(a_{v_1}^{(i)} a_{v_1}^{(i)} + a_{v_2}^{(i)} a_{v_2}^{(i)} + a_{v_3}^{(i)} a_{v_3}^{(i)} + a_{v_1}^{(i)} a_{v_2}^{(i)} + a_{v_2}^{(i)} a_{v_3}^{(i)} + a_{v_3}^{(i)} a_{v_1}^{(i)} \right) = 1.$$

By [Definition 4.9](#) we thus have

$$\sum_{i=1}^r \text{NAE}_3(a_{v_1}^{(i)}, a_{v_2}^{(i)}, a_{v_3}^{(i)}) = 1 \quad \text{for all } \{v_1, v_2, v_3\} \in \text{Triples}(E),$$

and thus $f^{(1)}, \dots, f^{(r)}$ are jointly NAE-satisfying. $\square$

Proposition 4.15. Let E be a tripled set and let r be a positive integer. Suppose $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ is a symmetric bilinear map and $f^{(1)}, \dots, f^{(r)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ are jointly NAE-satisfying linear functionals. If (4.2) holds for all $x, y \in \mathbb{F}_2^E$, then f is NAE-satisfying.

Proof. The proof follows the same lines as in Proposition 4.14, and we omit the details. $\square$

The following straightforward corollary of Proposition 4.15 will be used in Lemma 5.19.

Corollary 4.16. Let E be a nonempty tripled set. There exists an NAE-satisfying symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ of rank 1.

Proof. There clearly exists a nonzero linear functional $f^{(1)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ that is NAE-satisfying (by itself). We can then let $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ be the rank-1 bilinear map defined by $f(x \otimes y) = f^{(1)}(x)f^{(1)}(y)$ for all $x, y \in \mathbb{F}_2^E$, and apply Proposition 4.15 to show that f is NAE-satisfying. $\square$

Combining Propositions 4.11 and 4.15 yields the following “bilinear” version of Proposition 4.11.

Corollary 4.17. Suppose H is a 2-colorable 3-uniform hypergraph and k is a positive integer. Then there exists a rank-1 symmetric bilinear form $f : \mathbb{F}_2^{\mathcal{V}(H,k)} \otimes \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$ such that for any $E \in \mathcal{E}(H, k)$, the restriction $f|_{\mathbb{F}_2^E \otimes \mathbb{F}_2^E}$ is NAE-satisfying.

Proof. By Proposition 4.11, there is a (nonzero) linear functional $f^{(1)} : \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$ such that $f^{(1)}|_{\mathbb{F}_2^E}$ is NAE-satisfying for every $E \in \mathcal{E}(H, k)$. We can then let

$$f : \mathbb{F}_2^{\mathcal{V}(H,k)} \otimes \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$$

be the rank-1 symmetric bilinear map defined by $f(x \otimes y) = f^{(1)}(x)f^{(1)}(y)$ for all $x, y \in \mathbb{F}_2^{\mathcal{V}(H,k)}$, and apply Proposition 4.15 to show that $f|_{\mathbb{F}_2^E \otimes \mathbb{F}_2^E}$ is NAE-satisfying for each $E \in \mathcal{E}(H, k)$. $\square$

4.3 The Equation vs. Variable Game

We are now ready to start the construction of our outer PCP. The first version of our outer PCP is defined as follows (cf. Section 2.1.1).

Definition 4.18. Given positive integers k, r , nonnegative integers q_1, q_2 , a parameter $\beta \in [0, 1]$ and a 3-uniform hypergraph H , let $\text{Game1a}[H, k, q_1, q_2, r, \beta]$ be the 2-prover 1-round game where the verifier executes the following:

1. Sample a uniformly random tripled set $E \in \mathcal{E}(H, k)$.
2. Sample $(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$. Send $(E, A_{\text{in}}, A_{\text{mid}})$ to Alice⁶ and $(E', A_{\text{in}}, A_{\text{mid}})$ to Bob.
3. Alice must return r linear functionals $f^{(1)}, \dots, f^{(r)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ that are jointly NAE-satisfying; Bob must return r linear functionals $g^{(1)}, \dots, g^{(r)} : \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$. Accept if

$$f^{(i)}|_{\mathbb{F}_2^{E'}} = g^{(i)} \quad \text{for all } i \in [r].$$

⁶In Alice’s view, A_{in} and A_{mid} are sequences of vectors in $\mathbb{F}_2^E$, instead of in $\mathbb{F}_2^{E'}$; it is important that Alice does not get to see E' .

Remark 4.19. We remark that the game $\text{Game1a}[H, k, q_1, q_2, r, \beta]$ can be viewed as the k -fold parallel repetition of $\text{Game1a}[H, 1, q_1, q_2, r, \beta]$, and the game $\text{Game1a}[H, 1, 0, 0, r, 1]$ is the equation-vs.-variable game corresponding to the result of [Theorem 3.4](#).

We now analyze the completeness and the soundness of Game1a .

Lemma 4.20 (Game1a completeness). *For any positive integer k , nonnegative integers q_1, q_2 , parameter $\beta \in [0, 1]$ and 2-colorable 3-uniform hypergraph H , we have*

$$\text{val}\left(\text{Game1a}[H, k, q_1, q_2, 1, \beta]\right) = 1.$$

Proof. We obtain from [Proposition 4.11](#) a linear functional $f : \mathbb{F}_2^{\mathcal{Y}(H, k)} \rightarrow \mathbb{F}_2$, whose restriction on $\mathbb{F}_2^E$ is NAE-satisfying for any $E \in \mathcal{E}(H, k)$. We can then construct a strategy for Alice in the game $\text{Game1a}[H, k, q_1, q_2, 1, \beta]$, as follows:

1. Receive the question $(E, A_{\text{in}}, A_{\text{mid}})$.
2. Return the functional $f|_{\mathbb{F}_2^E}$, which is guaranteed by [Proposition 4.11](#) to be NAE-satisfying.

Similarly, the strategy for Bob is:

1. Receive the question $(E', A_{\text{in}}, A_{\text{mid}})$.
2. Return the functional $f|_{\mathbb{F}_2^{E'}}$.

It is clear that Bob's answer is always consistent with Alice's answer. Therefore, if Alice and Bob operate under such strategies, the verifier in the game $\text{Game1a}[H, k, q_1, q_2, 1, \beta]$ accepts with probability 1. $\square$

To show soundness of $\text{Game1a}[H, k, q_1, q_2, r, \beta]$, we start by analyzing the soundness of the basic game $\text{Game1a}[H, 1, 0, 0, r, 1]$, which is effectively the standard equation-versus-variable game with “superpositions.”

Lemma 4.21. *Fix a positive integer r and a parameter $\varepsilon \in (0, 1)$. Suppose H is a 3-uniform hypergraph such that in every 2^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}\left(\text{Game1a}[H, 1, 0, 0, r, 1]\right) \leq 1 - \frac{\varepsilon}{3}.$$

Proof. Let V be the vertex set of $H^{\sqcup 1}$ (which is isomorphic to H).

We fix an arbitrary strategy for Alice and Bob in the game $\text{Game1a}[H, 1, 0, 0, r, 1]$, and we will prove that the verifier rejects with probability at least $\varepsilon/3$. Since there are no advice vectors in this game, the question for Alice is simply a random edge of $H^{\sqcup 1}$; and as the smoothness parameter is set to 1, the question for Bob will be a single vertex.

Our goal is to define a 2^r -coloring map $\varphi : V \rightarrow \mathbb{F}_2^r$. For each vertex $v \in V$, the strategy for Bob must assign an answer to the question $\{v\}$, and the answer must be r linear functionals

$$g_v^{(1)}, \dots, g_v^{(r)} : \mathbb{F}_2^{\{v\}} \rightarrow \mathbb{F}_2.$$

Aggregating Bob's answers for all $v \in V$ yields r linear functionals

$$g^{(1)}, \dots, g^{(r)} : \mathbb{F}_2^V \rightarrow \mathbb{F}_2.$$

We can then let $\varphi : V \rightarrow \mathbb{F}_2^r$ be the unique assignment map such that

$$\left(g^{(1)}(x), g^{(2)}(x), \dots, g^{(r)}(x)\right) = \sum_{v \in V} \varphi(v) x_v \quad \text{for all } x \in \mathbb{F}_2^V. \quad (4.3)$$

By the assumption of the lemma, for at least ε fraction of the edges $\{v_1, v_2, v_3\} \in \mathcal{E}(H, 1)$, we have $\varphi(v_1) = \varphi(v_2) = \varphi(v_3)$. Fix such an edge $E = \{v_1, v_2, v_3\}$, and let $f^{(1)}, \dots, f^{(r)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ be Alice's answer to the question E . By [Definition 4.18](#), $f^{(1)}, \dots, f^{(r)}$ must be jointly NAE-satisfying. However, $\varphi(v_1) = \varphi(v_2) = \varphi(v_3)$ implies (via [Definition 4.10](#) and [Equation \(4.3\)](#)) that

$$g^{(1)}|_{\mathbb{F}_2^E}, g^{(2)}|_{\mathbb{F}_2^E}, \dots, g^{(r)}|_{\mathbb{F}_2^E}$$

are not jointly NAE-satisfying. Therefore, there exists a vertex $v \in \{v_1, v_2, v_3\}$ with

$$\left(f^{(1)}|_{\mathbb{F}_2^{\{v\}}}, f^{(2)}|_{\mathbb{F}_2^{\{v\}}}, \dots, f^{(r)}|_{\mathbb{F}_2^{\{v\}}}\right) \neq \left(g_v^{(1)}, g_v^{(2)}, \dots, g_v^{(r)}\right). \quad (4.4)$$

Conditioned on the event that Alice receives the question E , with probability $1/3$ the question for Bob is $\{v\}$, in which case their answers are not consistent due to (4.4). Since this is true for at least ε -fraction of the edges $E \in \mathcal{E}(H, 1)$, the verifier must reject with probability at least $\varepsilon/3$. $\square$

Next, we incorporate the advice as well as constantly many repetitions, and show that the value does not increase by too much:

Lemma 4.22. *Fix positive integers k, r , nonnegative integers q_1, q_2 and parameters $\beta, \varepsilon \in (0, 1)$ such that $k \geq 2^{q_1+q_2}\beta^{-1}$. Suppose H is a 3-uniform hypergraph such that in every 2^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}\left(\text{Game1a}[H, k, q_1, q_2, r, \beta]\right) \leq 1 - \frac{\varepsilon}{6}.$$

Proof. We write $q = q_1 + q_2$. As in [Remark 4.19](#), we view $\text{Game1a}[H, k, q_1, q_2, r, \beta]$ as the k -fold parallel repetition of the game $\text{Game1a}[H, 1, q_1, q_2, r, \beta]$. Let $(E, A_{\text{in}}, A_{\text{mid}})$ and $(E', A_{\text{in}}, A_{\text{mid}})$ be the questions for Alice and Bob in the k -fold repetition game, respectively. We write

$$A_{\text{in}} = (a^{(1)}, \dots, a^{(q_1)}) \quad \text{and} \quad A_{\text{mid}} = (a^{(q_1+1)}, \dots, a^{(q_1+q_2)}).$$

We say a triple $\{v_1, v_2, v_3\} \in \text{Triples}(E)$ is “critical” if we have

$$a_{v_1}^{(i)} = a_{v_2}^{(i)} = a_{v_3}^{(i)} = 0 \text{ for all } i \in [q] \quad \text{and} \quad |E' \cap \{v_1, v_2, v_3\}| = 1.$$

Let $I \subseteq [k]$ be the collection of indices $i \in [k]$ such that the i -th triple of E is critical (see [Remark 4.3](#)). Conditioned on the event that $I \neq \emptyset$, we pick a uniformly random $i \in I$ and note that the i -th “coordinate” of the parallel repetition is a copy of the equation vs. variable game $\text{Game1a}[H, 1, 0, 0, r, 1]$ and is independent of the remaining coordinates. Therefore, [Lemma 4.21](#) implies that conditioned on $\{I \neq \emptyset\}$, the verifier rejects with probability at least $\varepsilon/3$. Since

$$\mathbb{P}[I \neq \emptyset] = 1 - (1 - 2^{-q}\beta)^k \geq 1 - 2^{-k \cdot 2^{-q}\beta} \geq 1 - 2^{-1} = \frac{1}{2},$$

we conclude that in the k -fold repetition game $\text{Game1a}[H, k, q_1, q_2, r, \beta]$, the verifier rejects with probability at least $\frac{1}{2} \cdot \varepsilon/3 = \varepsilon/6$. $\square$

Finally, we apply the parallel repetition theorem for projection games by [Rao11] to get the soundness of **Game1a**.

Lemma 4.23 (Game1a soundness). *Assume [Condition 3.12](#). Suppose H is a 3-uniform hypergraph such that in every 4^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have⁷*

$$\text{val}\left(\text{Game1a}[H, k, q_1, q_2, 2r, \beta]\right) \leq \exp(-k^{1/5}).$$

Proof. Let $k_0 = \lceil 2^{q_1+q_2} \beta^{-1} \rceil$. By [Lemma 4.22](#) we know that

$$\text{val}\left(\text{Game1a}[H, k_0, q_1, q_2, 2r, \beta]\right) \leq 1 - \frac{\varepsilon}{6}.$$

Since $\text{Game1a}[H, k_0, q_1, q_2, 2r, \beta]$ is a projection game, we may apply [Rao11, Theorem 1.4] to conclude that its $\lfloor k/k_0 \rfloor$ -fold parallel repetition has value at most $\exp(-c\varepsilon^2 \lfloor k/k_0 \rfloor)$, for some absolute constant $c \in (0, 1)$. It is then easy to see (via [Remark 4.19](#)) that

$$\text{val}\left(\text{Game1a}[H, k, q_1, q_2, 2r, \beta]\right) \leq \exp(-c\varepsilon^2 \lfloor k/k_0 \rfloor) \leq \exp(-k^{1/5}),$$

where in the last transition we use the relation $k/k_0 \gg \varepsilon^{-2} k^{1/5}$ guaranteed by [Condition 3.12](#). $\square$

4.4 From Joint Satisfaction to Bilinear Forms

As hinted in [Section 2.2.4](#) and [Section 4.2.1](#), the last goal in the outer PCP stage is to change the format of the provers' responses to symmetric bilinear forms. More precisely, we will consider the following 2-prover 1-round game defined below. It is identical to $\text{Game1a}[H, k, q_1, q_2, r, \beta]$, except that the provers are expected to provide a single bilinear form of low-rank (instead of r linear forms).

Definition 4.24. Given positive integers k, r , nonnegative integers q_1, q_2 , a parameter $\beta \in [0, 1)$ and a 3-uniform hypergraph H , let $\text{Game1b}[H, k, q_1, q_2, r, \beta]$ be the 2-prover-1-round game where the verifier executes the following:

1. Sample a uniformly random tripled set $E \in \mathcal{E}(H, k)$.
2. Sample $(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$. Send $(E, A_{\text{in}}, A_{\text{mid}})$ to Alice and $(E', A_{\text{in}}, A_{\text{mid}})$ to Bob.
3. Alice must return a symmetric bilinear form $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ that is NAE-satisfying and has rank at most r ; Bob must return a bilinear form $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$. Accept if

$$f|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = g.$$

We now analyze the completeness and the soundness of **Game1b**.

Lemma 4.25 (Game1b completeness). *For any positive integer k , nonnegative integers q_1, q_2 , parameter $\beta \in [0, 1)$ and 2-colorable 3-uniform hypergraph H , we have*

$$\text{val}\left(\text{Game1b}[H, k, q_1, q_2, 1, \beta]\right) = 1.$$

⁷We have $2r$ instead of r as the rank parameter here, in order to prepare for applying [Lemma 4.27](#) later.

Proof. We obtain from [Corollary 4.17](#) a rank-1 symmetric bilinear map $f : \mathbb{F}_2^{\mathcal{V}(H,k)} \otimes \mathbb{F}_2^{\mathcal{V}(H,k)} \rightarrow \mathbb{F}_2$, whose restriction on $\mathbb{F}_2^E \otimes \mathbb{F}_2^E$ is NAE-satisfying for every $E \in \mathcal{E}(H,k)$. We can then construct a strategy for Alice in the game $\text{Game1b}[H, k, q_1, q_2, 1, \beta]$, as follows:

1. Receive the question $(E, A_{\text{in}}, A_{\text{mid}})$.
2. Return the symmetric bilinear map $f|_{\mathbb{F}_2^E \otimes \mathbb{F}_2^E}$, which is guaranteed by [Corollary 4.17](#) to be NAE-satisfying. Furthermore, it must have rank at most 1 because $\text{rank}(f) = 1$.

Similarly, the strategy for Bob is:

1. Receive the question $(E', A_{\text{in}}, A_{\text{mid}})$.
2. Return the symmetric bilinear map $f|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}}$.

It is clear that under this set of strategies, the verifier accepts with probability 1. $\square$

Remark 4.26. In $\text{Game1b}[H, k, q_1, q_2, 1, \beta]$, although Bob's answer $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$ to a question $(E', A_{\text{in}}, A_{\text{mid}})$ is not required to be symmetric or of rank at most 1 (we only pose such requirements on Alice's answer), we note that under the strategy in the completeness proof ([Lemma 4.25](#)), Bob's answers are indeed always symmetric and have rank at most 1. This feature will propagate to the subsequent constructions Game2a , Game2b , and their completeness proofs. Eventually, this observation will be used in the completeness proof of Game3 ([Lemma 6.32](#)).

We now move on to the soundness. The following lemma establishes a connection between the soundness of Game1a and Game1b , and more precisely it shows how to derive a strategy for the former from a strategy for the latter. Intuitively, this comes from the fact that a rank r bilinear form has at most $O_r(1)$ many decompositions into rank-1 bilinear forms, but some care is needed (specifically, the event that the rank of Alice's bilinear form drops in Bob's space is problematic, but thankfully it has low probability).

Lemma 4.27. *For any positive integers k, r , nonnegative integers q_1, q_2 , parameter $\beta \in [0, 4^{-q_1 - q_2})$ and 3-uniform hypergraph H , we have*

$$\text{val} \left(\text{Game1a}[H, k, q_1, q_2, 2r, \beta] \right) \geq 4^{-r^2} \left(\text{val} \left(\text{Game1b}[H, k, q_1, q_2, r, \beta] \right) - 4^{q_1 + q_2} r \beta \right).$$

Proof. We organize the proof into the following three steps.

Step 1: controlling rank drop. We denote

$$s = \text{val} \left(\text{Game1b}[H, k, q_1, q_2, r, \beta] \right).$$

Let $F[\cdot]$ and $G[\cdot]$ be the strategies of Alice and Bob, respectively, under which the verifier accepts with probability s in $\text{Game1b}[H, k, q_1, q_2, r, \beta]$. For each $E \in \mathcal{E}(H, k)$ and $(E', A_{\text{in}}, A_{\text{mid}})$ in the support of $\mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$, we have bilinear maps

$$F[E, A_{\text{in}}, A_{\text{mid}}] : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2 \quad \text{and} \quad G[E', A_{\text{in}}, A_{\text{mid}}] : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2.$$

A pair of questions $(E, A_{\text{in}}, A_{\text{mid}})$ and $(E', A_{\text{in}}, A_{\text{mid}})$ for Alice and Bob is said to be “good” if

$$F[E, A_{\text{in}}, A_{\text{mid}}]|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = G[E', A_{\text{in}}, A_{\text{mid}}];$$

it is said to be “excellent” if in addition to being good, it also satisfies

$$\text{rank}(F[E, A_{\text{in}}, A_{\text{mid}}]) = \text{rank}(G[E', A_{\text{in}}, A_{\text{mid}}]).$$

By definition, a random pair of questions is “good” with probability s . Furthermore, conditioned on each fixed Alice question $(E, A_{\text{in}}, A_{\text{mid}})$, since $\text{rank}(F[E, A_{\text{in}}, A_{\text{mid}}]) \leq r$, we know from [Corollary A.3](#) and [Proposition 4.7](#) that

$$\begin{aligned} \mathbb{P}_{E'} \left[\text{rank} \left(F[E, A_{\text{in}}, A_{\text{mid}}] \Big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \right) = \text{rank} \left(F[E, A_{\text{in}}, A_{\text{mid}}] \right) \Big| E, A_{\text{in}}, A_{\text{mid}} \right] &\geq (1 - 4^{q_1+q_2}\beta)^r \\ &\geq 1 - 4^{q_1+q_2}r\beta. \end{aligned}$$

Therefore, the probability that a random pair of questions is “good” but not “excellent” is at most $4^{q_1+q_2}r\beta$. Consequently, a random pair of questions is “excellent” with probability at least $s - 4^{q_1+q_2}r\beta$.

Step 2: deriving a strategy for Game1a. Note that in $\text{Game1a}[H, k, q_1, q_2, 2r, \beta]$ the joint distribution of questions to Alice and Bob is the same as in $\text{Game1b}[H, k, q_1, q_2, r, \beta]$. We next derive strategies for the provers in the former game from the tables $F[\cdot]$ and $G[\cdot]$. The strategy for Alice is as follows:

1. Receive the question $(E, A_{\text{in}}, A_{\text{mid}})$, and let $f = F[E, A_{\text{in}}, A_{\text{mid}}]$. Note that $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ is symmetric and NAE-satisfying.
2. Use [Lemma A.4](#) to obtain a tensor decomposition $(f^{(1)}, \dots, f^{(2r)})$ of f .
3. Return the linear functionals $f^{(1)}, \dots, f^{(2r)} : \mathbb{F}_2^E \rightarrow \mathbb{F}_2$. They must be jointly NAE-satisfying, due to [Proposition 4.14](#).

Accordingly, the strategy for Bob is:

1. Receive the question $(E', A_{\text{in}}, A_{\text{mid}})$, and let $g = G[E', A_{\text{in}}, A_{\text{mid}}]$.
2. For each $i \in [2r]$, select a linear functional $g^{(i)}$ from the subspace $\text{image}(T_g) \subseteq (\mathbb{F}_2^{E'})^*$ independently and uniformly at random.
3. Return the linear functionals $g^{(1)}, \dots, g^{(2r)} : \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$.

Step 3: analysis of the strategy. We show that the above strategy answers every “excellent” pair of questions consistently with probability at least 4^{-r^2} , thereby concluding the desired inequality

$$\text{val} \left(\text{Game1a}[H, k, q_1, q_2, 2r, \beta] \right) \geq 4^{-r^2} (s - 4^{q_1+q_2}r\beta).$$

Suppose $(E, A_{\text{in}}, A_{\text{mid}})$ and $(E', A_{\text{in}}, A_{\text{mid}})$ are an “excellent” pair of questions for Alice and Bob, and let

$$f = F[E, A_{\text{in}}, A_{\text{mid}}] \quad \text{and} \quad g = G[E', A_{\text{in}}, A_{\text{mid}}].$$

Let $(f^{(1)}, \dots, f^{(2r)})$ be an arbitrary tensor decomposition of f . By [Definition 4.13](#), we know that $f^{(i)} \in \text{image}(T_f)$ for each $i \in [2r]$. Furthermore, since $\text{rank}(f) = \text{rank}(g)$ (due to the excellence condition), it follows from [Corollary A.2](#) that

$$f^{(i)} \Big|_{\mathbb{F}_2^{E'}} \in \text{image}(T_g) \quad \text{for all } i \in [2r].$$

Since the cardinality of $\text{image}(T_g)$ is at most $2^{\text{rank}(g)} \leq 2^r$, if $g^{(1)}, \dots, g^{(2r)}$ are independently and uniformly sampled from $\text{image}(T_g)$, we have

$$\mathbb{P} \left[f^{(i)} \Big|_{\mathbb{F}_2^{E'}} = g^{(i)} \text{ for all } i \in [2r] \right] \geq (2^{-r})^{2r} = 4^{-r^2},$$

as desired. $\square$

Using [Lemma 4.27](#), we can now prove the soundness of **Game1b**.

Lemma 4.28 (Game1b soundness). *Assume [Condition 3.12](#). Suppose H is a 3-uniform hypergraph such that in every 4^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}(\text{Game1b}[H, k, q_1, q_2, r, \beta]) \leq k^{-1/2}.$$

Proof. Combining [Lemmas 4.23](#) and [4.27](#), we have

$$\text{val}(\text{Game1b}[H, k, q_1, q_2, r, \beta]) \leq 4^{q_1+q_2} r \beta + 4^{r^2} \exp(-k^{1/5}) \leq k^{-1/2},$$

where the last transition is due to [Condition 3.12](#). $\square$

5 The Middle PCP

In this section we construct and analyze our middle PCP as discussed in [Section 2.2.5](#). [Sections 5.1](#) to [5.3](#) are devoted to the design and analysis of **Game2a**, where we incorporate local tensor checks. We then perform a lazy parallel repetition to get **Game2b** in [Section 5.4](#).

5.1 Preparation: Thinning with Subspaces

In the middle PCP, we will use a Grassmann-type structure to perform “local tensor checks.” Along with a question $(E, A_{\text{in}}, A_{\text{mid}})$ sent to Alice (as in the outer PCP), the verifier also sends a subspace $U \subseteq \mathbb{F}_2^E$ and checks whether the restriction of Alice’s answer $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ to $U \otimes U$ has rank at most 1. The following augmentation of [Definition 4.5](#) captures the process by which the verifier samples the tensor-check subspace U .

Definition 5.1. Let E be a tripled set. Fix a parameter $\beta \in [0, 1]$ and nonnegative integers q_1, q_2, ℓ such that $\ell \geq q_2$. We let $\mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$ denote the output distribution of the following process:

1. Sample $(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$.
2. Sample $\ell - q_2$ vectors $a^{(1)}, \dots, a^{(\ell-q_2)} \in \mathbb{F}_2^{E'}$ independently and uniformly at random. Let $A' = (a^{(1)}, \dots, a^{(\ell-q_2)})$, and obtain a subspace $U = \text{span}(A_{\text{mid}}) + \text{span}(A') \subseteq \mathbb{F}_2^{E'}$.
3. Output the tuple $(E', A_{\text{in}}, A_{\text{mid}}, U)$.

Remark 5.2. Similarly to [Remark 4.6](#), the subspace $U \subseteq \mathbb{F}_2^{E'}$ in [Definition 5.1](#) is viewed also as a subspace of $\mathbb{F}_2^E$.

Remark 5.3. Consider a sample $(E', A_{\text{in}}, A_{\text{mid}}, U) \sim \mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$ as defined in [Definition 5.1](#). We note that the distribution of (E', A_{in}, U) does not depend on q_2 . This is because after fixing E' and A_{in} , the advice sequence A_{mid} is uniformly random over $(\mathbb{F}_2^{E'})^{q_2}$.

The next proposition (which can be derived from [Proposition 4.8](#)) is the crucial “covering property” we need in the middle PCP: a random subspace of $\mathbb{F}_2^{E'}$ (where E' is a random β -thinning of E) lifted to $\mathbb{F}_2^E$ is close to a random subspace of $\mathbb{F}_2^E$ (even with conditioning on an advice).

Proposition 5.4. Let E be a tripled set. Fix a parameter $\beta \in [0, 1)$ and nonnegative integers q_1, q_2, ℓ such that $|E| \geq \ell \geq q_2$. Fix arbitrary tuples

$$A_1 \in (\mathbb{F}_2^E)^{q_1} \quad \text{and} \quad A_2 \in (\mathbb{F}_2^E)^{q_2} \text{ such that } \dim \text{span}(A_2) = q_2.$$

Sample

$$(E', A_{\text{in}}, A_{\text{mid}}, U) \sim \mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$$

conditioned on the event $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$. Then the resulting marginal distribution of U has total variation distance at most

$$4^{q_1+\ell} \beta \sqrt{|E|/3} + 2^{\ell-|E|}$$

to the uniform distribution over the set $\{U \in \text{Gr}(\mathbb{F}_2^E, \ell) \mid \text{span}(A_2) \subseteq U\}$.

Proof. Deferred to [Appendix F.2](#). □

We also need the following simpler smoothness property of $\mathcal{J}_{\text{mid}}$ (derived from [Proposition 4.7](#)).

Proposition 5.5. Let E be a tripled set. Fix a parameter $\beta \in [0, 1)$ and nonnegative integers q_1, ℓ . Fix an arbitrary tuple $A \in (\mathbb{F}_2^E)^{q_1}$ and an arbitrary subspace $U_0 \in \text{Gr}(\mathbb{F}_2^E, \ell)$. Sample

$$(E', A_{\text{in}}, \text{empty}, U) \sim \mathcal{J}_{\text{mid}}(E, q_1, 0, \beta, \ell)$$

conditioned on the event $\{A_{\text{in}} = A\} \cap \{U = U_0\}$. Then for any subset $S \subseteq E$ with $|S| \leq 2$, the probability that $S \subseteq E'$ is at least $1 - 4^{q_1+\ell+1} \beta$.

Proof. According to [Definition 5.1](#), when $(E', A_{\text{in}}, A_{\text{mid}}, U)$ is sampled from $\mathcal{J}_{\text{mid}}(E, q_1, 0, \beta, \ell)$, a vector sequence $A' \in (\mathbb{F}_2^{E'})^\ell$ is generated, and then U is taken to be $\text{span}(A')$. Let

$$\mathcal{B} = \left\{ (a^{(1)}, \dots, a^{(\ell)}) \in (\mathbb{F}_2^E)^\ell \mid \text{span}(a^{(1)}, \dots, a^{(\ell)}) = U_0 \right\}$$

be the collection of bases of U_0 . The event $\{U = U_0\}$ is thus equal to the disjoint union of events $\bigcup_{B \in \mathcal{B}} \{A' = B\}$. It suffices to prove that for each $B \in \mathcal{B}$, conditioned on the event $\{A_{\text{in}} = A\} \cap \{A' = B\}$, we have $\mathbb{P}[S \subseteq E'] \geq 1 - 4^{q_1+\ell+1} \beta$ for any two-element subset $S \subseteq E$. It is easy to see that the distribution of E' conditioned on $\{A_{\text{in}} = A\} \cap \{A' = B\}$ is the same as in the following process (by comparing [Definitions 4.5](#) and [5.1](#)):

- sample $(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, \ell, \beta)$ conditioned on $\{A_{\text{in}} = A\} \cap \{A_{\text{mid}} = B\}$.

The desired conclusion thus easily follows from [Proposition 4.7](#). □

The following notation will be used later in [Section 6.4.2](#). Here the subscript “rev” stands for “reverse,” meaning that we reversely generate a thinning E' after seeing a subspace U contained in $\mathbb{F}_2^{E'}$.

Definition 5.6. Let E be a tripled set. Fix a parameter $\beta \in [0, 1)$ and a nonnegative integer ℓ . Given any subspace $U_0 \subseteq \mathbb{F}_2^E$ with dimension at most ℓ , we let $\mathcal{J}_{\text{rev}}(E, U_0, \beta, \ell)$ be the output distribution of the following process:

1. Sample $(E', \text{empty}, \text{empty}, U) \sim \mathcal{J}_{\text{mid}}(E, 0, 0, \beta, \ell)$ conditioned on the event $\{U = U_0\}$.
2. Output E' .

5.2 The Local Tensor Check Game

We now construct the first version of our middle PCP. The 2-prover 1-round game constructed in the next definition is similar to **Game1b** but with one important distinction. Letting f be Alice's response, instead of requiring $\text{rank}(f)$ is small, we require that $\text{rank}(f|_{U \otimes U})$ is small, where U is (roughly) a random ℓ -dimensional subspace in Alice's space $\mathbb{F}_2^E$ which is given to Alice as part of her challenge. Additionally, as part of his challenge, we give Bob a random subspace U' of dimension (roughly) $\ell + 1$ that contains U .

Definition 5.7. Given positive integers k, ℓ_2 , nonnegative integers q_1, q_2 such that $\ell_2 \geq q_2$, a parameter $\beta \in [0, 1)$ and a 3-uniform hypergraph H , let $\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]$ be the 2-Prover-1-Round game where the verifier executes the following:

1. Sample a uniformly random tripled set $E \in \mathcal{E}(H, k)$.
2. Sample $(E', A_{\text{in}}, A_{\text{mid}}, U) \sim \mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell_2)$. Sample a random vector $x \in \mathbb{F}_2^{E'}$ and let $U' = U + \text{span}(x)$.
3. Send (E, A_{in}, U) to Alice and (E', A_{in}, U') to Bob.
4. Alice must return an NAE-satisfying symmetric bilinear form $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ such that $\text{rank}(f|_{U \otimes U}) \leq 1$; Bob must return a bilinear form $g : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2$. Accept if

$$f|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = g.$$

Remark 5.8. In **Definition 5.7**, the verifier does not use A_{mid} after generating it. Therefore, the distribution of $(E, A_{\text{in}}, U, U')$ does not depend on q_2 . Consequently, the value of the game $\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]$ does not depend on q_2 either. The purpose of A_{mid} in **Definition 5.7** is solely for the convenience of its soundness analysis in **Section 5.3**.

Remark 5.9. In **Definition 5.7**, it is easy to see that the distribution of $(E', A_{\text{in}}, A_{\text{mid}}, U')$ is identical to $\mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell_2 + 1)$.

The completeness of **Game2a** is straightforward and is given in the following lemma.

Lemma 5.10 (Game2a completeness). *For any positive integers k, ℓ_2 , nonnegative integers q_1, q_2 such that $k \geq \ell_2 \geq q_2$, parameter $\beta \in [0, 1)$ and 2-colorable 3-uniform hypergraph H , we have*

$$\text{val}(\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]) = 1.$$

Proof. It is clear that the provers can ignore the subspaces U or U' given to them and pretend that they are in the game **Game1b** $[H, k, q_1, 0, 1, \beta]$. Since there is a strategy for **Game1b** $[H, k, q_1, 0, 1, \beta]$ with 0 rejection probability due to **Lemma 4.25**, it follows that the same strategy also passes **Game2a** $[H, k, \ell_2, q_1, q_2, \beta]$ with probability 1. $\square$

The soundness analysis of **Game2a**, presented in the next subsection, is much more involved. Intuitively, if we did not supply Bob with the space U' , the analysis would be relatively straightforward. Indeed, in that case, while in principle Alice's response could depend on the space U she receives, in actuality such strategies do not achieve a high value, as they have to be consistent with Bob (whose response does not depend on U at all). Thus, in that case Alice's response can be thought of as not being dependent on U , and hence the tensor test on U is random and faithfully checks whether Alice's response has low-rank globally.

To make our final game 4-to-1 we must supply Bob with the space U' (otherwise we would not be able to compose with the inner PCP), and the soundness analysis in that case becomes more complicated. Indeed, there are genuine cheating strategies that Alice and Bob can use, and our argument below analyzes them (using the soundness of the Grassmann test) and shows that they can still be converted into good strategies for **Game1b**.

5.3 Soundness Analysis

In this subsection, we fix a 3-uniform hypergraph H , positive integers k, ℓ_2 , nonnegative integers q_1, q_2 and a parameter $\beta \in (0, 1)$. We consider the game **Game2a** $[H, k, \ell_2, q_1, q_2, \beta]$ as defined in **Definition 5.7**. The following notational convention will be used throughout **Section 5.3** (but *not* in later parts of the paper).

Notation 5.11. We use $\mathcal{D}_{\text{mid}}$ to denote the joint distribution of $(E, A_{\text{in}}, A_{\text{mid}}, U, E', U')$ in the game **Game2a** $[H, k, \ell_2, q_1, q_2, \beta]$, where (E, A_{in}, U) is the question sent to Alice and (E', A_{in}, U') is the question sent to Bob. We use the symbol $*$ to denote marginalization over the corresponding component. For instance, sampling from the marginal distribution of (A_{in}, U, E') under $\mathcal{D}_{\text{mid}}$ is denoted by $(*, A_{\text{in}}, *, U, E', *) \sim \mathcal{D}_{\text{mid}}$.

Notation 5.12. We will often condition the distribution $\mathcal{D}_{\text{mid}}$ on some subset of the six components $(E, A_{\text{in}}, A_{\text{mid}}, U, E', U')$ and consider the induced joint distribution of the remaining components. For instance, if E and U' are fixed, then the conditional joint distribution of (U, E') is denoted by

$$_{(E, *, *, U, E', U') \sim \mathcal{D}_{\text{mid}}} \mathbb{P} \left[\cdot \mid E, U' \right].$$

Notation 5.13. A table $F[\cdot]$ is called an Alice-table if for each possible Alice-question (E, A_{in}, U) under $\mathcal{D}_{\text{mid}}$, the entry $F[E, A_{\text{in}}, U]$ is either **nil** or an NAE-satisfying symmetric bilinear form

$$F[E, A_{\text{in}}, U] : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2 \quad \text{such that} \quad \text{rank} \left(F[E, A_{\text{in}}, U]_{|U \otimes U} \right) \leq 1.$$

Similarly, a table $G[\cdot]$ is called a Bob-table if for each possible Bob-question (E', A_{in}, U') under $\mathcal{D}_{\text{mid}}$, the entry $G[E', A_{\text{in}}, U']$ is either **nil** or a bilinear form

$$G[E', A_{\text{in}}, U'] : \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'} \rightarrow \mathbb{F}_2.$$

In the following notation, the function $\text{Vrf}_{F,G}(\cdot, \cdot, \cdot, \cdot, \cdot, \cdot)$ is the indicator of whether the verifier accepts under the strategy given by $F[\cdot]$ and $G[\cdot]$. Since A_{mid} is irrelevant to the verifier's acceptance, the $\text{Vrf}_{F,G}(\cdot, \cdot, \cdot, \cdot, \cdot, \cdot)$ only has five arguments instead of six.

Notation 5.14. Fix an Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$. For any tuple $(E, A_{\text{in}}, *, U, E', U')$ with nonzero probability under $\mathcal{D}_{\text{mid}}$, we define

$$\text{Vrf}_{F,G}(E, A_{\text{in}}, U, E', U') = \begin{cases} 1, & \text{if } F[E, A_{\text{in}}, U]_{|\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = G[E', A_{\text{in}}, U'], \\ 0, & \text{otherwise.} \end{cases}$$

We will often sample $(E, A_{\text{in}}, *, U, E', U')$ from $\mathcal{D}_{\text{mid}}$ conditioned on some subset of its components. For instance, if E and U' are fixed, then we denote the corresponding conditional expectation of $\text{Vrf}_{F,G}(E, A_{\text{in}}, U, E', U')$ by

$$\text{Vrf}_{F,G}(E, *, *, *, U') = _{(E, A_{\text{in}}, *, U, E', U') \sim \mathcal{D}_{\text{mid}}} \mathbb{P} \left[F[E, A_{\text{in}}, U]_{|\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = G[E', A_{\text{in}}, U'] \mid E, U' \right].$$

When none of the components is fixed, we write $\text{Vrf}_{F,G} = \text{Vrf}_{F,G}(*, *, *, *, *)$ for short.

5.3.1 Preparing for Grassmann Decoding

The core of the soundness analysis of **Game2a** is to use the Grassmann decoding theorem (**Theorem 3.6**). In order to make use of that theorem, we first need to convert the agreement between Alice's and Bob's tables into the condition that Alice's table *alone* passes the “Grassmann equality test” (see **Equation (3.2)**) with noticeable probability. This is achieved by the following lemma.

Lemma 5.15. *Assume **Condition 3.12**. Let $F[\cdot]$ be an Alice-table and $G[\cdot]$ be a Bob-table. For any $E \in \mathcal{E}(H, k)$ and any $A_{\text{in}} \in (\mathbb{F}_2^E)^{q_1}$, we have*

$$\mathbb{P}_{(U_1, U_2) \sim \mathcal{G}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] \geq \text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *)^2 - 2^{-\ell_2}.$$

Proof. We organize the proof into the following three steps:

Step 1: fixing E' and U' . Fix a subset $E' \subseteq E$ with size $|E'| \geq \ell_2 + 1$ and a subspace $U' \in \text{Gr}(\mathbb{F}_2^{E'}, \ell_2 + 1)$ such that the tuple $(E, A_{\text{in}}, *, *, E', U')$ has nonzero probability under $\mathcal{D}_{\text{mid}}$. By **Definitions 5.1** and **5.7**, it is easy to see that sampling $(E, A_{\text{in}}, *, U, E', U') \sim \mathcal{D}_{\text{mid}}$ conditioned on E, A_{in}, E' and U' is equivalent to sampling a uniformly random subspace $U \in \text{Gr}(U', \ell_2)$. Therefore, we have

$$\begin{aligned} \text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 &= \mathbb{E}_{(E, A_{\text{in}}, *, U, E', U') \sim \mathcal{D}_{\text{mid}}} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, U, E', U') \mid E, A_{\text{in}}, E', U' \right]^2 \\ &= \mathbb{E}_{U_1, U_2 \in \text{Gr}(U', \ell_2)} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, U_1, E', U') \text{Vrf}_{F,G}(E, A_{\text{in}}, U_2, E', U') \right]. \end{aligned} \quad (5.1)$$

Expanding the right-hand side of **Equation (5.1)** by definition, we get

$$\begin{aligned} &\text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 \\ &= \mathbb{P}_{U_1, U_2 \in \text{Gr}(U', \ell_2)} \left[F[E, A_{\text{in}}, U_1] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = G[E', A_{\text{in}}, U'] = F[E, A_{\text{in}}, U_2] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \right] \\ &\leq \mathbb{P}_{U_1, U_2 \in \text{Gr}(U', \ell_2)} \left[F[E, A_{\text{in}}, U_1] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = F[E, A_{\text{in}}, U_2] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \right]. \end{aligned} \quad (5.2)$$

Step 2: fixing only U' . For any fixed $U' \in \text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)$ and $U_1, U_2 \in \text{Gr}(U', \ell_2)$ such that $F[E, A_{\text{in}}, U_1] \neq F[E, A_{\text{in}}, U_2]$, one of the following two possibilities holds:

- (1) At least one of $F[E, A_{\text{in}}, U_1]$ and $F[E, A_{\text{in}}, U_2]$ is **nil**.
- (2) Both of $F[E, A_{\text{in}}, U_1]$ and $F[E, A_{\text{in}}, U_2]$ are bilinear forms $\mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$, and their difference $f = F[E, A_{\text{in}}, U_1] - F[E, A_{\text{in}}, U_2]$ is nonzero. In this case, there exist two unit vectors $x, y \in \mathbb{F}_2^E$ (i.e. $|\text{supp}(x)| = |\text{supp}(y)| = 1$) such that $f(x \otimes y) = 1$. Therefore, for any subset $E' \subseteq E$ that contains $\text{supp}(x) \cup \text{supp}(y)$, we have $F[E, A_{\text{in}}, U_1] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \neq F[E, A_{\text{in}}, U_2] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}}$.

In either of the above two cases, it follows from **Proposition 5.5** and **Remark 5.9** that (note that U', U_1 and U_2 remain fixed in the following inequality)

$$\mathbb{P}_{(E, A_{\text{in}}, *, *, E', U') \sim \mathcal{D}_{\text{mid}}} \left[F[E, A_{\text{in}}, U_1] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = F[E, A_{\text{in}}, U_2] \big|_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \mid E, A_{\text{in}}, U' \right] \leq 4^{q_1 + \ell_2 + 2} \beta.$$

Therefore, taking expectation of Equation (5.2) over the conditional distribution of E' yields (note that U_1 and U_2 are no longer fixed in the following inequality)

$$\begin{aligned} & \mathbb{E}_{(E, A_{\text{in}}, *, *, E', U') \sim \mathcal{D}_{\text{mid}}} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 \mid E, A_{\text{in}}, U' \right] \\ & \leq \mathbb{P}_{U_1, U_2 \in \text{Gr}(U', \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] + 4^{q_1 + \ell_2 + 2} \beta. \end{aligned} \quad (5.3)$$

Step 3: both E' and U' unfixed. By Proposition 5.4 and Remark 5.9, we know that conditioned on the fixed E and A_{in} , the distribution of U' in the sample $(E, A_{\text{in}}, *, *, *, U') \sim \mathcal{D}_{\text{mid}}$ is $(4^{q_1 + \ell_2 + 1} \beta \sqrt{k} + 2^{\ell_2 + 1 - 3k})$ -close to uniform over $\text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)$. Therefore, we have

$$\begin{aligned} & \text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *)^2 \\ &= \mathbb{E}_{(E, A_{\text{in}}, *, *, E', U') \sim \mathcal{D}_{\text{mid}}} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 \mid E, A_{\text{in}} \right]^2 \quad (\text{by definition}) \\ &\leq \mathbb{E}_{(E, A_{\text{in}}, *, *, E', U') \sim \mathcal{D}_{\text{mid}}} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 \mid E, A_{\text{in}} \right] \quad (\text{by Cauchy-Schwarz}) \\ &\leq \mathbb{E}_{U' \in \text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)} \left[\mathbb{E}_{(E, A_{\text{in}}, *, *, E', U') \sim \mathcal{D}_{\text{mid}}} \left[\text{Vrf}_{F,G}(E, A_{\text{in}}, *, E', U')^2 \mid E, A_{\text{in}}, U' \right] \right] + \\ & \quad 4^{q_1 + \ell_2 + 1} \beta \sqrt{k} + 2^{\ell_2 + 1 - 3k}. \end{aligned}$$

We then apply Equation (5.3) to the above and get

$$\begin{aligned} \text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *)^2 &\leq \mathbb{E}_{U' \in \text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)} \left[\mathbb{P}_{U_1, U_2 \in \text{Gr}(U', \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] \right] + \\ & \quad 4^{q_1 + \ell_2 + 1} \beta \left(4 + \sqrt{k} \right) + 2^{\ell_2 + 1 - 3k}. \end{aligned} \quad (5.4)$$

For any fixed $U' \in \text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)$, two independent samples $U_1, U_2 \in \text{Gr}(U', \ell_2)$ are equal to each other with probability $(2^{\ell_2 + 1} - 1)^{-1}$. Furthermore, if $U' \in \text{Gr}(\mathbb{F}_2^E, \ell_2 + 1)$ is sampled uniformly at random and $U_1, U_2 \in \text{Gr}(U', \ell_2)$ are sampled uniformly conditioned on $U_1 \neq U_2$, the distribution of (U_1, U_2) is uniform over the edges of the Grassmann graph $\text{Gr}(\mathbb{F}_2^E, \ell_2)$. Therefore, Equation (5.4) implies

$$\begin{aligned} \text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *)^2 &\leq \mathbb{P}_{(U_1, U_2) \sim \mathcal{G}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] + \frac{1}{2^{\ell_2 + 1} - 1} \\ & \quad + 4^{q_1 + \ell_2 + 1} \beta \left(4 + \sqrt{k} \right) + 2^{\ell_2 + 1 - 3k} \\ &\leq \mathbb{P}_{(U_1, U_2) \sim \mathcal{G}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] + 2^{-\ell_2}, \end{aligned}$$

where we used Condition 3.12 in the last transition. $\square$

5.3.2 Invoking the Grassmann Decoding Theorem

We are now ready to apply the Grassmann decoding theorem to Alice's table. The advice A_{mid} , which played no real role in the definition of Game2a, helps us state the following lemma.

Lemma 5.16. Assume Condition 3.12. Let $F[\cdot]$ be an Alice-table and $G[\cdot]$ be a Bob-table. For any $E \in \mathcal{E}(H, k)$ and any $A_{\text{in}} \in (\mathbb{F}_2^E)^{q_1}$ such that $\text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *) \geq 2^{-q_2/3}$, the following holds:

with probability at least $4^{-\ell_2^2}$ over $(E, A_{\text{in}}, A, *, *, *) \sim \mathcal{D}_{\text{mid}}$ conditioned on E and A_{in} , there exists an NAE-satisfying symmetric bilinear map $f_A : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ of rank at most $2q_2 + 1$ satisfying

$$\mathbb{P}_{(E, A_{\text{in}}, A, U, *, *) \sim \mathcal{D}_{\text{mid}}} \left[F[E, A_{\text{in}}, U] = f_A \mid E, A_{\text{in}}, A \right] \geq 2^{-\ell_2^2}.$$

Proof. We organize the proof into the following three steps.

Step 1: Grassmann decoding. Since $\text{Vrf}_{F,G}(E, A_{\text{in}}, *, *, *) \geq 2^{-q_2/3}$, [Lemma 5.15](#) implies

$$\mathbb{P}_{(U_1, U_2) \sim \mathcal{G}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U_1] = F[E, A_{\text{in}}, U_2] \neq \text{nil} \right] \geq 2^{-2q_2/3} - 2^{-\ell_2} \geq 2^{-q_2+4},$$

where we used [Condition 3.12](#) in the last transition. Applying [Theorem 3.6](#) to the table $F[E, A_{\text{in}}, \cdot]$ yields⁸ a collection of subspaces $\mathcal{Q} \subseteq \text{Gr}(\mathbb{F}_2^E, q_2)$ such that:

- (1) $|\mathcal{Q}| \geq 2^{-q_2 - \ell_2^2} |\text{Gr}(\mathbb{F}_2^E, q_2)|$;
- (2) for each $Q \in \mathcal{Q}$, there exists a subspace $W_Q \in \text{Gr}(\mathbb{F}_2^E, 3k - q_2)$ and an NAE-satisfying symmetric bilinear map $h_Q : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ satisfying

$$\mathbb{P}_{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U] = h_Q \mid Q \subseteq U \subseteq W_Q \right] \geq 2^{-Cq_2^2}, \quad (5.5)$$

where C is an absolute constant. For any $U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)$ such that $F[E, A_{\text{in}}, U] = h_Q$, by definition (see [Notation 5.13](#)) we must have $\text{rank}(h_Q|_{U \otimes U}) \leq 1$. It thus follows from [Equation \(5.5\)](#) that

$$\mathbb{P}_{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)} \left[\text{rank}(h_Q|_{U \otimes U}) \leq 1 \mid Q \subseteq U \subseteq W_Q \right] \geq 2^{-Cq_2^2} > 2^{4 - (\ell_2 - q_2)/2},$$

where we used [Condition 3.12](#) in the last transition. By [Lemma A.5](#), we must have $\text{rank}(h_Q) \leq 2q_2 + 1$.

For each $Q \in \mathcal{Q}$, since W_Q has codimension q_2 with respect to $\mathbb{F}_2^E$, we have

$$\mathbb{P}_{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)} \left[U \subseteq W_Q \mid Q \subseteq U \right] = \frac{\binom{3k - 2q_2}{\ell_2 - q_2}_2}{\binom{3k - q_2}{\ell_2 - q_2}_2} \geq 2^{-\ell_2(q_2 + 1)}. \quad (5.6)$$

Combining [Equation \(5.5\)](#) and [Equation \(5.6\)](#) yields

$$\mathbb{P}_{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U] = h_Q \mid Q \subseteq U \right] \geq 2^{-Cq_2^2 - \ell_2(q_2 + 1)} \geq 2^{1 - \ell_2^2}, \quad (5.7)$$

where we used [Condition 3.12](#) in the last transition.

⁸We apply [Theorem 3.6](#) with Σ equal to the collection of NAE-satisfying symmetric bilinear maps from $\mathbb{F}_2^E \otimes \mathbb{F}_2^E$ to $\mathbb{F}_2$.

Step 2: good Q translates to good A . Now for any $A \in (\mathbb{F}_2^E)^{q_2}$, we let

$$f_A = \begin{cases} h_{\text{span}(A)}, & \text{if } \dim \text{span}(A) = q_2 \text{ and } \text{span}(A) \in \mathcal{Q}, \\ 0, & \text{otherwise.} \end{cases}$$

If $\dim \text{span}(A) = q_2$ and $\text{span}(A) \in \mathcal{Q}$, then by [Equation \(5.7\)](#) we have

$$\mathbb{P}_{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2)} \left[F[E, A_{\text{in}}, U] = f_A \mid \text{span}(A) \subseteq U \right] \geq 2^{1-\ell_2^2}. \quad (5.8)$$

By [Proposition 5.4](#), we know that conditioned on the fixed E , A_{in} and $A_{\text{mid}} = A$, the distribution of U in the sample $(E, A_{\text{in}}, A, U, *, *) \sim \mathcal{D}_{\text{mid}}$ is $(4^{q_1+q_2+\ell_2}\beta\sqrt{k} + 2^{\ell_2-3k})$ -close to uniform over the set $\{U \in \text{Gr}(\mathbb{F}_2^E, \ell_2) \mid \text{span}(A) \subseteq U\}$. Therefore, [Equation \(5.8\)](#) implies

$$\mathbb{P}_{(E, A_{\text{in}}, A, U, *, *) \sim \mathcal{D}_{\text{mid}}} \left[F[E, A_{\text{in}}, U] = f_A \mid E, A_{\text{in}}, A \right] \geq 2^{1-\ell_2^2} - 4^{q_1+q_2+\ell_2}\beta\sqrt{k} - 2^{\ell_2-3k} \geq 2^{-\ell_2^2},$$

where we used [Condition 3.12](#) in the last transition.

Step 3: abundance of good A 's. It remains to show that

$$\mathbb{P}_{(E, A_{\text{in}}, A, *, *, *) \sim \mathcal{D}_{\text{mid}}} \left[\dim \text{span}(A) = q_2 \text{ and } \text{span}(A) \in \mathcal{Q} \mid E, A_{\text{in}} \right] \geq 4^{-\ell_2^2}.$$

By [Proposition 4.8](#), it suffices to show

$$\mathbb{P}_{A \in (\mathbb{F}_2^E)^{q_2}} \left[\dim \text{span}(A) = q_2 \text{ and } \text{span}(A) \in \mathcal{Q} \right] \geq 4^{-\ell_2^2} + 4^{q_1+q_2}\beta\sqrt{k}.$$

But the left-hand side of the above display is clearly equal to

$$\mathbb{P}_{A \in (\mathbb{F}_2^E)^{q_2}} \left[\dim \text{span}(A) = q_2 \right] \cdot \frac{|\mathcal{Q}|}{|\text{Gr}(\mathbb{F}_2^E, q_2)|} \geq \frac{1}{4} \cdot 2^{-q_2-\ell_2^2} \geq 4^{-\ell_2^2} + 4^{q_1+q_2}\beta\sqrt{k},$$

where we used [Condition 3.12](#) in the last transition. □

5.3.3 Deriving Strategy for the Outer PCP

We now use the structural results regarding Alice's strategy to complete the soundness analysis of **Game2a**. Before we do so, fixing an Alice-table and a Bob-table, we prune the Alice-table and only keep the responses on questions which have noticeable success probability. This will ensure that whatever functions we decode from Alice's table have noticeable consistency with Bob's table.

Definition 5.17. Let $\eta \in (0, 1)$ be a threshold parameter. Given an Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$ for **Game2a** $[H, k, \ell_2, q_1, q_2, \beta]$, consider the Alice-table $F'[\cdot]$ defined by

$$F'[E, A_{\text{in}}, U] = \begin{cases} F[E, A_{\text{in}}, U], & \text{if } \text{Vrf}_{F,G}(E, A_{\text{in}}, U, *, *) \geq \eta, \\ \text{nil}, & \text{otherwise.} \end{cases}$$

The pair of tables (F', G) is called the η -pruning of (F, G) .

The following straightforward proposition shows that η -pruning drops the success probability of Alice and Bob by at most η .

Proposition 5.18. Let $\eta \in (0, 1)$ be a threshold parameter. Given an Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$ for $\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]$, let (F', G) be the η -pruning of (F, G) . Then

$$\text{Vrf}_{F', G} \geq \text{Vrf}_{F, G} - \eta.$$

Proof. For any $E \in \mathcal{E}(H, k)$, any $A_{\text{in}} \in (\mathbb{F}_2^E)^{q_1}$ and any subspace $U \subseteq \mathbb{F}_2^E$ with $\dim U \leq \ell_2$, from [Definition 5.17](#) it is easy to see that

$$\text{Vrf}_{F', G}(E, A_{\text{in}}, U, *, *) \geq \text{Vrf}_{F, G}(E, A_{\text{in}}, U, *, *) - \eta.$$

Taking expectation over $(E, A_{\text{in}}, *, U, *, *) \sim \mathcal{D}_{\text{mid}}$ then yields the desired conclusion. $\square$

We are now ready to state and prove the soundness of **Game2a**.

Lemma 5.19 (Game2a soundness). *Assume [Condition 3.12](#). Suppose that in every 4^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}\left(\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]\right) \leq 2^{-q_2/4}.$$

Proof. Assume on the contrary that the value of $\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]$ is larger than $2^{-q_2/4}$. Then by definition, there are an Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$ for $\text{Game2a}[H, k, \ell_2, q_1, q_2, \beta]$ such that $\text{Vrf}_{F, G} > 2^{-q_2/4}$. Let (F', G) be the $(2^{1-q_2/3})$ -pruning of (F, G) . By [Proposition 5.18](#) we have

$$\text{Vrf}_{F', G} \geq 2^{-q_2/4} - 2^{1-q_2/3} \geq 2^{1-q_2/3},$$

where we used $q_2 \geq 24$ (as guaranteed by [Condition 3.12](#)).

Step 1: strategy for Game1b. For each $E \in \mathcal{E}(H, k)$ and each possible sample $(E', A_{\text{in}}, A_{\text{mid}})$ from $\mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$, let $\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$ be the collection of all NAE-satisfying symmetric bilinear maps $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ such that $\text{rank}(f) \leq 2q_2 + 1$ and

$$\mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, U, *, *) \sim \mathcal{D}_{\text{mid}}} \left[F'[E, A_{\text{in}}, U] = f \mid E, A_{\text{in}}, A_{\text{mid}} \right] \geq 2^{-\ell_2^2}.$$

We now derive strategies for the provers in **Game1b** $[H, k, q_1, q_2, r, \beta]$ from the tables $F'[\cdot]$ and $G[\cdot]$. The strategy for Alice is as follows:

1. Receive the question $(E, A_{\text{in}}, A_{\text{mid}})$.
2. If $\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$ is empty, return an arbitrary NAE-satisfying symmetric bilinear map $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ of rank 1 (see [Corollary 4.16](#)).
3. If $\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$ is nonempty, return an arbitrary NAE-satisfying symmetric bilinear map $f \in \mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$. By the definition of $\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$, we have $\text{rank}(f) \leq 2q_2 + 1 = r$, where the last transition is due to [Condition 3.12](#).

The strategy for Bob is:

1. Receive the question $(E', A_{\text{in}}, A_{\text{mid}})$.
2. Conditioned on E', A_{in} and A_{mid} , sample $(*, A_{\text{in}}, A_{\text{mid}}, *, E', U') \sim \mathcal{D}_{\text{mid}}$.
3. Return the bilinear map $G[E', A_{\text{in}}, U']$ (note that by definition, the table $G[\cdot]$ does not contain **nil** entries).

Step 2: analysis of the strategy. Since

$$\mathbb{E}_{(E, A_{\text{in}}, *, *, *, *) \sim \mathcal{D}_{\text{mid}}} [\text{Vrf}_{F', G}(E, A_{\text{in}}, *, *, *)] = \text{Vrf}_{F', G} \geq 2^{1-q_2/3},$$

we have⁹

$$\mathbb{P}_{(E, A_{\text{in}}, *, *, *, *) \sim \mathcal{D}_{\text{mid}}} [\text{Vrf}_{F', G}(E, A_{\text{in}}, *, *, *) \geq 2^{-q_2/3}] \geq 2^{-q_2/3}. \quad (5.9)$$

For any $E \in \mathcal{E}(H, k)$ and $A_{\text{in}} \in (\mathbb{F}_2^E)^{q_1}$ such that $\text{Vrf}_{F', G}(E, A_{\text{in}}, *, *, *) \geq 2^{-q_2/3}$, we know from [Lemma 5.16](#) that

$$\mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, *, *, *) \sim \mathcal{D}_{\text{mid}}} [\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}] \neq \emptyset \mid E, A_{\text{in}}] \geq 4^{-\ell_2^2}.$$

Combining with [Equation \(5.9\)](#) yields

$$\mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, *, *, *) \sim \mathcal{D}_{\text{mid}}} [\mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}] \neq \emptyset] \geq 2^{-2\ell_2^2 - q_2/3}. \quad (5.10)$$

Given a tuple $(E, A_{\text{in}}, A_{\text{mid}})$ and an element $f \in \mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$, we have

$$\begin{aligned} & \mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, *, E', U') \sim \mathcal{D}_{\text{mid}}} [G[E', A_{\text{in}}, U'] = f \mid_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \mid E, A_{\text{in}}, A_{\text{mid}}] \\ & \geq \mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, U, E', U') \sim \mathcal{D}_{\text{mid}}} [F'[E, A_{\text{in}}, U] = f \text{ and } \text{Vrf}_{F', G}(E, A_{\text{in}}, U, E', U') = 1 \mid E, A_{\text{in}}, A_{\text{mid}}] \\ & = \mathbb{E}_{(E, A_{\text{in}}, A_{\text{mid}}, U, *, *) \sim \mathcal{D}_{\text{mid}}} [\mathbb{1}[F'[E, A_{\text{in}}, U] = f] \cdot \text{Vrf}_{F', G}(E, A_{\text{in}}, U, *, *) \mid E, A_{\text{in}}, A_{\text{mid}}] \\ & \geq 2^{1-q_2/3} \cdot \mathbb{P}_{(E, A_{\text{in}}, A_{\text{mid}}, U, *, *) \sim \mathcal{D}_{\text{mid}}} [F'[E, A_{\text{in}}, U] = f \mid E, A_{\text{in}}, A_{\text{mid}}] \\ & \quad \text{(because } (F', G) \text{ is the } (2^{1-q_2/3})\text{-pruning of } (F, G)) \\ & \geq 2^{1-\ell_2^2 - q_2/3}. \quad \text{(since } f \in \mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]) \end{aligned}$$

Importantly, conditioned on $E, A_{\text{in}}, A_{\text{mid}}$ and E' , the distribution of U' in a conditional sample $(E, A_{\text{in}}, A_{\text{mid}}, *, E', U') \sim \mathcal{D}_{\text{mid}}$ does not depend on E . Therefore, the above display implies that under the strategies presented in Step 1 of the proof, for any tuple $(E, A_{\text{in}}, A_{\text{mid}})$ with any element $f \in \mathcal{F}[E, A_{\text{in}}, A_{\text{mid}}]$, the following expectation is at least $2^{1-\ell_2^2 - q_2/3}$:

$$\mathbb{E}_{(E, A_{\text{in}}, A_{\text{mid}}, *, E', *) \sim \mathcal{D}_{\text{mid}}} \left[\mathbb{P}_{\text{Bob}} [\text{Bob returns } f \mid_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} \text{ on question } (E', A_{\text{in}}, A_{\text{mid}})] \mid E, A_{\text{in}}, A_{\text{mid}} \right].$$

Combining with [Equation \(5.10\)](#), this implies that¹⁰

$$\mathbb{E}_{(E, A_{\text{in}}, A_{\text{mid}}, *, E', *) \sim \mathcal{D}_{\text{mid}}} \left[\mathbb{P}_{\text{Bob}} [\text{Alice}(E, A_{\text{in}}, A_{\text{mid}}) \mid_{\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}} = \text{Bob}(E', A_{\text{in}}, A_{\text{mid}})] \right]$$

is at least

$$2^{-2\ell_2^2 - q_2/3} \cdot 2^{1-\ell_2^2 - q_2/3} > k^{-1/2},$$

where we used [Condition 3.12](#) in the last transition. Since the distribution of $(E, A_{\text{in}}, A_{\text{mid}}, E')$ in $\text{Game1b}[H, k, q_1, q_2, r, \beta]$ is identical to the distribution of the sample $(E, A_{\text{in}}, A_{\text{mid}}, *, E', *) \sim \mathcal{D}_{\text{mid}}$, it follows that our prescribed strategies pass $\text{Game1b}[H, k, q_1, q_2, r, \beta]$ with probability

$$\text{val}(\text{Game1b}[H, k, q_1, q_2, r, \beta]) > k^{-1/2},$$

contradicting [Lemma 4.28](#). □

⁹Here we use the fact that $\text{Vrf}_{F', G}(E, A_{\text{in}}, *, *, *)$ always lies in $[0, 1]$.

¹⁰Here we use $\text{Alice}(E, A_{\text{in}}, A_{\text{mid}})$ to denote Alice's answer to the question $(E, A_{\text{in}}, A_{\text{mid}})$, and $\text{Bob}(E', A_{\text{in}}, A_{\text{mid}})$ denotes Bob's answer to $(E', A_{\text{in}}, A_{\text{mid}})$.

5.4 Lazy Parallel Repetition

In this subsection, we apply a “lazy parallel repetition” to **Game2a** to get **Game2b**. More precisely, we consider the following 2-prover 1-round game, in which Alice and Bob get t -blocks of challenges, one of which is a true challenge from **Game2a**, whereas on each one of the rest of the blocks they receive the same randomly sampled challenge of Alice from **Game2a**. Additionally, on each block the players receive a list of advice vectors.

Definition 5.20. Given positive integers k, ℓ_2, t , nonnegative integers q_0, q_1 , a parameter $\beta \in [0, 1)$ and a 3-uniform hypergraph H , let **Game2b** $[H, k, \ell_2, t, q_0, q_1, \beta]$ be a 2-Prover 1-Round game where the verifier executes the following:

1. For each $j \in [t]$, sample a uniformly random tripled set $E_j \in \mathcal{E}(H, k)$.
2. Sample a uniformly random index $c \in [t]$. Sample $(E'_c, A_c, \text{empty}, U_c) \sim \mathcal{J}_{\text{mid}}(E_c, q_1, 0, \beta, \ell_2)$. Sample a random vector $x \in \mathbb{F}_2^{E'_c}$ and let $U'_c = U_c + \text{span}(x)$.
3. For each $j \in [t] \setminus \{c\}$, do the following:
 - Sample a uniformly random advice sequence $A_j = (a^{(j,1)}, \dots, a^{(j,q_0)}) \in (\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j})^{q_0}$, i.e. $a^{(j,i)}$ is a uniformly random vector in $\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j}$ for each $i \in [q_0]$.
 - Sample $(E_j^{\text{ghost}}, \text{empty}, \text{empty}, U_j) \sim \mathcal{J}_{\text{mid}}(E_j, 0, 0, \beta, \ell_2)$.
 - Let $E'_j = E_j$ and $U'_j = U_j$.
4. Denote sequences

$$\begin{aligned} \mathcal{E} &= (E_1, \dots, E_t), & \mathcal{U} &= (U_1, \dots, U_t), & \mathcal{A} &= (A_1, \dots, A_t), & \text{and} \\ \mathcal{E}' &= (E'_1, \dots, E'_t), & \mathcal{U}' &= (U'_1, \dots, U'_t). \end{aligned}$$

5. Send $(\mathcal{E}, \mathcal{A}, \mathcal{U})$ to Alice and $(c, \mathcal{E}', \mathcal{A}, \mathcal{U}')$ to Bob.
6. Alice must return NAE-satisfying symmetric bilinear forms

$$f_j : \mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \rightarrow \mathbb{F}_2 \text{ such that } \text{rank}(f_j|_{U_j \otimes U_j}) \leq 1 \quad \text{for each } j \in [t];$$

Bob must return bilinear forms

$$g_j : \mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j} \rightarrow \mathbb{F}_2 \quad \text{for each } j \in [t].$$

Accept if g_j is the restriction of f_j to $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$ for each $j \in [t]$.

If we ignore the lists A_j , the game we have above is exactly the lazy parallel repetition version of **Game2a**. Lazy parallel repetition is well-known to preserve completeness and soundness (but not improve them), as well as to improve the “smoothness” of a game. We include the lists A_j to enable the advice feature in the inner PCP, and we show that they do not hurt the soundness of the construction (they have no effect on other features of the construction).

The completeness of **Game2b** is again straightforward:

Lemma 5.21 (Game2b completeness). *For any positive integers k, ℓ_2, t such that $k \geq \ell_2$, nonnegative integers q_0, q_1 , parameter $\beta \in [0, 1)$ and 2-colorable 3-uniform hypergraph H , we have*

$$\text{val}(\text{Game2b}[H, k, \ell_2, t, q_0, q_1, \beta]) = 1.$$

Proof. We fix strategies from [Lemma 5.10](#) that achieve value 1. Alice ignores the lists A_j and answers each block $j \in [t]$ separately according to her strategy from [Game2a](#). Bob answers according to Alice's strategy for [Game2a](#) on the noncritical blocks $j \in [t] \setminus \{c\}$, and according to Bob's strategy for [Game2a](#) on the critical block $j = c$. $\square$

The following lemma establishes the soundness of [Game2b](#).

Lemma 5.22 (Game2b soundness). *Assume [Condition 3.12](#). Suppose that in every 4^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}\left(\text{Game2b}[H, k, \ell_2, t, q_0, q_1, \beta]\right) \leq 2^{-q_2/4}.$$

Proof. It suffices to show that

$$\text{val}\left(\text{Game2b}[H, k, \ell_2, t, q_0, q_1, \beta]\right) \leq \text{val}\left(\text{Game2a}[H, k, \ell_2, q_1, 0, \beta]\right),$$

after which the conclusion follows from [Lemma 5.19](#) (combined with [Remark 5.3](#)).

Assume Alice and Bob have a strategy for [Game2b](#) $[H, k, \ell_2, t, q_0, q_1, \beta]$, and we next show how to derive a strategy for [Game2a](#) $[H, k, \ell_2, q_1, 0, \beta]$. In the latter game, Alice and Bob can first agree upon the following “shared data” using public randomness:

- a uniformly random critical index $c \in [t]$, and
- a uniformly random tuple (E_j, A_j, U_j) for each non-critical index $j \in [t] \setminus \{c\}$. More precisely, sample E_j from $\mathcal{E}(H, k)$ uniformly, sample A_j from $(\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j})^{q_0}$ uniformly, and sample U_j by drawing $(E_j^{\text{ghost}}, \text{empty}, \text{empty}, U_j) \sim \mathcal{J}_{\text{mid}}(E_j, 0, 0, \beta, \ell_2)$.

Given a question (E, A, U) in [Game2a](#) $[H, k, \ell_2, q_1, 0, \beta]$, Alice can construct $(\mathcal{E}, \mathcal{A}, \mathcal{U})$ by planting (E, A, U) in the critical block c and using the shared data for the non-critical blocks. Similarly, given a question (E', A', U') , Bob can construct $(\mathcal{E}', \mathcal{A}', \mathcal{U}')$ by planting (E', A', U') in the critical block c and using the shared data for the non-critical blocks. The provers can then pretend that they are in [Game2b](#) $[H, k, \ell_2, t, q_0, q_1, \beta]$, and use their strategy for [Game2b](#) $[H, k, \ell_2, t, q_0, q_1, \beta]$ to answer the verifier in [Game2a](#) $[H, k, \ell_2, q_1, 0, \beta]$. Whenever the strategy for [Game2b](#) $[H, k, \ell_2, t, q_0, q_1, \beta]$ provides consistent answers to $(\mathcal{E}, \mathcal{A}, \mathcal{U})$ and $(c, \mathcal{E}', \mathcal{A}', \mathcal{U}')$, the consistency in the critical block implies that the derived answers to the questions (E, A, U) and (E', A', U') in [Game2a](#) $[H, k, \ell_2, q_1, 0, \beta]$ are also consistent. Therefore, the verifier in [Game2a](#) $[H, k, \ell_2, q_1, 0, \beta]$ accepts with probability at least the acceptance probability in [Game2b](#) $[H, k, \ell_2, t, q_0, q_1, \beta]$. $\square$

6 The Inner PCP

In this section we construct and analyze our inner PCP as discussed in [Section 2.2.6](#). We first prepare some necessary framework in [Sections 6.1](#) and [6.2](#). The final sub-4-to-1 game, denoted by [Game3](#), will then be defined in [Section 6.3](#). The proof of the soundness of [Game3](#) is rather long, and will be completed in [Section 6.4](#).

6.1 Preparation: Tripled Packets

In the inner PCP, we will add another layer of Grassmann-type structure onto [Game2b](#), which is already somewhat complicated. To make future notations more concise, in this subsection we set up some notational framework for the objects featured in [Game2b](#) ([Definition 5.20](#)).

Recall that in [Definition 5.20](#), for each index $j \in [t]$, Alice needs to return a bilinear map $f : \mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \rightarrow \mathbb{F}_2$ that is both symmetric and NAE-satisfying. The following definition combines the two conditions, exploiting the fact that both are “linear” conditions in f .

Definition 6.1. Let E be a tripled set. For any $v \in E$, we let $e_v \in \mathbb{F}_2^E$ denote the standard basis vector supported on v ; that is, for $u \in E$ let $(e_v)_u = 1$ if and only if $u = v$.

- (1) We define $\mathcal{N}_1(E) \subseteq \mathbb{F}_2^E \otimes \mathbb{F}_2^E$ to be the linear subspace spanned by all vectors of the form

$$e_{v_1} \otimes e_{v_1} + e_{v_2} \otimes e_{v_2} + e_{v_3} \otimes e_{v_3} + e_{v_1} \otimes e_{v_2} + e_{v_2} \otimes e_{v_3} + e_{v_3} \otimes e_{v_1},$$

where $\{v_1, v_2, v_3\}$ ranges in $\text{Triples}(E)$.¹¹

- (2) We let $\mathcal{N}_2(E) \subseteq \mathbb{F}_2^E \otimes \mathbb{F}_2^E$ be the linear subspace spanned by all anti-symmetric vectors, i.e.

$$\mathcal{N}_2(E) = \text{span} \{x \otimes y + y \otimes x \mid x, y \in \mathbb{F}_2^E\}.$$

- (3) Let $\mathcal{N}(E) = \mathcal{N}_1(E) + \mathcal{N}_2(E)$ be the sum of the two subspaces.

- (4) A linear map $f : \mathcal{N}(E) \rightarrow \mathbb{F}_2$ is said to be *SymNAE-satisfying* if we have:

- $f(e_{v_1} \otimes e_{v_1} + e_{v_2} \otimes e_{v_2} + e_{v_3} \otimes e_{v_3} + e_{v_1} \otimes e_{v_2} + e_{v_2} \otimes e_{v_3} + e_{v_3} \otimes e_{v_1}) = 1$ for all triples $\{v_1, v_2, v_3\} \in \text{Triples}(E)$; and
- $f(x \otimes y + y \otimes x) = 0$ for all $x, y \in \mathbb{F}_2^E$.

Intuitively, the space $\mathcal{N}_1(E)$ from the first item above is the subspace of $\mathbb{F}_2^E \otimes \mathbb{F}_2^E$ on which the value of a bilinear form $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ is fully determined if it is NAE-satisfying. The space $\mathcal{N}_2(E)$ from the second item above is the subspace of $\mathbb{F}_2^E \otimes \mathbb{F}_2^E$ on which the value of a bilinear form $f : \mathbb{F}_2^E \otimes \mathbb{F}_2^E \rightarrow \mathbb{F}_2$ is fully determined if it is symmetric. Thus, overall, whether f is both NAE-satisfying and symmetric is fully captured by its value on $\mathcal{N}(E)$, and this is the definition of SymNAE-satisfying.

The following proposition asserts that there is always a linear map on $\mathcal{N}(E)$ which is SymNAE-satisfying.

Proposition 6.2. For any tripled set E , there is a unique linear map $f : \mathcal{N}(E) \rightarrow \mathbb{F}_2$ that is SymNAE-satisfying.

Proof. This is clear because $\mathcal{N}_1(E) \cap \mathcal{N}_2(E) = \{0\}$. □

In order to aggregate the spaces $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$ in all blocks, we introduce the following notation. Here we use $\mathcal{E}'$ instead of $\mathcal{E}$ to emphasize that the sets $E'_1, \dots, E'_t$ are not necessarily tripled sets.

Definition 6.3. For a sequence of (not necessarily tripled) finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, we let $\mathcal{V}(\mathcal{E}')$ denote the $\mathbb{F}_2$ -vector space

$$\mathcal{V}(\mathcal{E}') = \bigoplus_{j=1}^t \left(\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j} \right).$$

¹¹We assume that for each triple $\{v_1, v_2, v_3\} \in \text{Triples}(E)$, there is a fixed ordering of the elements v_1, v_2, v_3 .

Remark 6.4. Let H be a 3-uniform hypergraph. For $E_1, \dots, E_t \in \mathcal{E}(H, k)$ and $\mathcal{E} = (E_1, \dots, E_t)$, the space $\mathcal{V}(\mathcal{E})$ can be regarded as a subspace of the huge ambient space

$$\left(\mathbb{F}_2^{\mathcal{Y}(H, k)} \otimes \mathbb{F}_2^{\mathcal{Y}(H, k)} \right)^t.$$

Next, we define subspaces of $\mathcal{V}(\mathcal{E}')$ that correspond to the tensor checks we impose on Alice or Bob in **Game2b**.

Definition 6.5. Fix a sequence of (not necessarily tripled) finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$ and a sequence of linear subspaces $\mathcal{U} = (U_1, \dots, U_t)$ with $U_j \subseteq \mathbb{F}_2^{E'_j}$ for each $j \in [t]$. We let $\bigoplus \mathcal{U} \subseteq \mathcal{V}(\mathcal{E}')$ be the linear subspace defined by

$$\bigoplus \mathcal{U} = \bigoplus_{j=1}^t (U_j \otimes U_j) \subseteq \bigoplus_{j=1}^t (\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}) = \mathcal{V}(\mathcal{E}').$$

A linear map $f : \bigoplus \mathcal{U} \rightarrow \mathbb{F}_2$ is said to be *SR-satisfying*¹² if for each $j \in [t]$, the restriction $f|_{U_j \otimes U_j}$ is a symmetric bilinear map of rank at most 1.

Combining the side conditions, symmetry and tensor checks gives rise to the space $\mathcal{N}(\mathcal{E}, \mathcal{U})$ defined as follows.

Definition 6.6. A *tripled packet* is a pair $(\mathcal{E}, \mathcal{U})$, where $\mathcal{E} = (E_1, \dots, E_t)$ is a sequence of tripled sets, and $\mathcal{U} = (U_1, \dots, U_t)$ is a sequence of linear subspaces with $U_j \subseteq \mathbb{F}_2^{E_j}$ for each $j \in [t]$. We let $\mathcal{N}(\mathcal{E}, \mathcal{U}) \subseteq \mathcal{V}(\mathcal{E})$ be the linear subspace defined by

$$\mathcal{N}(\mathcal{E}, \mathcal{U}) = \bigoplus_{j=1}^t (\mathcal{N}(E_j) + U_j \otimes U_j) \subseteq \bigoplus_{j=1}^t (\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j}) = \mathcal{V}(\mathcal{E}).$$

Thus, whether $f : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ satisfies all side conditions, symmetry and tensor tests amounts to checking the following condition on $f|_{\mathcal{N}(\mathcal{E}, \mathcal{U})}$.

Definition 6.7. Given a tripled packet $(\mathcal{E}, \mathcal{U})$ where $\mathcal{E} = (E_1, \dots, E_t)$ and $\mathcal{U} = (U_1, \dots, U_t)$, a linear map $f : \mathcal{N}(\mathcal{E}, \mathcal{U}) \rightarrow \mathbb{F}_2$ is said to be *SNR-satisfying*¹³ if we have:

- $f|_{\mathcal{N}(E_j)}$ is SymNAE-satisfying for each $j \in [t]$.
- $\text{rank}(f|_{U_j \otimes U_j}) \leq 1$ for each $j \in [t]$.

6.1.1 Thinning of Tripled Packets

Recall that in **Game2b**, we plant the true challenge in one randomly chosen coordinate, and it plays a crucial role in our argument. We often refer to it as the *critical index/coordinate/block*, and make use of the following notations.

Definition 6.8. Let $(E_1, \dots, E_t)$ be a sequence of tripled sets. Fix an index $c \in [t]$ and a parameter $\beta \in [0, 1]$. We write $\mathcal{E}' \sim \text{Thin}_{c, \beta}(\mathcal{E})$ for the random sequence $\mathcal{E}' = (E'_1, \dots, E'_t)$ obtained by setting $E'_j = E_j$ for all $j \in [t] \setminus \{c\}$ and sampling $E'_c \sim \text{Thin}_\beta(E_c)$. A sequence $\mathcal{E}'$ in the support of the distribution $\text{Thin}_{c, 1/2}(\mathcal{E})$ is called a *c-critical descendant* of $\mathcal{E}$.

¹²In this terminology, “S” stands for symmetric, and “R” stands for rank.

¹³In this terminology, “S” stands for symmetric, “N” stands for NAE, and “R” stands for rank.

The following definition captures the distribution of $(\mathcal{U}, \mathcal{E}', \mathcal{U}')$ conditioned on $\mathcal{E}$ in [Definition 5.20](#). Here we do not take into consideration the advice list $\mathcal{A}$, because it will not be used to construct our final sub-4-to-1 game (it is crucial however for the soundness analysis).

Definition 6.9. Let $\mathcal{E} = (E_1, \dots, E_t)$ be a sequence of tripled sets. Fix a parameter $\beta \in [0, 1]$ and a nonnegative integer ℓ . We let $\mathcal{J}_{\text{in}}(\mathcal{E}, \beta, \ell)$ denote the output distribution of the following process:

1. Sample a uniformly random index $c \in [t]$. Sample $(E'_c, \text{empty}, \text{empty}, U_c) \sim \mathcal{J}_{\text{mid}}(E_c, 0, 0, \beta, \ell)$. Sample a random vector $x \in \mathbb{F}_2^{E'_c}$ and let $U'_c = U_c + \text{span}(x)$.
2. For each $j \in [t] \setminus \{c\}$, sample $(E_j^{\text{ghost}}, \text{empty}, \text{empty}, U_j) \sim \mathcal{J}_{\text{mid}}(E_j, 0, 0, \beta, \ell)$. Let $E'_j = E_j$ and $U'_j = U_j$.
3. Let $\mathcal{E}' = (E'_1, \dots, E'_t)$, $\mathcal{U} = (U_1, \dots, U_t)$ and $\mathcal{U}' = (U'_1, \dots, U'_t)$.
4. Output the tuple $(c, \mathcal{U}, \mathcal{E}', \mathcal{U}')$.

We will make use of the following simple observation:

Proposition 6.10. In the setting and notation of [Definition 6.9](#), the random subspaces $U_1, \dots, U_t$ are mutually independent. Furthermore, they are jointly independent of the random index c .

Proof. Regardless of whether $j = c$ or $j \neq c$, the subspace U_j is spanned by ℓ independent vectors supported on a random β -thinning of E_j . $\square$

6.2 Preparation: Low-Rank Grassmann

As discussed in [Section 2.2.6](#), in the inner PCP we want to use linear subspaces of $\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}$ that consist only of low-rank vectors. As stated in [Definition 2.6](#), these linear subspaces will form a subset $\text{LGr}(\mathbb{F}_2^{E_c}, \ell)$ of $\text{Gr}(\mathbb{F}_2^{E_c} \otimes \mathbb{F}_2^{E_c}, \ell)$, and the subgraph it induces from the Grassmann graph is called the *low-rank Grassmann graph*. In this subsection, we give formal definitions of the low-rank Grassmann and prove a number of elementary facts about it. We will primarily be interested in the basic “statistical” properties of $\text{LGr}(\mathbb{F}_2^{E_c}, \ell)$, such as its zoom-out probabilities being close to those of the full Grassmann graph:

$$\mathbb{P}_{L \in \text{LGr}(V, \ell)} [L \subseteq W] \approx \mathbb{P}_{L \in \text{Gr}(V \otimes V, \ell)} [L \subseteq W], \quad (6.1)$$

for any vector space V and subspace $W \subseteq V \otimes V$ with small codimension. More sophisticated analysis of the low-rank Grassmann graph, such as its spectral expansion (see [\[Gol23\]](#)), will not be used in this paper.

6.2.1 Construction from Hadamard Code

The definition of the low-rank Grassmann will use linear combinations of vectors given by the Hadamard matrix, defined as follows.

Definition 6.11. Let ℓ be a positive integer. For each $i \in \{0, 1, \dots, 2^\ell - 1\}$ and $b \in \{0, 1, \dots, \ell - 1\}$, define $\text{Bit}_\ell(i, b) \in \mathbb{F}_2$ to be the mod-2 remainder of the integer $\lfloor i \cdot 2^{-b} \rfloor$. Equivalently, the sequence

$$(\text{Bit}_\ell(i, \ell - 1), \text{Bit}_\ell(i, \ell - 2), \dots, \text{Bit}_\ell(i, 0))$$

is the length- ℓ binary representation of i , with the most significant bit listed first.

For each integer $i \in \{0, 1, \dots, 2^\ell - 1\}$ and vector $u \in \mathbb{F}_2^\ell$, define

$$\text{Had}_\ell(u, i) = \sum_{b=1}^{\ell} u_b \text{Bit}_\ell(i, \ell - b) \in \mathbb{F}_2,$$

to be the “inner product” of u with the binary representation of i (viewed as a vector in $\mathbb{F}_2^\ell$).

We next define the span of a list of vectors according to the Hadamard matrix.

Definition 6.12. Let ℓ, s be positive integers, and let $q = 2s(2^\ell - 1)$. Suppose E' is a finite set, and $A \in (\mathbb{F}_2^{E'})^q$ is a sequence of vectors

$$A = (a^{(1)}, \dots, a^{(q)}).$$

For each $u \in \mathbb{F}_2^\ell$, define a vector

$$\text{Lvec}(A, \ell, u) = \sum_{i=0}^{2^\ell-2} \left(\text{Had}_\ell(u, 2^\ell - i - 1) \sum_{j=1}^s a^{(2si+2j-1)} \otimes a^{(2si+2j)} \right) \in \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}. \quad (6.2)$$

Since $u \mapsto \text{Had}_\ell(u, 2^\ell - i - 1)$ is a linear map for each i , the map $u \mapsto \text{Lvec}(A, \ell, u)$ from $\mathbb{F}_2^\ell$ to $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$ is also linear. For any linear subspace $U \subseteq \mathbb{F}_2^\ell$, we denote the image of the latter linear map restricted to U by

$$\text{Lspan}(A, \ell, U) = \{\text{Lvec}(A, \ell, u) \mid u \in U\} \subseteq \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}.$$

Let us make a few remarks about [Equation \(6.2\)](#). To get some intuition it is useful to consider a vector defined along the lines of [Equation \(6.2\)](#), except that we replace the sum of rank 1 vectors with arbitrary vectors $x^{(i)} \in \mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$, getting

$$\sum_{i=0}^{2^\ell-2} \text{Had}_\ell(u, 2^\ell - i - 1) x^{(i)}. \quad (6.3)$$

Ranging over all $u \in \mathbb{F}_2^\ell$, the resulting collection of vectors is easily seen to be a linear subspace of $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$ of dimension at most ℓ . Moreover, if the vectors $x^{(i)}$ are taken uniformly at random, then, conditioned on this subspace having dimension ℓ , it is uniformly distributed among all ℓ -dimensional subspaces of $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$.

It follows that the space $\text{Lspan}(A, \ell, U)$ is also a subspace of $\mathbb{F}_2^{E'} \otimes \mathbb{F}_2^{E'}$ with at most ℓ dimensions. However, it is not distributed uniformly when the vectors in the list A are taken uniformly, and this fact is crucial for us. Indeed, it is easy to see that each vector in $\text{Lspan}(A, \ell, U)$ has rank at most $2^{\ell-1}s$; this is the source of the term “low-rank” in the name. In the following remark, we argue that if the list A is generic, then the rank of each nonzero vector is exactly $2^{\ell-1}s$ (which will be convenient for us for technical reasons).

Remark 6.13. In the setting and notation of [Definition 6.12](#), suppose that the odd-indexed vectors $a^{(1)}, a^{(3)}, \dots, a^{(q-1)}$ are linearly independent, and that the even-indexed vectors $a^{(2)}, a^{(4)}, \dots, a^{(q)}$ are also linearly independent. Then for any $u \in \mathbb{F}_2^\ell \setminus \{0\}$, since $\text{Had}_\ell(u, i) = 1$ for exactly $2^{\ell-1}$ of the i 's in $\{1, 2, \dots, 2^\ell - 1\}$, it follows from [Equation \(6.2\)](#) that

$$\text{rank}(\text{Lvec}(A, \ell, u)) = 2^{\ell-1}s.$$

Furthermore, it is easy to see that $\dim(\text{Lspan}(A, \ell, \mathbb{F}_2^\ell)) = \ell$.

6.2.2 Mixed-Type Advice Sequences

Our inner PCP will include a tensor product of the low-rank Grassmann graph (on the critical block) with the standard Grassmann graph (on non-critical blocks). In this section, we present a few notations that will be useful in presenting and working with the resulting product space.

Definition 6.14. Given a sequence of finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a subset of indices $J \subseteq [t]$ and positive integers ℓ, s , we let $\mathcal{A}_J(\mathcal{E}', \ell, s)$ be the collection of advice sequences $(A_1, \dots, A_t)$ such that:

- (1) For each $j \in [t] \setminus J$, the component A_j is a sequence of ℓ vectors $A_j = (a^{(j,1)}, \dots, a^{(j,\ell)})$, where

$$a^{(j,i)} \in \mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j} \quad \text{for all } i \in [\ell].$$

- (2) For each $c \in J$, the component A_c is a sequence of $q = 2s(2^\ell - 1)$ vectors $A_c = (a^{(c,1)}, \dots, a^{(c,q)})$, where

$$a^{(c,i)} \in \mathbb{F}_2^{E'_c} \quad \text{for all } i \in [q].$$

If both sequences $(a^{(c,1)}, a^{(c,3)}, \dots, a^{(c,q-1)})$ and $(a^{(c,2)}, a^{(c,4)}, \dots, a^{(c,q)})$ are linearly independent, we say that A_c is *saturated*.

We let $\mathcal{A}_J^*(\mathcal{E}', \ell, s)$ denote the sub-collection of advice sequences $(A_1, \dots, A_t) \in \mathcal{A}_J(\mathcal{E}', \ell, s)$ such that A_c is saturated for each $c \in J$.

Remark 6.15. A few remarks are in order:

- (1) The set of coordinates in J in [Definition 6.14](#) should be thought of as the potentially critical coordinates, hence the collection there is specified by vectors from the base space $\mathbb{F}_2^{E'_j}$. The coordinates outside J are not critical, and the vectors there are completely arbitrary vectors from $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$.
- (2) An advice sequence in $\mathcal{A}_J(\mathcal{E}', \ell, s)$ should be thought of as the analog of a spanning set of a subspace. In other words, there may be linear dependencies between vectors in a member from $\mathcal{A}_J(\mathcal{E}', \ell, s)$. In our setting of parameters this will be rare (analogously to the fact that a random set of $o(n)$ independently chosen vectors in $\mathbb{F}_2^n$ are linearly independent with high probability), and $\mathcal{A}_J^*(\mathcal{E}', \ell, s) \subseteq \mathcal{A}_J(\mathcal{E}', \ell, s)$ is the subcollection that corresponds to tuples with no linear dependencies.

The following definition associates vectors from $\mathcal{V}(\mathcal{E}')$ with each advice sequence. In words, on each potentially critical coordinate we take the low-rank Hadamard span as per [Definition 6.12](#), and on non-critical coordinates we take the span for arbitrary vectors as per [Equation \(6.3\)](#).

Definition 6.16. Fix a sequence of finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a proper subset of indices $J \subsetneq [t]$ and positive integers ℓ, s . Given an advice sequence $\mathcal{A} = (A_1, \dots, A_t) \in \mathcal{A}_J(\mathcal{E}', \ell, s)$, write $A_j = (a^{(j,1)}, \dots, a^{(j,\ell)})$ for each $j \in [t] \setminus J$. For each $u \in \mathbb{F}_2^\ell$, define¹⁴

$$\text{Mvec}_J(\mathcal{A}, u) = \sum_{c \in J} \text{Lvec}(A_c, \ell, u) + \sum_{j \in [t] \setminus J} \left(\sum_{b=1}^{\ell} u_b \cdot a^{(j,b)} \right) \in \mathcal{V}(\mathcal{E}'). \quad (6.4)$$

For any linear subspace $U \subseteq \mathbb{F}_2^\ell$, we denote

$$\text{Mspan}_J(\mathcal{A}, U) = \{\text{Mvec}_J(\mathcal{A}, u) \mid u \in U\} \subseteq \mathcal{V}(\mathcal{E}'). \quad (6.5)$$

¹⁴We suppress the parameters ℓ, s in the notation $\text{Mvec}_J(\mathcal{A}, u)$; indeed, the values of ℓ and s can be inferred from $\mathcal{A}$, as long as $J \neq \emptyset$ and $J \neq [t]$.

Notation 6.17. In the remainder of the paper, we will often use the notation $\text{Mspan}_J(\mathcal{A}, U)$ (defined in Equation (6.5)) with $U = \mathbb{F}_2^\ell$. When J is clear from context, we abbreviate

$$\sigma(\mathcal{A}) := \text{Mspan}_J(\mathcal{A}, \mathbb{F}_2^\ell).$$

We also write

$$\rho(\mathcal{A}) := (\text{Mvec}_J(\mathcal{A}, e_1), \dots, \text{Mvec}_J(\mathcal{A}, e_\ell)) \in (\mathcal{V}(\mathcal{E}'))^\ell,$$

where $e_1, \dots, e_\ell$ denote the standard basis vectors of $\mathbb{F}_2^\ell$. Thus, $\sigma(\mathcal{A})$ is the linear span of the vectors in the sequence $\rho(\mathcal{A})$, and we write $\sigma(\mathcal{A}) = \text{span}(\rho(\mathcal{A}))$.

Given an advice sequence $\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)$, the subspace $\sigma(\mathcal{A})$ is “mixed-type” in the sense that its projection on a critical block $c \in J$ consists of low-rank vectors in $\mathbb{F}_2^{E'_c} \otimes \mathbb{F}_2^{E'_c}$, while its projection on a non-critical block $j \in [t] \setminus J$ consists of generic vectors in $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$.

Next, we will want to facilitate notions analogous to subspace containment for mixed-type subspaces. Towards this end, it is useful to note that if we considered Equation (6.3) and only looked at vectors u with $u_\ell = 0$, then we would get an $(\ell - 1)$ -dimensional space which is a subspace of the larger ℓ -dimensional space resulting from taking all u . Moreover, this subspace would not depend on what is $x^{(2^\ell - 2)}$ (as its coefficient will always be 0). Generalizing this intuition, we get the following analogous notion of sub-advice.

Definition 6.18. Fix a sequence of finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a proper subset of indices $J \subsetneq [t]$, positive integers ℓ, s and a nonnegative integer $q_0 \leq \ell$. Given an advice sequence $\mathcal{A} = (A_1, \dots, A_t) \in \mathcal{A}_J(\mathcal{E}', \ell, s)$, we define a *sub-advice* $\mathcal{A}_{[q_0]} = (A'_1, \dots, A'_t) \in \mathcal{A}_J(\mathcal{E}', q_0, 2^{\ell - q_0} s)$ as follows:

- (1) For each $j \in [t] \setminus J$, write $A_j = (a^{(j,1)}, \dots, a^{(j,\ell)})$ and let $A'_j = (a^{(j,1)}, \dots, a^{(j,q_0)})$.
- (2) For each $c \in J$, write $A_c = (a^{(c,1)}, \dots, a^{(c,q)})$, where $q = 2s(2^\ell - 1)$. Denote $q_1 = 2s(2^\ell - 2^{\ell - q_0})$ and let $A'_c = (a^{(c,1)}, \dots, a^{(c,q_1)})$.

The following proposition formalizes the intuition that taking a sub-advice corresponds to spanning a subspace of the original space.

Proposition 6.19. In the setting and notation of Definition 6.18, we have¹⁵

$$\text{Mvec}_J(\mathcal{A}, u) = \text{Mvec}_J(\mathcal{A}_{[q_0]}, u) \quad \text{for all } u \in \mathbb{F}_2^{q_0},$$

Consequently, by Equation (6.5) we have

$$\text{Mspan}_J(\mathcal{A}, \mathbb{F}_2^{q_0}) = \text{Mspan}_J(\mathcal{A}_{[q_0]}, \mathbb{F}_2^{q_0}).$$

Proof. Denote $s_1 = 2^{\ell - q_0} s$. As in Definition 6.18, let $q = 2s(2^\ell - 1)$ and $q_1 = 2s(2^\ell - 2^{\ell - q_0})$.

Let i be an integer ranging in $\{0, 1, \dots, 2^\ell - 2\}$. For each $u \in \mathbb{F}_2^{q_0}$ considered as an ℓ -bit string, since its last $(\ell - q_0)$ bits are all 0's, the value of

$$\text{Had}_\ell(u, 2^\ell - i - 1) = \sum_{b=1}^{q_0} u_b(1 - \text{Bit}_\ell(i, \ell - b))$$

does not depend on the last $(\ell - q_0)$ bits of the binary representation of i . Furthermore, if the first q_0 bits of i are all 1's, then $\text{Had}_\ell(u, 2^\ell - i - 1) = 0$. Therefore, if we define $\pi(i) = 2^{\ell - q_0} \lfloor i / 2^{\ell - q_0} \rfloor$ for

¹⁵Here, we identify $\mathbb{F}_2^{q_0}$ with the subspace $\mathbb{F}_2^{q_0} \times \{0\}^{\ell - q_0} \subseteq \mathbb{F}_2^\ell$; that is, a q_0 -bit string is extended to an ℓ -bit string by appending $\ell - q_0$ zeros.

each $i \in \{0, 1, \dots, 2^\ell - 2^{\ell-q_0} - 1\}$, for each $c \in J$ and $u \in \mathbb{F}_2^{q_0}$ we can deduce from Equation (6.2) that

$$\begin{aligned} \text{Lvec}(A_c, \ell, u) &= \sum_{i=0}^{2^\ell - 2^{\ell-q_0} - 1} \left(\text{Had}_\ell(u, 2^\ell - \pi(i) - 1) \sum_{j=1}^s a^{(c, 2s_1i+2j-1)} \otimes a^{(c, 2s_1i+2j)} \right) \\ &= \sum_{i=0}^{2^{q_0}-2} \left(\text{Had}_\ell(u, 2^\ell - 2^{\ell-q_0}i - 1) \sum_{j=1}^{s_1} a^{(c, 2s_1i+2j-1)} \otimes a^{(c, 2s_1i+2j)} \right) \\ &= \sum_{i=0}^{2^{q_0}-2} \left(\text{Had}_{q_0}(u, 2^{q_0} - i - 1) \sum_{j=1}^{s_1} a^{(c, 2s_1i+2j-1)} \otimes a^{(c, 2s_1i+2j)} \right) = \text{Lvec}(A'_c, q_0, u). \end{aligned}$$

It then follows from Equation (6.4) that

$$\text{Mvec}_J(\mathcal{A}, u) = \sum_{c \in J} \text{Lvec}(A'_c, q_0, u) + \sum_{j \in [t] \setminus J} \left(\sum_{b=1}^{q_0} u_b \cdot a^{(j,b)} \right) = \text{Mvec}_J(\mathcal{A}_{[q_0]}, u),$$

for any $u \in \mathbb{F}_2^{q_0}$. $\square$

Notation 6.20. Throughout the remainder of the paper, the set $J \subseteq [t]$ of critical indices will always satisfy $|J| \in \{1, 2\}$. When $J = \{c_1, c_2\}$ with $c_1 \neq c_2$, we suppress the braces and write c_1, c_2 in place of $\{c_1, c_2\}$ whenever J appears as a subscript. For example, we write

$$\mathcal{A}_{c_1, c_2}(\mathcal{E}', \ell, s) \quad \text{instead of} \quad \mathcal{A}_{\{c_1, c_2\}}(\mathcal{E}', \ell, s).$$

Similarly, when $J = \{c\}$, we write, for instance,

$$\text{Mspan}_c(\mathcal{A}, U) \quad \text{instead of} \quad \text{Mspan}_{\{c\}}(\mathcal{A}, U).$$

6.2.3 Zoom-out Probabilities

We next prove a few elementary properties of the “zoom-out probabilities” associated with mixed-type advice sequences. Specifically, given a linear subspace $W \subseteq \mathcal{V}(\mathcal{E}')$ of small codimension, we aim to show that the probability that $\sigma(\mathcal{A}) \subseteq W$, where $\mathcal{A}$ is sampled at random from $\mathcal{A}_J(\mathcal{E}', \ell, s)$, is close to the probability that a random subspace $L \in \text{Gr}(\mathcal{V}(\mathcal{E}'), \ell)$ is contained in W .

For technical reasons, we also need a “zoomed-in” version of this comparison. Specifically, we consider a random advice sequence $\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)$ conditioned on $\sigma(\mathcal{A}_{[q_0]}) = Q$, where $Q \subseteq \mathcal{V}(\mathcal{E}')$ is a fixed q_0 -dimensional subspace. This should be analogous to sampling a random subspace $L \in \text{Gr}(\mathcal{V}(\mathcal{E}'), \ell)$ conditioned on $Q \subseteq L$. Our main goal is to argue that

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\sigma(\mathcal{A}) \subseteq W \mid \sigma(\mathcal{A}_{[q_0]}) = Q] \approx \mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}'), \ell)} [L \subseteq W \mid Q \subseteq L].$$

The first step is to show that conditioned on a fixed sub-advice $\mathcal{A}_{[q_0]}$, the vectors in $\sigma(\mathcal{A}) \setminus \sigma(\mathcal{A}_{[q_0]})$ still behave randomly with respect to any test function $f : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$.

Proposition 6.21. Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a subset of indices $J \subsetneq [t]$, positive integers ℓ, s and a nonnegative integer $q_0 < \ell$. Let $f : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$ be an arbitrary linear functional that is not identically zero. For any fixed advice sequence $\mathcal{A}' \in \mathcal{A}_J(\mathcal{E}', q_0, 2^{\ell-q_0}s)$ and any vector $u \in \mathbb{F}_2^\ell \setminus \mathbb{F}_2^{q_0}$, we have

$$\frac{1}{2} - 2^{-s-1} \leq \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [f(\text{Mvec}_J(\mathcal{A}, u)) = 1 \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] \leq \frac{1}{2} + 2^{-s-1}.$$

Proof. As usual, we denote $\mathcal{A} = (A_1, \dots, A_t)$ and $A_j = (a^{(j,1)}, a^{(j,2)}, \dots)$ for each $j \in [t]$. Since f is not identically zero, there exists an index $j \in [t]$ such that the restriction of f to $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$ is nonzero. Depending on whether this index lies in J , we divide into two cases:

Case 1: the restriction of f to $\mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$ is nonzero for some $j \in [t] \setminus J$. In this case, if we let $b \in \{q_0 + 1, \dots, \ell\}$ be an index such that $u_b = 1$, even after conditioning on all vectors in $\mathcal{A}$ except for $a^{(j,b)}$, the value of $f(\text{Mvec}_J(\mathcal{A}, u))$ (see Equation (6.4)) is still an unbiased Bernoulli random variable purely due to the randomness of the vector $a^{(j,b)} \in \mathbb{F}_2^{E'_j} \otimes \mathbb{F}_2^{E'_j}$. Since $a^{(j,b)}$ is not included in the sub-advice $\mathcal{A}_{[q_0]}$, we conclude that

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [f(\text{Mvec}_J(\mathcal{A}, u)) = 1 \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] = \frac{1}{2}.$$

Case 2: the restriction of f to $\mathbb{F}_2^{E'_c} \otimes \mathbb{F}_2^{E'_c}$ is nonzero for some $c \in J$. As in case 1, we let $b \in \{q_0 + 1, \dots, \ell\}$ be an index such that $u_b \neq 0$. Now let $i = 2^\ell - 2^{\ell-b} - 1$, whose ℓ -bit binary representation has a 0 in the b -th position and 1's in all other positions. Even after conditioning on all vectors in $\mathcal{A}$ except for the $2s$ vectors (none of which is included in the sub-advice $\mathcal{A}_{[q_0]}$)

$$a^{(c, 2si+1)}, a^{(c, 2si+2)}, \dots, a^{(c, 2si+2s)},$$

the value of $f(\text{Mvec}_J(\mathcal{A}, u))$ (see Equations (6.2) and (6.4)) is still the Bernoulli random variable

$$X = \sum_{j=1}^s f(a^{(c, 2si+2j-1)} \otimes a^{(c, 2si+2j)})$$

or its negation. By independence among the vectors in $\mathcal{A}$, it is easy to see that $\mathbb{P}[X = 1]$ lies in the interval $[\frac{1}{2} - 2^{-s-1}, \frac{1}{2} + 2^{-s-1}]$, and hence we have

$$\frac{1}{2} - 2^{-s-1} \leq \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [f(\text{Mvec}_J(\mathcal{A}, u)) = 1 \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] \leq \frac{1}{2} + 2^{-s-1}. \quad \square$$

Recall that if $W \in \text{Gr}(\mathbb{F}_2^n, n - w)$, $L' \in \text{Gr}(W, \ell - 1)$, and we choose an ℓ -dimensional subspace $L \subseteq \mathbb{F}_2^n$ uniformly at random containing L' , then $L \subseteq W$ with probability $2^{-w} + o(1)$. The following proposition establishes an analogous fact, with the notion of sub-advice replacing the containment $L' \subseteq L$.

Proposition 6.22. Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a subset of indices $J \subsetneq [t]$, and positive integers ℓ, s . Let $W \subseteq \mathcal{V}(\mathcal{E}')$ be a linear subspace with codimension w . For any fixed advice sequence $\mathcal{A}' \in \mathcal{A}_J(\mathcal{E}', \ell - 1, 2s)$ such that $\sigma(\mathcal{A}') \subseteq W$, we have

$$2^{-w} - 2^{-s} \leq \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\sigma(\mathcal{A}) \subseteq W \mid \mathcal{A}_{[\ell-1]} = \mathcal{A}'] \leq 2^{-w} + 2^{-s}.$$

Proof. We fix an arbitrary vector $u \in \mathbb{F}_2^\ell \setminus \mathbb{F}_2^{\ell-1}$. Since $\sigma(\mathcal{A}') \subseteq W$ and

$$\sigma(\mathcal{A}) = \sigma(\mathcal{A}_{[\ell-1]}) + \text{span}(\text{Mvec}_J(\mathcal{A}, u)),$$

the desired inequality is equivalent to

$$2^{-w} - 2^{-s} \leq \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\text{Mvec}_J(\mathcal{A}, u) \in W \mid \mathcal{A}_{[\ell-1]} = \mathcal{A}'] \leq 2^{-w} + 2^{-s}. \quad (6.6)$$

Let $\mathcal{F}$ be the collection of linear functionals $f : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$ such that $W \subseteq \ker(f)$, and denote

$$p = \mathbb{E}_{f \in \mathcal{F}} \left[\mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [f(\text{Mvec}_J(\mathcal{A}, u)) = 1 \mid \mathcal{A}_{[\ell-1]} = \mathcal{A}'] \right]. \quad (6.7)$$

Note that $|\mathcal{F}| = 2^w$, and for each $f \in \mathcal{F}$ that is not identically zero we may apply [Proposition 6.21](#) to estimate the probability expression on the right-hand side of [Equation \(6.7\)](#), which yields

$$\frac{2^w - 1}{2^w} \left(\frac{1}{2} - 2^{-s-1} \right) \leq p \leq \frac{2^w - 1}{2^w} \left(\frac{1}{2} + 2^{-s-1} \right). \quad (6.8)$$

On the other hand, by exchanging the expectation and the probability on the right-hand side of [Equation \(6.7\)](#) (i.e. double counting), we have

$$p = \frac{1}{2} \left(1 - \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\text{Mvec}_J(\mathcal{A}, u) \in W \mid \mathcal{A}_{[\ell-1]} = \mathcal{A}'] \right). \quad (6.9)$$

Comparing [Equations \(6.8\)](#) and [\(6.9\)](#) immediately yields the desired [Equation \(6.6\)](#). $\square$

Given $\mathcal{A}' \in \mathcal{A}_J(\mathcal{E}', \ell - 1, 2s)$ such that $\sigma(\mathcal{A}') \subseteq W$, [Proposition 6.22](#) estimates the probability that a random extension $\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)$ of $\mathcal{A}'$ still “stays in” W , in the sense that $\sigma(\mathcal{A}) \subseteq W$. Roughly speaking, this means that “random extension” by 1 dimension from $\sigma(\mathcal{A}_{[\ell-1]})$ to $\sigma(\mathcal{A})$ behaves nicely with respect to zoom-outs. This allows us to iterate the process and show that a random extension by $\ell - q_0$ dimensions from $\sigma(\mathcal{A}_{[q_0]})$ to $\sigma(\mathcal{A})$ also behaves as expected with respect to zoom-outs.

Corollary 6.23. *Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a subset of indices $J \subsetneq [t]$, and positive integers ℓ, s . Let $W \subseteq \mathcal{V}(\mathcal{E}')$ be a linear subspace with codimension w , and suppose that $s \geq \ell + w$. Then for any nonnegative integer $q_0 < \ell$ and any fixed advice sequence $\mathcal{A}' \in \mathcal{A}_J(\mathcal{E}', q_0, 2^{\ell-q_0}s)$ such that $\sigma(\mathcal{A}') \subseteq W$, we have*

$$2^{-w(\ell-q_0)-1} \leq \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\sigma(\mathcal{A}) \subseteq W \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] \leq 2^{-w(\ell-q_0)+1}.$$

Proof. For each $i \in \{q_0, \dots, \ell\}$, let Γ_i denote the event $\{\sigma(\mathcal{A}_{[i]}) \subseteq W\}$.

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\sigma(\mathcal{A}) \subseteq W \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] = \prod_{i=q_0}^{\ell-1} \mathbb{P} [\Gamma_{i+1} \mid \{\mathcal{A}_{[q_0]} = \mathcal{A}'\} \cap \Gamma_i].$$

Since we can apply [Proposition 6.22](#) to every factor on the right-hand side, the conclusion easily follows. Note that the condition $s \geq \ell + w$ guarantees

$$(2^{-w} - 2^{-s})^{\ell-q_0} \geq 2^{-w(\ell-q_0)} (1 - (\ell - q_0)2^{-s+w}) \geq 2^{-w(\ell-q_0)} (1 - 2^{\ell-1-s+w}) \geq 2^{-w(\ell-q_0)-1},$$

and similarly for the upper bound. $\square$

6.2.4 Mixed-Type Grassmann Graph

So far, we have mainly worked with uniformly random mixed-type advice sequences $\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)$, the vectors in which may have linear dependencies (though unlikely). It will be useful later in the analysis of our inner PCP to consider those $\mathcal{A}$ with no linear dependency among their vectors, spanning actual ℓ -dimensional subspaces $\sigma(\mathcal{A}) \subseteq \mathcal{V}(\mathcal{E}')$.

This naturally leads us to the sub-collection $\mathcal{A}_J^*(\mathcal{E}', \ell, s)$ defined in [Definition 6.14](#). For sequences $\mathcal{A} = (A_1, \dots, A_t) \in \mathcal{A}_J^*(\mathcal{E}', \ell, s)$, the lists A_c in the critical blocks $c \in J$ are always saturated, and by [Remark 6.13](#), it follows that $\dim \sigma(\mathcal{A}) = \ell$ (as long as J is nonempty). Therefore, these subspaces $\sigma(\mathcal{A})$ lie in the domain $\text{Gr}(\mathcal{V}(\mathcal{E}'), \ell)$, and they induce a subgraph of the Grassmann graph $\text{Gr}(\mathcal{V}(\mathcal{E}'), \ell)$. We call this subgraph a “mixed-type Grassmann graph,” as defined below.

Definition 6.24. Fix a sequence of finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a nonempty subset of indices $J \subsetneq [t]$ and positive integers ℓ, s . Define $\text{MGr}_J(\mathcal{E}', \ell, s)$ to be the following collection of linear subspaces:

$$\text{MGr}_J(\mathcal{E}', \ell, s) = \{\sigma(\mathcal{A}) \mid \mathcal{A} \in \mathcal{A}_J^*(\mathcal{E}', \ell, s)\} \subseteq \text{Gr}(\mathcal{V}(\mathcal{E}'), \ell).$$

An important fact (whose proof we omit) is that for different subspaces $L \in \text{MGr}_J(\mathcal{E}', \ell, s)$, the number of $\mathcal{A} \in \mathcal{A}_J^*(\mathcal{E}', \ell, s)$ such that $\sigma(\mathcal{A}) = L$ is the same.¹⁶ Therefore, if we sample a uniformly random $\mathcal{A} \in \mathcal{A}_J^*(\mathcal{E}', \ell, s)$, the span $\sigma(\mathcal{A})$ is uniformly random over $\text{MGr}_J(\mathcal{E}', \ell, s)$. The next proposition asserts that even if one chose $\mathcal{A}$ from $\mathcal{A}_J(\mathcal{E}', \ell, s)$, the resulting distribution of $\sigma(\mathcal{A})$ is still close to uniform over $\text{MGr}_J(\mathcal{E}', \ell, s)$, since $|\mathcal{A}_J^*(\mathcal{E}', \ell, s)| = (1 - o(1)) \cdot |\mathcal{A}_J(\mathcal{E}', \ell, s)|$.

Proposition 6.25. Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a nonempty subset of indices $J \subsetneq [t]$, positive integers ℓ, s and a nonnegative integer $q_0 < \ell$. Assume that $|E'_c| \geq 2^{\ell+2}s$ for each $c \in J$. For any fixed advice sequence $\mathcal{A}' \in \mathcal{A}_J^*(\mathcal{E}', q_0, 2^{\ell-q_0}s)$, if we sample $\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)$ conditioned on $\sigma(\mathcal{A}_{[q_0]}) = \sigma(\mathcal{A}')$, the resulting distribution of $\sigma(\mathcal{A})$ has total variation distance at most

$$\sum_{c \in J} 2^{-|E'_c|/2}$$

to the uniform distribution over the set $\{L \in \text{MGr}_J(\mathcal{E}', \ell, s) \mid \sigma(\mathcal{A}') \subseteq L\}$.

Proof. It is not hard to see that if we sample $\mathcal{A} \in \mathcal{A}_J^*(\mathcal{E}', \ell, s)$ conditioned on $\sigma(\mathcal{A}_{[q_0]}) = \sigma(\mathcal{A}')$, the resulting distribution of $\sigma(\mathcal{A})$ is exactly the uniform distribution over $\{L \in \text{MGr}_J(\mathcal{E}', \ell, s) \mid \sigma(\mathcal{A}') \subseteq L\}$. On the other hand, writing $q = 2s(2^\ell - 1)$ and $q_1 = 2s(2^\ell - 2^{\ell-q_0})$, for any $\mathcal{A}' \in \mathcal{A}_J^*(\mathcal{E}', q_0, 2^{\ell-q_0}s)$ we have

$$\begin{aligned} & \mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\mathcal{A} \in \mathcal{A}_J^*(\mathcal{E}', \ell, s) \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] \\ &= \mathbb{P} \left[(a^{(c,1)}, \dots, a^{(c,q)}) \text{ is saturated for each } c \in J \mid \text{fixed saturated sequences } (a^{(c,1)}, \dots, a^{(c,q_1)}) \right] \\ & \quad \text{(where } a^{(c,i)} \text{ (for } c \in J \text{ and } i \in [q]) \text{ are sampled independently and uniformly from } \mathbb{F}_2^{E'_c}) \\ &\geq \prod_{c \in J} \left(1 - 2^{(2^\ell - 1)s - |E'_c|} \right)^2 \geq 1 - \sum_{c \in J} 2^{-|E'_c|/2}. \end{aligned} \quad \square$$

The next proposition asserts that for a valid zoom-in and zoom-out pair Q, W (i.e., $Q \subseteq W$), among the subspaces in $\text{MGr}_J(\mathcal{E}', \ell, s)$ containing Q , the fraction of them contained in W behaves similarly to the standard Grassmann domain.

Proposition 6.26. Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a subset of indices $J \subsetneq [t]$ such that $1 \leq |J| \leq 2$, positive integers ℓ, s and nonnegative integers q_0, w . Assume

$$s \geq \ell + w, \quad q_0 < \ell, \quad \text{and} \quad |E'_c| \geq 2^{\ell+2}s \text{ for each } c \in J.$$

¹⁶To prove that, one needs to use the fact that for any $\mathbb{F}_2$ -vector space V and any $x \in V \otimes V$ of rank s , the number of ways to write $x = a^{(1)} \otimes a^{(2)} + \dots + a^{(2s-1)} \otimes a^{(2s)}$, where $a^{(i)} \in V$ for each $i \in [2s]$, depends only on s .

Then for any fixed subspaces

$$Q \in \text{MGr}_J(\mathcal{E}', q_0, 2^{\ell-q_0}s) \quad \text{and} \quad W \in \text{Gr}(\mathcal{V}(\mathcal{E}'), \dim \mathcal{V}(\mathcal{E}') - w)$$

such that $Q \subseteq W$, we have

$$2^{-w(\ell-q_0)-2} \leq \mathbb{P}_{L \in \text{MGr}_J(\mathcal{E}', \ell, s)} [L \subseteq W \mid Q \subseteq L] \leq 2^{-w(\ell-q_0)+2}.$$

Proof. Pick $\mathcal{A}'$ uniformly at random from the set

$$\left\{ \mathcal{A}' \in \mathcal{A}_J(\mathcal{E}', q_0, 2^{\ell-q_0}s) \mid \sigma(\mathcal{A}') = Q \right\}.$$

It follows from [Proposition 6.25](#) that

$$\left| \mathbb{P}_{L \in \text{MGr}_J(\mathcal{E}', \ell, s)} [L \subseteq W \mid Q \subseteq L] - \mathbb{E}_{\mathcal{A}'} \left[\mathbb{P}_{\mathcal{A} \in \mathcal{A}_J(\mathcal{E}', \ell, s)} [\sigma(\mathcal{A}) \subseteq W \mid \mathcal{A}_{[q_0]} = \mathcal{A}'] \right] \right| \leq \sum_{c \in J} 2^{-|E'_c|/2} \leq 2^{-w\ell-2}.$$

Combining the above with [Corollary 6.23](#) yields the desired conclusion. $\square$

6.2.5 Extension of Agreement

The next somewhat technical result is needed (only) in [Section 6.4.4](#), and to explain it we first give the analog in the simpler Grassmann setting. Suppose we have a table F that assigns to each subspace in $\text{Gr}(\mathbb{F}_2^n, \ell + 1)$ a linear function $F[L]$ (or $\mathbf{nil}$), a subspace $W \subseteq \mathbb{F}_2^n$ of constant codimension, and a linear function $f : W \rightarrow \mathbb{F}_2$ that largely agrees with F in the sense that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell+1)} [f|_{L \cap W} = F[L]|_{L \cap W}] \geq \delta.$$

We wish to extend f into a linear function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ that agrees with F not only on the intersection with W . Then a random extension would suffice: for any L such that $f|_{L \cap W} = F[L]|_{L \cap W}$ we will have that $g|_L = F[L]$ with constant probability. The following lemma establishes an analogous statement in the context of mixed-type subspaces.

Lemma 6.27. *Fix a sequence of non-empty finite sets $\mathcal{E}' = (E'_1, \dots, E'_t)$, a critical index $c \in [t]$, positive integers ℓ, s , nonnegative integers q_0, w and a parameter $\delta \in (0, 1)$. Assume*

$$s \geq 2\ell \quad \text{and} \quad \ell > 2q_0 + 2w.$$

Let $W \subseteq \mathcal{V}(\mathcal{E}')$ be a linear subspace with codimension w , and $Q \subseteq W$ a linear subspace such that $\sigma(\mathcal{A}) = Q$ for some $\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', q_0, 2^{\ell+1-q_0}s)$. Suppose $F[\cdot]$ is a table where $F[L] \in L^ \cup \{\mathbf{nil}\}$ for each linear subspace $L \subseteq \mathcal{V}(\mathcal{E}')$, and there exists a linear function $f : W \rightarrow \mathbb{F}_2$ such that*

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell+1, s)} \left[F[\sigma(\mathcal{A})]|_{\sigma(\mathcal{A}_{[\ell]})} = f|_{\sigma(\mathcal{A}_{[\ell]})} \mid \sigma(\mathcal{A}_{[q_0]}) = Q \text{ and } \sigma(\mathcal{A}_{[\ell]}) \subseteq W \right] \geq \delta. \quad (6.10)$$

Then there exists a subspace $W' \subseteq \mathcal{V}(\mathcal{E}')$ containing W and a linear function $g : W' \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell+1, s)} \left[F[\sigma(\mathcal{A})] = g|_{\sigma(\mathcal{A})} \mid \sigma(\mathcal{A}_{[q_0]}) = Q \text{ and } \sigma(\mathcal{A}) \subseteq W' \right] \geq \frac{\delta}{5}. \quad (6.11)$$

Proof. We let η be the maximum possible value of the left-hand side of Equation (6.11) when W' ranges in the set of linear subspaces containing W and g ranges in $(W')^*$. The goal is to show that $5\eta \geq \delta$. Throughout the proof, we let $L, L' \subseteq \mathcal{V}(\mathcal{E}')$ be random subspaces sampled by the following process:

1. Sample $\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell + 1, s)$ conditioned on $\sigma(\mathcal{A}_{[q_0]}) = Q$.
2. Let $L = \sigma(\mathcal{A}_{[\ell]})$ and $L' = \sigma(\mathcal{A})$.

The most important fact about the joint distribution of (L, L') that we are going to use is the following: conditioned on L' , for any linear subspace such that $Q \subseteq L_0 \subseteq L'$ and $\dim L_0 = \dim L' - 1$, the probability that $L = L_0$ is exactly $(2^{\ell+1-q_0} - 1)^{-1}$.

Let $p = \mathbb{P}[L' \subseteq W]$ and denote

$$\begin{aligned}\gamma_0 &= \mathbb{P}\left[F[L'] = f|_{L'} \mid L' \subseteq W\right], \\ \gamma_1 &= \mathbb{P}\left[F[L']|_Q = f|_Q \text{ but } F[L'] \neq f|_{L'} \mid L' \subseteq W\right].\end{aligned}$$

By the definitions of γ_0 and η , we immediately have $\eta \geq \gamma_0$. Furthermore, by picking a random $g : W \rightarrow \mathbb{F}_2$ conditioned on $g|_Q = f|_Q$, we have

$$\mathbb{E}_g \left[\mathbb{P}\left[F[L'] = g|_{L'} \text{ and } L' \subseteq W\right] \right] \geq 2^{-(\ell+1-q_0)} \cdot (\gamma_0 p + \gamma_1 p),$$

and hence

$$\eta \geq \mathbb{E}_g \left[\mathbb{P}\left[F[L'] = g|_{L'} \mid L' \subseteq W\right] \right] \geq 2^{-(\ell+1-q_0)} \cdot (\gamma_0 + \gamma_1). \quad (6.12)$$

We denote by $\mathcal{W}$ the collection of linear subspaces $W' \subseteq \mathcal{V}(\mathcal{E}')$ such that $\dim W' = 1 + \dim W$ and $W \subseteq W'$. For each $W' \in \mathcal{W}$, we let

$$\begin{aligned}p_{W'} &= \mathbb{P}\left[L' \subseteq W' \text{ but } L' \not\subseteq W\right], \text{ and} \\ \gamma_{W'} &= \begin{cases} \mathbb{P}\left[F[L']|_{L' \cap W} = f|_{L' \cap W} \mid L' \subseteq W' \text{ but } L' \not\subseteq W\right], & \text{if } p_{W'} > 0 \\ 0, & \text{if } p_{W'} = 0. \end{cases}\end{aligned}$$

For each $W' \in \mathcal{W}$, there are exactly two linear extensions of f to W' . If we choose $g : W' \rightarrow \mathbb{F}_2$ to be a uniformly random one of the two, then it is easy to see that

$$\mathbb{E}_g \left[\mathbb{P}\left[F[L'] = g|_{L'} \text{ and } L' \subseteq W'\right] \right] = \gamma_0 p + \frac{1}{2} \gamma_{W'} p_{W'},$$

and hence

$$\eta \geq \mathbb{E}_g \left[\mathbb{P}\left[F[L'] = g|_{L'} \mid L' \subseteq W'\right] \right] = \frac{\gamma_0 p + \gamma_{W'} p_{W'}/2}{p + p_{W'}}. \quad (6.13)$$

It is not hard to see that

$$\mathbb{P}[L \subseteq W] = p + \frac{1}{2^{\ell+1-q_0} - 1} \sum_{W' \in \mathcal{W}} p_{W'}, \quad (6.14)$$

and furthermore,

$$\mathbb{P}\left[F[L']|_L = f|_L \text{ and } L \subseteq W\right]$$

$$\begin{aligned}
&= \gamma_0 p + \frac{1}{2^{\ell+1-q_0} - 1} \left(\gamma_1 p + \sum_{W' \in \mathcal{W}} \gamma_{W'} p_{W'} \right) \\
&\leq \gamma_0 p + 2 \cdot 2^{-(\ell+1-q_0)} \cdot (\gamma_0 + \gamma_1) p + \frac{2}{2^{\ell+1-q_0} - 1} \sum_{W' \in \mathcal{W}} \left(\gamma_0 p + \frac{1}{2} \gamma_{W'} p_{W'} \right) \\
&\leq 3\eta \cdot p + 2\eta \cdot \frac{1}{2^{\ell+1-q_0} - 1} \sum_{W' \in \mathcal{W}} (p + p_{W'}) \quad (\text{using } \gamma_0 \leq \eta \text{ and Equations (6.12) and (6.13)}) \\
&\leq 5\eta \cdot \mathbb{P}[L \subseteq W]. \quad (\text{using Equation (6.14) and } |\mathcal{W}| = 2^w - 1 \leq 2^{\ell+1-q_0} - 1)
\end{aligned}$$

This gives the desired inequality

$$5\eta \geq \mathbb{P} \left[F[L']|_L = f|_L \mid L \subseteq W \right] \geq \delta,$$

where we used Equation (6.10) in the last transition. $\square$

6.3 The 4-to-1 Game Construction

In this subsection, we use the framework prepared in Sections 6.1 and 6.2 to construct our final sub-4-to-1 game. Before defining the sub-4-to-1 game, we first rewrite the description of Game2b (defined in Section 5.4) using the notations introduced in Sections 6.1 and 6.2.

Definition 6.28. Let H be a 3-uniform hypergraph. Given positive integers k and t , we let $\mathcal{E}(H, k, t)$ denote the collection of all sequences $\mathcal{E} = (E_1, \dots, E_t)$ such that $E_j \in \mathcal{E}(H, k)$ for all $j \in [t]$.

We can now rewrite the definition of Game2b[$H, k, \ell_2, t, q_0, q_1, \beta$] as follows.

Definition 6.29. Given positive integers k, ℓ_2, t, s_1 , a nonnegative integer q_0 , a parameter $\beta \in [0, 1)$ and a 3-uniform hypergraph H , let Game2c[$H, k, \ell_2, t, s_1, q_0, \beta$] be a 2-prover 1-round game where the verifier executes the following:

1. Sample a uniformly random sequence $\mathcal{E} = (E_1, \dots, E_t) \in \mathcal{E}(H, k, t)$.
2. Sample $(c, \mathcal{U}, \mathcal{E}', \mathcal{U}') \sim \mathcal{J}_{\text{in}}(\mathcal{E}, \beta, \ell_2)$.
3. Sample a uniformly random sequence $\mathcal{A} = (A_1, \dots, A_t) \in \mathcal{A}_c(\mathcal{E}', q_0, s_1)$.¹⁷
4. Send $(\mathcal{E}, \mathcal{A}, \mathcal{U})$ to Alice and $(c, \mathcal{E}', \mathcal{A}, \mathcal{U}')$ to Bob.
5. Alice must return a linear map $f : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ such that $f|_{\mathcal{N}(\mathcal{E}, \mathcal{U})}$ is SNR-satisfying; Bob must return a linear map $g : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$. Accept if $f|_{\mathcal{V}(\mathcal{E}')} = g$.

It is easy to observe that Definition 6.29 defines the same game as substituting $q_1 = 2s_1(2^{q_0} - 1)$ in Definition 5.20 does.

Proposition 6.30. For any positive integers k, ℓ_2, t, s_1 , nonnegative integer q_0 , parameter $\beta \in [0, 1)$ and 3-uniform hypergraph H , we have

$$\text{val}(\text{Game2b}[H, k, \ell_2, t, q_0, 2s_1(2^{q_0} - 1), \beta]) = \text{val}(\text{Game2c}[H, k, \ell_2, t, s_1, q_0, \beta]).$$

¹⁷If $q_0 = 0$, we take $\mathcal{A} = \text{empty}$ to be an empty sequence.

Proof. It is easy to see the equivalence between Game2b and Game2c by comparing Definitions 5.20 and 6.29. $\square$

We are now ready to define our sub-4-to-1 game based on Game2c. The main idea here is that instead of providing the functions f, g fully as in the game in Game2c, the provers are expected to provide an encoding of them based on the mixed-type Grassmann graph. More specifically, each player receives a linear subspace of their ambient space, and is requested to respond by a linear function on it. In order to make the game sub-4-to-1, the subspace Alice receives is contained in the subspace Bob receives and is of 1 less dimension, and additionally we incorporate inside it the local tensor tests as well as the side-condition equations.

Definition 6.31. Given positive integers k, ℓ_1, ℓ_2, t, s , a parameter $\beta \in [0, 1)$ and a 3-uniform hypergraph H , let $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$ be a 2-prover 1-round game where the verifier executes the following:

1. Sample a uniformly random sequence $\mathcal{E} = (E_1, \dots, E_t) \in \mathcal{E}(H, k, t)$.
2. Sample $(c, \mathcal{U}, \mathcal{E}', \mathcal{U}') \sim \mathcal{J}_{\text{in}}(\mathcal{E}, \beta, \ell_2)$.
3. Sample a uniformly random sequence $\mathcal{A} = (A_1, \dots, A_t) \in \mathcal{A}_c(\mathcal{E}', 2\ell_1, s)$. Let

$$L = \sigma(\mathcal{A}_{[\ell_1]}) \subseteq \mathcal{V}(\mathcal{E}') \quad \text{and} \quad L' = \sigma(\mathcal{A}_{[\ell_1+1]}) \subseteq \mathcal{V}(\mathcal{E}').$$

4. Send $(\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U}))$ to Alice and $(c, \mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}')$ to Bob.
5. Alice must return a linear map $f : (L + \mathcal{N}(\mathcal{E}, \mathcal{U})) \rightarrow \mathbb{F}_2$ such that $f|_{\mathcal{N}(\mathcal{E}, \mathcal{U})}$ is SNR-satisfying; Bob must return a linear map $g : (L' + \bigoplus \mathcal{U}') \rightarrow \mathbb{F}_2$ such that $g|_{\bigoplus \mathcal{U}'}$ is SR-satisfying. Accept if $g|_{(L + \bigoplus \mathcal{U})} = f|_{(L + \bigoplus \mathcal{U})}$.

The game defined in Definition 6.31 is clearly a sub-4-to-1 game, in the sense that for any response of Alice there are at most 4 responses for Bob which would make the verifier accept. We will make a more formal argument at the end of this subsection.

The completeness of Game3 is straightforward and is given in the following lemma.

Lemma 6.32 (Game3 completeness). *For any positive integers k, ℓ_1, ℓ_2, t, s , a parameter $\beta \in [0, 1)$ and a 2-colorable 3-uniform hypergraph H , we have*

$$\text{val}(\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]) = 1.$$

Proof. By Lemma 5.21 and Proposition 6.30, there is a set of strategies for Alice and Bob that achieve value 1 in $\text{Game2c}[H, k, \ell_2, t, s_1, 0, \beta]$ (here we may take $s_1 = 1$, but it is irrelevant anyway). Note that since the second-to-last parameter in $\text{Game2c}[H, k, \ell_2, t, s_1, 0, \beta]$ is set to be zero, there is no advice in this game. Suppose the strategies are represented by a table $F[\cdot]$ for Alice and a table $G[\cdot]$ for Bob, where $F[\mathcal{E}, \mathcal{U}] : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ is a linear map for each Alice-question $(\mathcal{E}, \mathcal{U})$, and $G[c, \mathcal{E}', \mathcal{U}'] : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$ is a linear map for each Bob-question $(c, \mathcal{E}', \mathcal{U}')$.

We can then construct a strategy for Alice in the game $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$ as follows:

1. Receive the question $(\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U}))$.
2. Let f be the restriction of $F[\mathcal{E}, \mathcal{U}]$ to $L + \mathcal{N}(\mathcal{E}, \mathcal{U})$, and return f . Note that by Definition 6.29, the restriction of $F[\mathcal{E}, \mathcal{U}]$ to $\mathcal{N}(\mathcal{E}, \mathcal{U})$ must be SNR-satisfying.

Similarly, the strategy for Bob is:

1. Receive the question $(c, \mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}')$.
2. Let g be the restriction of $G[c, \mathcal{E}', \mathcal{U}']$ to $L' + \bigoplus \mathcal{U}'$, and return g . Although the definition of **Game2c** itself does not require the restriction $G[c, \mathcal{E}', \mathcal{U}']|_{\bigoplus \mathcal{U}'}$ to be SR-satisfying, the way we constructed $G[\cdot]$ does lead to SR-satisfying restrictions (see [Remark 4.26](#)).

Since we always have $F[\mathcal{E}, \mathcal{U}]|_{\mathcal{V}(\mathcal{E}')} = G[c, \mathcal{E}', \mathcal{U}']$, it is clear that we also have $f|_{(L + \bigoplus \mathcal{U})} = g|_{(L + \bigoplus \mathcal{U})}$. Moreover, we choose F, G to be the strategies induced from the proper 2-coloring of the original graph through the series of reductions. The strategies are symmetric and have rank at most 1 restricted to each block. Therefore, under this set of strategies, the verifier of **Game3** $[H, k, \ell_1, \ell_2, t, s, \beta]$ accepts with probability 1. $\square$

The soundness of **Game3** is stated in the following lemma.

Lemma 6.33 (Game3 soundness). *Assume [Condition 3.12](#). Suppose that in every 4^r -coloring of H , at least ε fraction of the edges are monochromatic. Then we have*

$$\text{val}\left(\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]\right) \leq \delta.$$

The proof of [Lemma 6.33](#) is significantly more involved, and will be completed in [Section 6.4](#). We first assume this soundness lemma and prove the main theorem ([Theorem 3.3](#), restated below).

Theorem 3.3. *For any $\delta \in (0, 1)$, there exists a positive integer N such that $\text{GapS-4-to-1}_N(1, \delta)$ is NP-hard.*

Proof assuming [Lemma 6.33](#). Without loss of generality, assume $\delta < 1/2$. Using the parameters in [Condition 3.12](#), we show a polynomial-time reduction from the gap problem in [Theorem 3.4](#) (with the number of colors $c = 4^r$) to $\text{GapS-4-to-1}_N(1, \delta)$, for $N = 2^{\ell_2 t + \ell_1 + 2}$.

The reduction runs as follows: given a 3-uniform hypergraph H , we construct the 2-prover 1-round game **Game3** $[H, k, \ell_1, \ell_2, t, s, \beta]$, which is viewed as a label-cover instance.¹⁸ By the definition of **Game3** ([Definition 6.31](#)), this label-cover instance can be constructed in $\text{poly}(n)$ time, where n is the size of H . The completeness and soundness of the reduction are already given by [Lemmas 6.32](#) and [6.33](#), respectively. It only remains to show that **Game3** $[H, k, \ell_1, \ell_2, t, s, \beta]$ is always a sub-4-to-1 game.

As in [Definition 6.31](#), consider a question $L + \mathcal{N}(\mathcal{E}, \mathcal{U})$ sent to Alice and a question $L' + \bigoplus \mathcal{U}'$ sent to Bob.

Given any possible response $g : (L' + \bigoplus \mathcal{U}') \rightarrow \mathbb{F}_2$ of Bob, if Alice's response $f : (L + \mathcal{N}(\mathcal{E}, \mathcal{U})) \rightarrow \mathbb{F}_2$ makes the verifier accept, the restriction $f|_{L + \bigoplus \mathcal{U}}$ must be the fixed function $g|_{L + \bigoplus \mathcal{U}}$. Furthermore, by [Proposition 6.2](#) and [Definition 6.7](#), any linear functional on $\bigoplus \mathcal{U}$ has at most one SNR-satisfying extension to $\mathcal{N}(\mathcal{E}, \mathcal{U})$. Therefore, there exists at most one extension of $g|_{L + \bigoplus \mathcal{U}}$ to $(L + \mathcal{N}(\mathcal{E}, \mathcal{U}))$ that has an SNR-satisfying restriction on $\mathcal{N}(\mathcal{E}, \mathcal{U})$.

Conversely, given any possible response $f : (L + \mathcal{N}(\mathcal{E}, \mathcal{U})) \rightarrow \mathbb{F}_2$ of Alice, we claim that there are at most 4 possible responses $g : (L' + \bigoplus \mathcal{U}') \rightarrow \mathbb{F}_2$ of Bob that make the verifier accept. Indeed, in order to pass the verifier's test, the restriction $g|_{L + \bigoplus \mathcal{U}}$ must be the fixed function $f|_{L + \bigoplus \mathcal{U}}$. Since $\mathcal{U}' = (U'_1, \dots, U'_t)$ differs from $\mathcal{U} = (U_1, \dots, U_t)$ in only one critical block c , for which $\dim U'_c$ is larger than $\dim U_c$ by at most 1, we know that $f|_{\bigoplus \mathcal{U}}$ has at most 2 extensions to $\bigoplus \mathcal{U}'$ that are SR-satisfying. Since $\dim L'$ is larger than $\dim L$ by at most 1, we know that $f|_L$ has at most 2 linear extensions to L' . Therefore, $f|_{L + \bigoplus \mathcal{U}}$ has at most 4 extensions to $L' + \bigoplus \mathcal{U}'$ that have an SR-satisfying restriction on $\bigoplus \mathcal{U}'$. $\square$

¹⁸For the standard translation between 2-prover 1-round games and label-cover instances, see the discussion at the beginning of [Section 2.1.1](#).

6.4 Soundness Analysis

The goal of this subsection is to prove [Lemma 6.33](#). Throughout this subsection, we fix a 3-uniform hypergraph H , positive integers k, ℓ_1, ℓ_2, t, s , a nonnegative integer q_0 and a parameter $\beta \in (0, 1)$. We consider the game $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$ as defined in [Definition 6.31](#).

At a high-level, the proof of [Lemma 6.33](#) proceeds in four steps:

1. **Constructing tables:** recall that for each question $(\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U}))$ to Alice, her response is a linear function $L + \mathcal{N}(\mathcal{E}, \mathcal{U}) \rightarrow \mathbb{F}_2$ which, in particular, restricts to a linear function $L \rightarrow \mathbb{F}_2$. For each fixed pair $(\mathcal{E}, \mathcal{U})$, these responses uniquely determine a table $F[\mathcal{E}, \mathcal{U}, \cdot]$ that assigns to each linear subspace $L \subseteq \mathcal{V}(\mathcal{E})$ either an element of L^* or nil . Similarly, for each fixed pair $(\mathcal{E}', \mathcal{U}')$, we record Bob's responses in a table $G[\mathcal{E}', \mathcal{U}', \cdot]$.
2. **Decoding strategy for Alice:** our first goal is to use the consistency between $F[\cdot]$ and $G[\cdot]$, together with the Cauchy–Schwarz inequality as in [Lemma 5.15](#), to show that, on average, $F[\mathcal{E}, \mathcal{U}, \cdot]$ passes the Grassmann agreement test with noticeable probability. Because of the critical coordinate, the distribution of L induced by the construction is not exactly uniform over $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$. Nevertheless, lazy parallel repetition ensures that this distribution is close to uniform; we refer to this fact as the *covering property of mixed-type subspaces*.

Applying the Grassmann decoding theorem ([Theorem 3.5](#)) then yields a family $\mathcal{Q}$ of constant-dimensional zoom-ins in $\mathcal{V}(\mathcal{E})$ of noticeable relative size. For each $Q \in \mathcal{Q}$, there is a zoom-out $W \subseteq \mathcal{V}(\mathcal{E})$ of constant codimension and a global linear function $f_{\mathcal{E}, \mathcal{U}, Q, W}: W \rightarrow \mathbb{F}_2$ such that $F[\mathcal{E}, \mathcal{U}, L] = f_{\mathcal{E}, \mathcal{U}, Q, W}|_L$ for a noticeable fraction of the ℓ_1 -dimensional subspaces L satisfying $Q \subseteq L \subseteq W$.

Alice uses this observation to construct her strategy in Game2c . More precisely, she chooses Q using her advice, and chooses W for which a global linear function as above exists. Strictly speaking, she has to choose W to be inclusion-maximal among the subspaces with this property; this is to ensure (via [Lemma 3.9](#)) that for a fixed Q , the list of possible answers Alice may give is small.

3. **Decoding strategy for Bob:** for fixed $\mathcal{E}'$ and $\mathcal{U}'$, the distribution of L' induced by the construction is not close to uniform over $\text{Gr}(\mathcal{V}(\mathcal{E}'), \ell_1 + 1)$, but only close to uniform over the mixed-type Grassmann domain $\text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1}s)$. Unlike in Alice's case, for this mixed-type Grassmann domain we have neither a decoding theorem like [Theorem 3.5](#) nor a list-decoding bound like [Lemma 3.9](#). To argue that Bob can still construct a strategy for Game2c from his table $G[\mathcal{E}', \mathcal{U}', \cdot]$, we utilize the consistency between $F[\cdot]$ and $G[\cdot]$ to show that Alice's decoding is often also good for Bob.
4. **Consistency of decodings:** the preceding step only established that Alice's decoding has noticeable agreement with Bob's table $G[\cdot]$. It does not guarantee that Bob can actually decode from $G[\cdot]$ a global function compatible with Alice's decoding. This is because there may be a very large number of global linear functions that have noticeable agreement with $G[\mathcal{E}', \mathcal{U}', \cdot]$, and Bob may not be able to identify the one that corresponds to Alice's decoding: the preceding step guarantees only that such a function exists.

The usual approach is to bound the number of global linear functions with noticeable agreement with $G[\mathcal{E}', \mathcal{U}', \cdot]$. If this were an ordinary Grassmann table, [Lemma 3.9](#) would provide the desired bound. However, our $G[\mathcal{E}', \mathcal{U}', \cdot]$ is defined on a mixed-type Grassmann domain, for which we do not have an analogous list-decoding bound, although we expect one to hold.

We work around this issue by exploiting the consistency between $F[\cdot]$ and $G[\cdot]$ a second time. Without bounding the number of possible decodings Bob may choose from, we let Bob choose an arbitrary global function from his potentially unbounded list, and then “transfer” his decoding back to Alice’s side. Roughly speaking, we argue that whichever global functions Bob chooses for the pairs $(\mathcal{E}', \mathcal{U}')$, a noticeable fraction of them will “appear” in Alice’s list (of possible decodings from $F[\cdot]$) for some $(\mathcal{E}, \mathcal{U})$. Since Alice’s lists have bounded size by [Lemma 3.9](#), she can select the correct candidates (i.e. those that are transferred from Bob’s side) with probability bounded away from zero.

The downside is that it is harder to “transfer” decodings back from Bob to Alice (than we did from Alice to Bob). The primary reason is that Bob’s decoded global functions are defined on $\mathcal{V}(\mathcal{E}')$, which is smaller than Alice’s space $\mathcal{V}(\mathcal{E})$ (by quite a lot). A single decoded function $g: \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$ is therefore insufficient for such a transfer. Instead, we use the fact that Bob has chosen a decoding for *every* suitable pair $(\mathcal{E}', \mathcal{U}')$. We show that sufficiently many of these decodings, corresponding to different pairs $(\mathcal{E}', \mathcal{U}')$, can be patched together into a linear function $\mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ and *jointly* transferred to Alice’s table $F[\mathcal{E}, \mathcal{U}, \cdot]$.

6.4.1 Notation Setup

We begin by setting up some notational conventions that will be used throughout [Section 6.4](#). We will use the following abuse of notation:

Notation 6.34. Recall that in [Definition 6.31](#), the sequence $\mathcal{E}' = (E'_1, \dots, E'_t)$ is a c -critical descendant (see [Definition 6.8](#)) of $\mathcal{E}$. It is not necessarily the case that one can tell the critical coordinate c from $\mathcal{E}'$ itself: when $|E'_c|$ happens to be $3k$ (although this happens with only a very small probability), the sequence $\mathcal{E}'$ is equal to $\mathcal{E}$. However, in the rest of the proof, we assume that the critical coordinate is implicit in the notation $\mathcal{E}'$. For instance, in [Game2c](#), the question sent to Bob can be written as $(\mathcal{E}', \mathcal{A}, \mathcal{U}')$.

The next two notational definitions below are parallels of [Notations 5.11](#) and [5.12](#) in [Section 5.3](#).

Notation 6.35. We use $\mathcal{D}_{\text{in}}$ to denote the joint distribution of $(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A})$ sampled by the verifier in [Game3](#) $[H, k, \ell_1, \ell_2, t, s, \beta]$. We also need a variant of $\mathcal{D}_{\text{in}}$ where the five components are expanded into seven components: denote $\mathcal{D}_{\text{in}}^+$ to be the joint distribution of $(\mathcal{E}, \mathcal{U}, L, Q, \mathcal{E}', \mathcal{U}', L')$, where $(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A})$ is sampled from $\mathcal{D}_{\text{in}}$ and

$$Q := \sigma(\mathcal{A}_{[q_0]}), \quad L := \sigma(\mathcal{A}_{[\ell_1]}), \quad L' = \sigma(\mathcal{A}_{[\ell_1+1]}).$$

We use the symbol $*$ to denote marginalization over the corresponding component. For instance, sampling from the marginal distribution of $(\mathcal{U}, \mathcal{E}')$ under $\mathcal{D}_{\text{in}}$ is denoted by $(*, \mathcal{U}, \mathcal{E}', *, *) \sim \mathcal{D}_{\text{in}}$.

Notation 6.36. We will often condition the distribution $\mathcal{D}_{\text{in}}$ on some subset of the five components $(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A})$ and consider the induced joint distribution of the remaining components. For instance, if $\mathcal{E}$ and $\mathcal{U}'$ are fixed, then the conditional joint distribution of $(\mathcal{U}, \mathcal{E}')$ is denoted by

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}} [\cdot \mid \mathcal{E}, \mathcal{U}'] .$$

Similar conditioning notation will be used for the seven-component joint distribution $\mathcal{D}_{\text{in}}^+$.

The notions of *Alice-table* and *Bob-table* to be defined in [Notation 6.38](#) are slightly more nuanced than their counterparts in [Notation 5.13](#). In particular, the entries of an Alice-table do not exactly correspond to the possible questions Alice may receive.

Notation 6.37. For any possible sample $(\mathcal{E}, \mathcal{U}, *, *, *) \sim \mathcal{D}_{\text{in}}$, the pair $(\mathcal{E}, \mathcal{U})$ is called an *Alice-packet*. Similarly, a pair $(\mathcal{E}', \mathcal{U}')$ is called a *Bob-packet* if $(*, *, \mathcal{E}', \mathcal{U}', *)$ has nonzero probability under $\mathcal{D}_{\text{in}}$. For any possible sample $(\mathcal{E}, \mathcal{U}, L, *, *, *, *) \sim \mathcal{D}_{\text{in}}^+$, the tuple $(\mathcal{E}, \mathcal{U}, L)$ is called an *unfolded-Alice-question*. Similarly, a tuple $(\mathcal{E}', \mathcal{U}', L')$ is called an *unfolded-Bob-question* if $(*, *, *, *, \mathcal{E}', \mathcal{U}', L')$ has nonzero probability under $\mathcal{D}_{\text{in}}^+$.

Notation 6.38. A table $F[\cdot]$ is called an Alice-table if for each Alice-packet $(\mathcal{E}, \mathcal{U})$ and each linear subspace $L \subseteq \mathcal{V}(\mathcal{E})$, the entry $F[\mathcal{E}, \mathcal{U}, L]$ is either `nil` or a linear functional $F[\mathcal{E}, \mathcal{U}, L] : L \rightarrow \mathbb{F}_2$. Similarly, a table $G[\cdot]$ is called a Bob-table if for each Bob-packet $(\mathcal{E}', \mathcal{U}')$ and each linear subspace $L' \subseteq \mathcal{V}(\mathcal{E}')$, the entry $G[\mathcal{E}', \mathcal{U}', L']$ is either `nil` or a linear functional $G[\mathcal{E}', \mathcal{U}', L'] : L' \rightarrow \mathbb{F}_2$.

The following definition is a parallel of [Notation 5.14](#).

Notation 6.39. Fix an Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$. For any tuple $(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L')$ with nonzero probability under $\mathcal{D}_{\text{in}}^+$, we define

$$\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') = \begin{cases} 1, & \text{if } G[\mathcal{E}', \mathcal{U}', L']|_L = F[\mathcal{E}, \mathcal{U}, L], \\ 0, & \text{otherwise.} \end{cases}$$

We will often sample $(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L')$ from $\mathcal{D}_{\text{in}}^+$ conditioned on some subset of its components. For instance, if $\mathcal{E}$ and $\mathcal{U}'$ are fixed, then the conditional expectation of $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L')$ is denoted by

$$\text{Vrf}_{F,G}(\mathcal{E}, *, *, *, \mathcal{U}', *) = \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[G[\mathcal{E}', \mathcal{U}', L']|_L = F[\mathcal{E}, \mathcal{U}, L] \mid \mathcal{E}, \mathcal{U}' \right].$$

When none of the components is fixed, we write $\text{Vrf}_{F,G} = \text{Vrf}_{F,G}(*, *, *, *, *, *)$ for short.

6.4.2 Covering Property of Mixed-Type Subspaces

Note that in [Definition 6.31](#), the subspace L sent to Alice is not uniformly chosen from her space $\mathcal{V}(\mathcal{E})$, and instead it is chosen from $\mathcal{V}(\mathcal{E}')$ with a random critical coordinate c . For the test we perform to make sense from Alice's perspective (as well as for the advice feature we arranged to work) it is crucial that the distribution of L is statistically close to being uniform over subspaces of her ambient space. The following definition and lemma make this assertion more precise, and in fact they show that the two distributions are close even conditioning on a small number of fixed vectors being contained in L .

Definition 6.40. For a fixed Alice-packet $(\mathcal{E}, \mathcal{U})$ and a sequence of vectors

$$B = (a^{(1)}, \dots, a^{(q_0)}) \in (\mathcal{V}(\mathcal{E}))^{q_0},$$

let $\text{TVD}_{\mathcal{E}, \mathcal{U}}(B)$ denote the total variation distance between

- (1) the distribution of $\rho(\mathcal{A})$ when $(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ is sampled conditioned on the fixed Alice-packet $(\mathcal{E}, \mathcal{U})$ and the event $\{\rho(\mathcal{A}_{[q_0]}) = B\}$ (if this event happens with zero probability, let $\text{TVD}_{\mathcal{E}, \mathcal{U}}(B) = 1$); and
- (2) the uniform distribution over the set

$$\left\{ (a^{(1)}, \dots, a^{(q_0)}, b^{(q_0+1)}, \dots, b^{(2\ell_1)}) \mid b^{(q_0+1)}, \dots, b^{(2\ell_1)} \in \mathcal{V}(\mathcal{E}) \right\} \subseteq (\mathcal{V}(\mathcal{E}))^{2\ell_1}.$$

Lemma 6.41. Assume [Condition 3.12](#). For any fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, we have

$$\mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E}, \mathcal{U}}(\rho(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \leq t^{-1/3}.$$

Proof. Towards the goal of applying [Proposition F.1](#), we set up some notation. Write

$$\mathcal{E} = (E_1, \dots, E_t) \quad \text{and} \quad \mathcal{U} = (U_1, \dots, U_t).$$

For each $j \in [t]$, define sets $\mathcal{A}_j, \mathcal{B}_j$ and a map $\pi_j : \mathcal{A}_j \rightarrow \mathcal{B}_j$ by

$$\begin{aligned} \mathcal{A}_j &= \left\{ (a^{(1)}, \dots, a^{(2\ell_1)}) \mid a^{(i)} \in \mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \text{ for each } i \in [2\ell_1] \right\} = \left(\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \right)^{2\ell_1}, \\ \mathcal{B}_j &= \left(\mathbb{F}_2^{E_j} \otimes \mathbb{F}_2^{E_j} \right)^{q_0}, \quad \text{and} \quad \pi_j : (a^{(1)}, \dots, a^{(2\ell_1)}) \mapsto (a^{(1)}, \dots, a^{(q_0)}). \end{aligned}$$

For each $j \in [t]$, let μ_j be the output distribution of the following process:

1. Sample $E'_j \sim \mathcal{J}_{\text{rev}}(E_j, U_j, \beta, \ell_2)$.
2. Pick $q = 2(2^{2\ell_1} - 1)s$ vectors $a^{(j,1)}, \dots, a^{(j,q)}$ from $\mathbb{F}_2^{E'_j}$ independently and uniformly at random. Let $A = (a^{(j,1)}, \dots, a^{(j,q)})$.
3. Output the sequence

$$(\text{Lvec}(A, 2\ell_1, e_1), \dots, \text{Lvec}(A, 2\ell_1, e_{2\ell_1})) \in \mathcal{A}_j,$$

where $e_1, \dots, e_{2\ell_1} \in \mathbb{F}_2^{2\ell_1}$ are the standard basis vectors.

We can then define a distribution μ over $\prod_{j=1}^t \mathcal{A}_j$ as in the statement of [Proposition F.1](#); it is easy to see (using [Proposition 6.10](#)) that μ is identical to the distribution of $\rho(\mathcal{A})$ when $(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ is sampled conditioned on $(\mathcal{E}, \mathcal{U})$.

Now we can apply [Proposition F.1](#) to $\mathcal{A}_j, \mathcal{B}_j, \pi_j$ and μ_j as defined above. The conclusion of [Proposition F.1](#) says that

$$\mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E}, \mathcal{U}}(\rho(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \leq \sqrt{\frac{2^{18k^2\ell_1}}{4t}} \leq t^{-1/3},$$

where we used [Condition 3.12](#) in the last transition. $\square$

While [Definition 6.40](#) deals with the vector list $\rho(\mathcal{A})$, we eventually need to study Alice's space L , which is spanned by the first ℓ_1 vectors in $\rho(\mathcal{A})$. The next definition is a variation of [Definition 6.40](#) that directly addresses the distribution of L (the reason we started with [Definition 6.40](#) was purely to facilitate the application of [Proposition F.1](#) in [Lemma 6.41](#)).

Definition 6.42. For a fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, a linear subspace $Q \subseteq \mathcal{V}(\mathcal{E})$ and a linear subspace $W \subseteq \mathcal{V}(\mathcal{E})$ containing Q , let $\text{TVD}_{\mathcal{E}, \mathcal{U}, W}(Q)$ be the total variation distance between

- (1) the distribution of $\sigma(\mathcal{A}_{[\ell_1]})$ when $(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ is sampled conditioned on the fixed Alice-packet $(\mathcal{E}, \mathcal{U})$ and the event $\{\sigma(\mathcal{A}_{[q_0]}) = Q\} \cap \{\sigma(\mathcal{A}_{[\ell_1]}) \subseteq W\}$ (if this event happens with zero probability, let $\text{TVD}_{\mathcal{E}, \mathcal{U}, W}(Q) = 1$); and
- (2) the uniform distribution over the set $\{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1) \mid Q \subseteq L \subseteq W\}$.

If $W = \mathcal{V}(\mathcal{E})$, we omit the subscript W and write $\text{TVD}_{\mathcal{E},\mathcal{U}}(Q) = \text{TVD}_{\mathcal{E},\mathcal{V}(\mathcal{E})}(Q)$.

The following three lemmas about [Definition 6.42](#) are easy to prove.

Lemma 6.43. Assume [Condition 3.12](#). Fix an Alice-packet $(\mathcal{E}, \mathcal{U})$, a linear subspace $Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)$ and a linear subspace $W \subseteq \mathcal{V}(\mathcal{E})$ containing Q . Let $w = \text{codim } W$, and suppose $\dim W \geq \ell_1$. We always have

$$\text{TVD}_{\mathcal{E},\mathcal{U},W}(Q) \leq 2^{\ell_1(w+1)} \cdot \text{TVD}_{\mathcal{E},\mathcal{U}}(Q).$$

Proof. This is simply due to

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} [L \subseteq W \mid Q \subseteq L] \geq 2^{-\ell_1(w+1)}. \quad \square$$

Lemma 6.44. Fix an Alice-packet $(\mathcal{E}, \mathcal{U})$ and a linear subspace $Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)$. We have

$$\text{TVD}_{\mathcal{E},\mathcal{U}}(Q) \leq \mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E},\mathcal{U}}(\rho(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \text{ and } \{\sigma(\mathcal{A}_{[q_0]}) = Q\} \right] + 2^{\ell_1 - 9k^2t}.$$

Proof. Use the following fact to pass from the uniform distribution over $(\mathcal{V}(\mathcal{E}))^{\ell_1}$ to the uniform distribution over $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$: for any sequence of vectors $B = (a^{(1)}, \dots, a^{(q_0)}) \in (\mathcal{V}(\mathcal{E}))^{q_0}$ such that $\text{span}(B) = Q$, if $b^{(q_0+1)}, \dots, b^{(\ell_1)} \in \mathcal{V}(\mathcal{E})$ are sampled independently and uniformly at random, the probability that $a^{(1)}, \dots, a^{(q_0)}, b^{(q_0+1)}, \dots, b^{(\ell_1)}$ are not linearly independent is at most $2^{\ell_1 - 9k^2t}$. $\square$

Lemma 6.45. Assume [Condition 3.12](#). For any fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, we have

$$\mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E},\mathcal{U}}(\sigma(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \leq t^{-1/4}.$$

Proof. Using [Lemma 6.44](#) followed by [Lemma 6.41](#), we have

$$\begin{aligned} & \mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E},\mathcal{U}}(\sigma(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \\ & \leq \mathbb{E}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{TVD}_{\mathcal{E},\mathcal{U}}(\rho(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] + 2^{\ell_1 - 9k^2t} + \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\dim \sigma(\mathcal{A}_{[q_0]}) < q_0 \mid \mathcal{E}, \mathcal{U} \right] \\ & \leq t^{-1/3} + 2^{\ell_1 - 9k^2t} + 2^{q_0 - 9k^2(t-1)} \leq t^{-1/4}, \end{aligned}$$

where we used [Condition 3.12](#) in the last transition. $\square$

To summarize the discussion, we define the notion of a smooth zoom-in, which is a subspace Q such that conditioned on $(\mathcal{E}, \mathcal{U}, Q)$, the distribution of L in $(\mathcal{E}, \mathcal{U}, L, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+$ is close to the uniform distribution over the set $\{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1) \mid Q \subseteq L\}$.

Definition 6.46. For a fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, a linear subspace $Q \subseteq \mathcal{V}(\mathcal{E})$ is said to be *smooth* with respect to $(\mathcal{E}, \mathcal{U})$ if $\dim Q = q_0$ and $\text{TVD}_{\mathcal{E},\mathcal{U}}(Q) \leq t^{-1/8}$.

The following corollary shows that Q is smooth with probability close to 1.

Corollary 6.47. Assume [Condition 3.12](#). For any fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, we have

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+} [Q \text{ is smooth with respect to } (\mathcal{E}, \mathcal{U}) \mid \mathcal{E}, \mathcal{U}] \geq 1 - t^{-1/8}.$$

Proof. Immediate from [Lemma 6.45](#) and Markov's inequality. $\square$

Finally, we record a covering property without advice, meaning that the distribution of L in $(\mathcal{E}, \mathcal{U}, L, *, *, *, *) \sim \mathcal{D}_{\text{in}}^+$ (without conditioning on Q) is close to uniform over $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$.

Proposition 6.48. Assume [Condition 3.12](#). Fix a positive integer $\ell \leq 2\ell_1$. For any fixed Alice-packet $(\mathcal{E}, \mathcal{U})$, if we sample $(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ conditioned on $(\mathcal{E}, \mathcal{U})$, the resulting distribution of $\sigma(\mathcal{A}_{[\ell]})$ has total variation distance at most $t^{-1/4}$ to the uniform distribution over $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell)$.

Proof. The proof is entirely analogous to the (combined) proofs of [Lemmas 6.41](#) and [6.44](#), and is hence omitted. The main difference is that when one invokes [Proposition F.1](#), this time one can take $\mathcal{B}_j$ to be a singleton set for each $j \in [t]$. $\square$

6.4.3 Alice's Existence of Decoding

The following lemma, analogous to [Lemma 5.15](#), shows that Alice's table passes the Grassmann agreement test with noticeable probability.

Lemma 6.49. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table and $G[\cdot]$ be a Bob-table. For any Alice-packet $(\mathcal{E}, \mathcal{U})$, we have

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right] \geq \text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, *, *, *, *)^2 - 2^{-\ell_1}.$$

Proof. We organize the proof into the following two steps.

Step 1: fixing $(\mathcal{E}', \mathcal{U}', L')$. Fix a Bob-packet $(\mathcal{E}', \mathcal{U}')$ and a subspace $L' \in \text{Gr}(\mathcal{V}(\mathcal{E}'), \ell_1 + 1)$ such that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\sigma(\mathcal{A}_{[\ell_1+1]}) = L' \mid \mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}' \right] > 0.$$

By [Definition 6.31](#), it is clear that if we sample $(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ conditioned on $\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}'$ and the event $\{\sigma(\mathcal{A}_{[\ell_1+1]}) = L'\}$, the resulting distribution of $\sigma(\mathcal{A}_{[\ell_1]})$ is uniform over the set $\text{Gr}(L', \ell_1)$. Therefore, we have

$$\begin{aligned} & \text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', L')^2 \\ &= \mathbb{E}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', L') \mid \mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}' \text{ and } \{\sigma(\mathcal{A}_{[\ell_1+1]}) = L'\} \right]^2 \\ &= \mathbb{E}_{L_1, L_2 \in \text{Gr}(L', \ell_1)} \left[\text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, L_1, \mathcal{E}', \mathcal{U}', L') \text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, L_2, \mathcal{E}', \mathcal{U}', L') \right]. \end{aligned} \quad (6.15)$$

Expanding the right-hand side of [Equation \(6.15\)](#), we get

$$\begin{aligned} & \text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', L')^2 \\ &= \mathbb{P}_{L_1, L_2 \in \text{Gr}(L', \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1] = G[\mathcal{E}', \mathcal{U}', L']|_{L_1} \text{ and } F[\mathcal{E}, \mathcal{U}, L_2] = G[\mathcal{E}', \mathcal{U}', L']|_{L_2} \right] \\ &\leq \mathbb{P}_{L_1, L_2 \in \text{Gr}(L', \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right]. \end{aligned} \quad (6.16)$$

Step 2: $(\mathcal{E}', \mathcal{U}', L')$ unfixed. By [Proposition 6.48](#), we know that conditioned on $(\mathcal{E}, \mathcal{U})$, the distribution of $\sigma(\mathcal{A}_{[\ell_1+1]})$ in the sample $(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}$ is $t^{-1/4}$ -close to uniform over $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1 + 1)$. Therefore, we have

$$\text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, *, *, *, *)^2$$

$$\begin{aligned}
&= \mathbb{E}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', \sigma(\mathcal{A}_{[\ell_1+1]})) \mid \mathcal{E}, \mathcal{U} \right]^2 && \text{(by definition)} \\
&\leq \mathbb{E}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', \sigma(\mathcal{A}_{[\ell_1+1]}))^2 \mid \mathcal{E}, \mathcal{U} \right] && \text{(by Cauchy-Schwarz)} \\
&\leq \mathbb{E}_{L' \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1+1)} \left[\mathbb{E}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, \mathcal{E}', \mathcal{U}', L')^2 \mid \mathcal{E}, \mathcal{U} \text{ and } \{\sigma(\mathcal{A}_{[\ell_1+1]}) = L'\} \right] \right] + t^{-1/4}.
\end{aligned}$$

We can now apply [Equation \(6.16\)](#) to the above and get

$$\begin{aligned}
&\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, *, *, *)^2 \\
&\leq \mathbb{E}_{L' \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1+1)} \left[\mathbb{P}_{L_1, L_2 \in \text{Gr}(L', \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right] \right] + t^{-1/4} \\
&\leq \mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right] + \frac{1}{2^{\ell_1+1} - 1} + t^{-1/4} \\
&\leq \mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right] + 2^{-\ell_1}, \quad \text{(using [Condition 3.12](#))}
\end{aligned}$$

as desired. $\square$

When we eventually prove the soundness of **Game3**, we will need to “decode” a strategy for **Game2c** based on tables $F[\cdot]$ and $G[\cdot]$. The following definition captures the type of tuples $(\mathcal{E}, \mathcal{U}, Q)$ for which Alice can successfully decode an answer in **Game2c**.

Definition 6.50. Let $F[\cdot]$ be an Alice table, and let $(\mathcal{E}, \mathcal{U})$ be an Alice-packet. For any linear subspace $Q \subseteq \mathcal{V}(\mathcal{E})$ with $\dim Q \leq q_0$, we say that the tuple $(\mathcal{E}, \mathcal{U}, Q)$ is *answerable* with respect to $F[\cdot]$ if $\dim Q = q_0$ and the following statement holds: there exists a linear subspace $W \in \text{Gr}(\mathcal{V}(\mathcal{E}), 9k^2t - q_0)$ containing Q and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q \subseteq L \subseteq W \right] \geq \exp(-q_0^3).$$

Combining [Lemma 6.49](#) and the Grassmann decoding theorem ([Theorem 3.5](#)) shows that with noticeable probability, Alice can decode an answer in **Game2c** from the table $F[\cdot]$.

Lemma 6.51. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table and let $G[\cdot]$ be a Bob-table. For any Alice-packet $(\mathcal{E}, \mathcal{U})$ such that $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, *, *, *) \geq 2^{-q_0/3}$, we have

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}, \mathcal{U}, Q) \text{ is answerable with respect to } F[\cdot] \mid \mathcal{E}, \mathcal{U} \right] \geq 4^{-\ell_1^2}.$$

Proof. Since $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, *, *, *) \geq 2^{-q_0/3}$, [Lemma 6.49](#) implies

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2} \right] \geq 2^{-2q_0/3} - 2^{-\ell_1} \geq 2^{-q_0+5},$$

where we used [Condition 3.12](#) in the last transition. Applying [Theorem 3.5](#) to the table $F[\mathcal{E}, \mathcal{U}, L]$, where L ranges in $\text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$, yields a collection of subspaces $\mathcal{Q} \subseteq \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)$ such that:

$$(1) \quad |\mathcal{Q}| \geq 2^{-q_0 - \ell_1^2} |\text{Gr}(\mathcal{V}(\mathcal{E}), q_0)|;$$

- (2) for each $Q \in \mathcal{Q}$, there exists a linear subspace $W_Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), 9k^2t - q_0)$ and a linear map $f_Q : W_Q \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f_Q|_L \mid Q \subseteq L \subseteq W_Q \right] \geq \exp(-Cq_0^2) \geq \exp(-q_0^3),$$

where C is an absolute constant and the last transition is due to [Condition 3.12](#). By [Definition 6.50](#), this means that for each $Q \in \mathcal{Q}$, the tuple $(\mathcal{E}, \mathcal{U}, Q)$ is answerable with respect to $F[\cdot]$.

Therefore, it now suffices to show that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\sigma(\mathcal{A}_{[q_0]}) \in \mathcal{Q} \mid \mathcal{E}, \mathcal{U} \right] \geq 4^{-\ell_1^2}.$$

But it follows immediately from [Proposition 6.48](#) that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\sigma(\mathcal{A}_{[q_0]}) \in \mathcal{Q} \mid \mathcal{E}, \mathcal{U} \right] \geq \mathbb{P}_{Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)} [Q \in \mathcal{Q}] - t^{-1/4} \geq 2^{-q_0 - \ell_1^2} - t^{-1/4} \geq 4^{-\ell_1^2},$$

where we used [Condition 3.12](#) in the last transition. $\square$

6.4.4 Bob's Existence of Decoding

We next develop tools for showing that Bob can also use the table $G[\cdot]$ to obtain answers in **Game2c**. As mentioned earlier, the Bob-table $G[\cdot]$ uses mixed-type Grassmann graphs (instead of standard Grassmann graphs) to encode answers, and we do not have a decoding theorem for mixed-type Grassmann graphs. As a workaround, we will argue that Bob can still decode by “transferring” Alice’s decoding to Bob. We stress that Bob will still decode from his table $G[\cdot]$, not Alice’s table $F[\cdot]$; the “transfer” happens only in the sense that we use the properties satisfied by $F[\cdot]$ to deduce a similar property of $G[\cdot]$.

Definition 6.52. Let $G[\cdot]$ be a Bob table, and let $(\mathcal{E}', \mathcal{U}')$ be a Bob-packet with critical index $c \in [t]$. For any linear subspace $Q \subseteq \mathcal{V}(\mathcal{E}')$ with $\dim Q \leq q_0$, we say that the tuple $(\mathcal{E}', \mathcal{U}', Q)$ is *pre-answerable* with respect to $G[\cdot]$ if the following statements hold:

- (1) The tuple $(*, *, *, Q, \mathcal{E}', \mathcal{U}', *)$ has nonzero probability under $\mathcal{D}_{\text{in}}^+$. In other words, $Q = \sigma(\mathcal{A})$ for some $\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', q_0, 2^{2\ell_1 - q_0}s)$.
- (2) There exists a linear subspace $W \subseteq \mathcal{V}(\mathcal{E}')$ containing Q with $\text{codim } W \leq q_0$ and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell_1 + 1, s')} \left[G[\mathcal{E}', \mathcal{U}', \sigma(\mathcal{A})] = f|_{\sigma(\mathcal{A})} \mid \sigma(\mathcal{A}_{[q_0]}) = Q \text{ and } \sigma(\mathcal{A}) \subseteq W \right] \geq \exp(-q_0^4),$$

where $s' = 2^{\ell_1 - 1}s$.

The next definition formalizes the type of “pruning” we need for Alice’s decoding to be able to “transfer” to Bob’s side.

Definition 6.53. Let $\eta \in (0, 1)$ be a threshold parameter. An Alice-table $F[\cdot]$ and a Bob-table $G[\cdot]$ are said to be η -*transferable* (with each other) if the following statements hold:

(1) For any unfolded-Alice-question $(\mathcal{E}, \mathcal{U}, L)$ such that $F[\mathcal{E}, \mathcal{U}, L] \neq \text{nil}$, we have

$$\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, *, *, *) \geq \eta.$$

(2) For any unfolded-Bob-question $(\mathcal{E}', \mathcal{U}', L')$ such that $G[\mathcal{E}', \mathcal{U}', L'] \neq \text{nil}$, we have

$$\text{Vrf}_{F,G}(*, *, *, \mathcal{E}', \mathcal{U}', L') \geq \eta.$$

The next lemma shows how to transfer Alice's decoding to Bob's side, if the tables $F[\cdot]$ and $G[\cdot]$ are transferable with each other.

Lemma 6.54. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table, and let $G[\cdot]$ be a Bob-table that is 2^{-q_0} -transferable with $F[\cdot]$. Fix an Alice-packet $(\mathcal{E}, \mathcal{U})$ and a linear subspace $Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)$ such that

- (1) Q is smooth with respect to $(\mathcal{E}, \mathcal{U})$ (as per [Definition 6.46](#)), and
- (2) $(\mathcal{E}, \mathcal{U}, Q)$ is answerable with respect to $F[\cdot]$ (as per [Definition 6.50](#)).

Then

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}', Q) \text{ is pre-answerable with respect to } G[\cdot] \mid \mathcal{E}, \mathcal{U}, Q \right] \geq 4^{-\ell_1^2}. \quad (6.17)$$

Proof. We organize the proof into the following three steps.

Step 1: transference. Since $(\mathcal{E}, \mathcal{U}, Q)$ is answerable with respect to $F[\cdot]$, by [Definition 6.50](#) there exists a linear subspace $W \in \text{Gr}(\mathcal{V}(\mathcal{E}), 9k^2t - q_0)$ and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q \subseteq L \subseteq W \right] \geq \exp(-q_0^3).$$

We then have

$$\begin{aligned} & \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid \mathcal{E}, \mathcal{U}, Q \text{ and } \{L \subseteq W\} \right] \\ & \geq \mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q \subseteq L \subseteq W \right] - \text{TVD}_{\mathcal{E}, \mathcal{U}, W}(Q) \quad (\text{by } \text{Definition 6.42}) \\ & \geq \exp(-q_0^3) - 2^{\ell_1(q_0+1)} \text{TVD}_{\mathcal{E}, \mathcal{U}}(Q) \quad (\text{by } \text{Lemma 6.43}) \\ & \geq \exp(-q_0^3) - 2^{\ell_1(q_0+1)} t^{-1/8} \geq \exp(-2q_0^3). \quad (\text{by } \text{Definition 6.46} \text{ and } \text{Condition 3.12}) \end{aligned}$$

By the definition of $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, \mathcal{E}', \mathcal{U}', L')$ in [Notation 6.39](#), we have

$$\begin{aligned} & \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[G[\mathcal{E}', \mathcal{U}', L']|_L = f|_L \mid \mathcal{E}, \mathcal{U}, Q \text{ and } \{L \subseteq W\} \right] \\ & \geq \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \text{ and } \text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, \mathcal{E}', \mathcal{U}', L') = 1 \mid \mathcal{E}, \mathcal{U}, Q \text{ and } \{L \subseteq W\} \right] \\ & \geq 2^{-q_0} \cdot \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid \mathcal{E}, \mathcal{U}, Q \text{ and } \{L \subseteq W\} \right] \\ & \quad (\text{since } F[\cdot] \text{ and } G[\cdot] \text{ are } 2^{-q_0} \text{ transferable}) \\ & \geq 2^{-q_0} \exp(-2q_0^3) \geq \exp(-3q_0^3). \end{aligned}$$

Step 2: locating good Bob-packets. For any Bob-packet $(\mathcal{E}', \mathcal{U}')$ such that $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *)$ has nonzero probability under $\mathcal{D}_{\text{in}}^+$, we say it is “good” if

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[G[\mathcal{E}', \mathcal{U}', L']|_L = f|_L \mid \mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}' \text{ and } \{L \subseteq W\} \right] \geq \exp(-3q_0^3)/2. \quad (6.18)$$

By the conclusion from Step 1 of the proof, it follows that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}') \text{ is good} \mid \mathcal{E}, \mathcal{U}, Q \text{ and } \{L \subseteq W\} \right] \geq \exp(-3q_0^3)/2. \quad (6.19)$$

Since Q is smooth with respect to $(\mathcal{E}, \mathcal{U})$, by [Definitions 6.42](#) and [6.46](#) we have

$$\begin{aligned} \mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, Q, *, *, *) \sim \mathcal{D}_{\text{in}}^+} \left[L \subseteq W \mid \mathcal{E}, \mathcal{U}, Q \right] &\geq \mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[L \subseteq W \mid Q \subseteq L \right] - \text{TVD}_{\mathcal{E}, \mathcal{U}}(Q) \\ &\geq 2^{-\ell_1(q_0+1)} - t^{-1/8} \geq 2^{-\ell_1^2}, \end{aligned}$$

where we used [Condition 3.12](#) in the last transition. Consequently, [Equation \(6.19\)](#) implies

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}') \text{ is good} \mid \mathcal{E}, \mathcal{U}, Q \right] \geq 2^{-\ell_1^2} \cdot \exp(-3q_0^3)/2 \geq 4^{-\ell_1^2}, \quad (6.20)$$

where we used [Condition 3.12](#) in the last transition.

Step 3: extension. By [Definition 6.31](#), the condition [Equation \(6.18\)](#) is equivalent to

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell_1+1, s')} \left[G[\mathcal{E}', \mathcal{U}', \sigma(\mathcal{A})]|_{\sigma(\mathcal{A}_{[\ell_1]})} = f|_{\sigma(\mathcal{A}_{[\ell_1]})} \mid \sigma(\mathcal{A}_{[q_0]}) = Q \text{ and } \sigma(\mathcal{A}_{[\ell_1]}) \subseteq W \right] \geq \exp(-3q_0^3)/2,$$

where c is the critical index of $\mathcal{E}'$ and $s' = 2^{\ell_1-1}s$. By [Lemma 6.27](#), this implies

$$\mathbb{P}_{\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell_1+1, s')} \left[G[\mathcal{E}', \mathcal{U}', \sigma(\mathcal{A})] = g|_{\sigma(\mathcal{A})} \mid \sigma(\mathcal{A}_{[q_0]}) = Q \text{ and } \sigma(\mathcal{A}) \subseteq W' \right] \geq \exp(-3q_0^3)/10 \geq \exp(-q_0^4),$$

for some linear subspace $W' \subseteq \mathcal{V}(\mathcal{E}')$ containing $W \cap \mathcal{V}(\mathcal{E}')$ and some linear function $g : W' \rightarrow \mathbb{F}_2$. Since the codimension of W' in $\mathcal{V}(\mathcal{E}')$ is at most

$$\dim \mathcal{V}(\mathcal{E}') - \dim(W \cap \mathcal{V}(\mathcal{E}')) \leq \dim \mathcal{V}(\mathcal{E}) - \dim W = q_0,$$

this means that $(\mathcal{E}', \mathcal{U}', Q)$ is pre-answerable with respect to $G[\cdot]$ whenever $(\mathcal{E}', \mathcal{U}')$ is good. Therefore, [Equation \(6.20\)](#) implies the desired [Equation \(6.17\)](#). $\square$

For technical reasons, we will later use the following slightly stricter version of [Definition 6.52](#). We upgrade the notion of “pre-answerable” to “answerable” if the same type of decoding as in [Definition 6.52](#) can be done on the mixed-type Grassmann domain (in [Definition 6.52](#), with a very small probability $\sigma(\mathcal{A})$ may fall outside of the mixed-type Grassmann domain).

Definition 6.55. Let $G[\cdot]$ be a Bob table, and let $(\mathcal{E}', \mathcal{U}')$ be a Bob-packet with critical index $c \in [t]$. For any linear subspace $Q \subseteq \mathcal{V}(\mathcal{E}')$ with $\dim Q \leq q_0$, we say that the tuple $(\mathcal{E}', \mathcal{U}', Q)$ is *answerable* with respect to $G[\cdot]$ if $Q \in \text{MGr}_c(\mathcal{E}', q_0, 2^{2\ell_1-q_0}s)$ and the following statement holds: there exist a linear subspace $W \subseteq \mathcal{V}(\mathcal{E}')$ containing Q with $\text{codim } W \leq q_0$ and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L' \in \text{MGr}(\mathcal{E}', \ell_1+1, s')} \left[G[\mathcal{E}', \mathcal{U}', L'] = f|_{L'} \mid Q \subseteq L' \subseteq W \right] \geq \exp(-q_0^5),$$

where $s' = 2^{\ell_1-1}s$. More specifically, we also say that $(\mathcal{E}', \mathcal{U}', Q)$ is *answerable with respect to $G[\cdot]$ using (f, W)* , and define $\mathcal{S}_G[\mathcal{E}', \mathcal{U}', Q]$ to be a list of such pairs (f, W) .

The following proposition shows that as long as Q itself is in the mixed-type Grassmann domain $\text{MGr}(\mathcal{E}', q_0, 2^{2\ell_1 - q_0} s)$, the pre-answerability of $(\mathcal{E}', \mathcal{U}', Q)$ can be automatically upgraded to answerability.

Proposition 6.56. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table, and let $G[\cdot]$ be a Bob-table that is 2^{-q_0} -transferable with $F[\cdot]$. Suppose $(\mathcal{E}', \mathcal{U}')$ is a Bob-packet with critical index c . Then for any $Q \in \text{MGr}_c(\mathcal{E}', q_0, 2^{2\ell_1 - q_0} s)$ such that $(\mathcal{E}', \mathcal{U}', Q)$ is pre-answerable with respect to $G[\cdot]$, the same tuple $(\mathcal{E}', \mathcal{U}', Q)$ is also answerable with respect to $G[\cdot]$.

Proof. By [Proposition 6.25](#),¹⁹ the total variation distance between the following two distributions of L' is at most, say, k^{-2} :

- (1) sample $L' \in \text{MGr}_c(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)$ conditioned on $Q \subseteq L'$; and
- (2) sample $\mathcal{A} \in \mathcal{A}_c(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)$ conditioned on $\sigma(\mathcal{A}_{[q_0]}) = Q$, and let $L' = \sigma(\mathcal{A})$.

We know from [Proposition 6.26](#) that even if we further condition both distributions on $\{L' \subseteq W\}$, for any linear subspace $W \subseteq \mathcal{V}(\mathcal{E}')$ of codimension at most q_0 , the resulting distributions are still k^{-1} -close in total variation distance. By definition, this allows one to convert pre-answerability to answerability. $\square$

We can now conclude the following counterpart of [Lemma 6.51](#), showing that answerability on Bob's side also happens with noticeable probability.

Lemma 6.57. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table, and let $G[\cdot]$ be a Bob-table that is 2^{-q_0} -transferable with $F[\cdot]$. Then for any Alice-packet $(\mathcal{E}, \mathcal{U})$ such that $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, *, *, *) \geq 2^{-q_0/3}$, we have

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}', Q) \text{ is answerable with respect to } G[\cdot] \mid \mathcal{E}, \mathcal{U} \right] \geq \exp(-6\ell_1^2).$$

Proof. First of all, combining [Corollary 6.47](#) with [Lemmas 6.51](#) and [6.54](#) yields

$$\begin{aligned} \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}', Q) \text{ is pre-answerable with respect to } G[\cdot] \mid \mathcal{E}, \mathcal{U} \right] &\geq (4^{-\ell_1^2} - t^{-1/8}) \cdot 4^{-\ell_1^2} \\ &\geq \exp(-5\ell_1^2), \end{aligned} \quad (6.21)$$

where we used [Condition 3.12](#) in the last transition.

Using [Condition 3.12](#), it is not hard to see (cf. [Proposition 6.25](#))

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', *, *) \sim \mathcal{D}_{\text{in}}^+} \left[Q \in \text{MGr}(\mathcal{E}', q_0, 2^{2\ell_1 - q_0} s) \mid \mathcal{E}, \mathcal{U} \right] \geq 1 - k^{-1}. \quad (6.22)$$

For any Bob-packet $(\mathcal{E}', \mathcal{U}')$ and any $Q \in \text{MGr}(\mathcal{E}', q_0, 2^{2\ell_1 - q_0} s)$, the pre-answerability of $(\mathcal{E}', \mathcal{U}', Q)$ can be converted to answerability, due to [Proposition 6.56](#). Therefore, combining [Equations \(6.21\)](#) and [\(6.22\)](#) yields the desired conclusion. $\square$

Corollary 6.58. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table, and let $G[\cdot]$ be a Bob-table that is 2^{-q_0} -transferable with $F[\cdot]$. If $\text{Vrf}_{F,G} \geq 2^{-q_0/4}$, then

$$\mathbb{P}_{(*, *, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', \mathcal{U}', Q) \text{ is answerable with respect to } G[\cdot] \right] \geq \exp(-7\ell_1^2).$$

¹⁹When applying [Proposition 6.25](#), note that we always have $|E'_c| \geq k$.

Proof. This follows immediately from [Lemma 6.57](#) because the condition $\text{Vrf}_{F,G} \geq 2^{-q_0/4} \geq 2^{1-q_0/3}$ implies

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, *, *, *) \sim \mathcal{D}_{\text{in}}^+} \left[\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, *, *, *, *) \geq 2^{-q_0/3} \right] \geq 2^{-q_0/3}. \quad \square$$

6.4.5 Sending Bob's Decoding back to Alice

As mentioned in the introductory text of [Section 6.4](#), the next main goal is to argue that Bob's decoded functions (those in the list $\mathcal{S}_G[\mathcal{E}', \mathcal{U}', Q]$) can be “transferred” back to Alice's side.

For intuition, we invite the reader to imagine that each answerable tuple $(\mathcal{E}', \mathcal{U}', Q)$ on Bob's side may “send” one of the elements of $\mathcal{S}_G[\mathcal{E}', \mathcal{U}', Q]$ to each of the Alice-side tuples $(\mathcal{E}, \mathcal{U}, Q)$ such that $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *)$ has nonzero probability under $\mathcal{D}_{\text{in}}^+$. The tuples $(\mathcal{E}, \mathcal{U}, Q)$ will then check whether the messages they receive have noticeable agreement with the Alice-table $F[\mathcal{E}, \mathcal{U}, \cdot]$.

We will define two levels of compatibility between these received “messages” and $F[\mathcal{E}, \mathcal{U}, \cdot]$. The first level is called *F-friendliness*, defined as follows.

Definition 6.59. Let $F[\cdot]$ be an Alice-table. For any possible sample $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', *, *)$ under $\mathcal{D}_{\text{in}}^+$, any linear subspace $W \subseteq \mathcal{V}(\mathcal{E}')$ containing Q , and any linear map $f : W \rightarrow \mathbb{F}_2$, we say that $(\mathcal{E}, \mathcal{U}, Q)$ is *F-friendly* to the message $(\mathcal{E}', Q', f, W)$ if the following holds:

- (1) $Q \in \text{MGr}(\mathcal{E}', q_0, 2^{2\ell_1 - q_0}s)$, and $\text{codim}_{\mathcal{V}(\mathcal{E}')} W \leq q_0$;
- (2) $Q' \subseteq Q$ is a subspace of codimension $\dim Q - \dim Q' = b \in \{0, 1\}$; and
- (3) the following probability is at least $\exp(-2q_0^5)$:

$$\mathbb{P}_{L \in \text{MGr}(\mathcal{E}', \ell_1, 2^{\ell_1}s)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q' \subseteq L \subseteq W \text{ and } Q + L \in \text{MGr}(\mathcal{E}', \ell_1 + b, 2^{\ell_1 - b}s) \right]. \quad (6.23)$$

We use $\mathcal{R}_F[\mathcal{E}, \mathcal{U}, Q]$ to denote the set of messages that $(\mathcal{E}, \mathcal{U}, Q)$ is *F-friendly* to.

The notion of *F-friendliness* does not require too much: it only inspects the entries of $F[\mathcal{E}, \mathcal{U}, \cdot]$ at the mixed-type-Grassmann locations, which (in some sense) are directly “connected” to Bob's table $G[\mathcal{E}', \mathcal{U}', \cdot]$. The next level of compatibility, defined as follows, is much more stringent. It checks (almost) the full Grassmann table $F[\mathcal{E}, \mathcal{U}, \cdot]$, only with a small-codimensional zoom-out W_0 , and is satisfied only if there exists some global well-agreed function $f_0 : W_0 \rightarrow \mathbb{F}_2$ that is compatible with the incoming message.

Definition 6.60. In the setting and notation of [Definition 6.59](#), we say that $(\mathcal{E}, \mathcal{U}, Q)$ is *F-attached* to the message $(\mathcal{E}', Q', f, W)$ if in addition to the listed three conditions, the following fourth condition is also satisfied.

- (4) There exist:
 - a linear subspace $W_0 \subseteq \mathcal{V}(\mathcal{E})$ such that $\text{codim}_{\mathcal{V}(\mathcal{E})}(W_0) \leq 2q_0$ and $W \subseteq W_0$; and
 - a linear map $f_0 : W_0 \rightarrow \mathbb{F}_2$ such that $f_0|_W = f$ and

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f_0|_L \mid Q' \subseteq L \subseteq W_0 \right] \geq \exp(-q_0^9).$$

We first show below that for each message $(\mathcal{E}', Q', f, W)$ sent by $(\mathcal{E}', \mathcal{U}', Q)$, a noticeable fraction of the receivers $(\mathcal{E}, \mathcal{U}, Q)$ will be *F-friendly* to the message. In [Section 6.4.6](#), we will argue that any $(\mathcal{E}, \mathcal{U}, Q)$ that receives sufficiently many *F-friendly* messages would be *F-attached* to one of them.

Lemma 6.61. Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table, and let $G[\cdot]$ be a Bob-table that is 2^{-q_0} -transferable with $F[\cdot]$. Let $(\mathcal{E}', \mathcal{U}')$ be a Bob-packet and $Q \in \text{MGr}(\mathcal{E}', q_0, 2^{2\ell_1 - q_0} s)$. Suppose that $(\mathcal{E}', \mathcal{U}', Q)$ is answerable with respect to $G[\cdot]$ using (f, W) . Then

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', Q', f, W) \in \mathcal{R}_F[\mathcal{E}, \mathcal{U}, Q] \text{ for some } Q' \mid \mathcal{E}', \mathcal{U}', Q \right] \geq \exp(-2q_0^5).$$

Proof. By the definition of answerability and transferability, we have

$$\mathbb{E}_{L' \in \text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)} \left[\mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid \mathcal{E}', \mathcal{U}', L' \right] \mid Q \subseteq L' \subseteq W \right] \geq \gamma, \quad (6.24)$$

where $\gamma = 2^{-q_0} \exp(-q_0^5)$.

Note that if we sample $(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+$ conditioned on $(\mathcal{E}', \mathcal{U}')$, then $(\mathcal{E}, \mathcal{U})$ is distributed independently of (L, L') . Furthermore, once L' is also fixed and has dimension $\ell_1 + 1$, the subspace L is distributed uniformly over $\text{Gr}(L', \ell_1)$. Therefore, [Equation \(6.24\)](#) implies that with probability at least $\gamma/2$ over $(\mathcal{E}, \mathcal{U})$, we have

$$\mathbb{E}_{L' \in \text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)} \left[\mathbb{P}_{L \in \text{Gr}(L', \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \right] \mid Q \subseteq L' \subseteq W \right] \geq \gamma/2. \quad (6.25)$$

Let $\mathcal{Q}$ be the distribution of $L \cap Q$ in the following sampling process:

1. Sample L' uniformly at random from $\text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)$ conditioned on $Q \subseteq L' \subseteq W$.
2. Sample L uniformly at random from $\text{Gr}(L', \ell_1)$.

We can equivalently describe the above process as follows:

1. Sample $Q' \sim \mathcal{Q}$.
2. If $\dim Q' = \dim Q - 1$, sample $L \in \text{MGr}(\mathcal{E}', \ell_1, 2^{\ell_1} s)$ conditioned on $Q' \subseteq L \subseteq W$ and $Q + L \in \text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)$ (note that this always leads to $L \cap Q = Q'$).
3. If $\dim Q' = \dim Q$ (which means $Q' = Q$), sample L' uniformly at random from $\text{MGr}(\mathcal{E}', \ell_1 + 1, 2^{\ell_1 - 1} s)$ conditioned on $Q \subseteq L' \subseteq W$, and then sample a uniformly random hyperplane $L \in \text{Gr}(L', \ell_1)$ containing Q .

Note that in the case $Q' = Q$, we can replace the third step above by directly sampling a uniformly random $L \in \text{MGr}(\mathcal{E}', \ell_1, 2^{\ell_1} s)$ conditioned on $Q \subseteq L \subseteq W$, at the cost of incurring a total variation distance of at most $2^{-s/2}$.²⁰ Therefore, we can unify the cases $\dim Q' = \dim Q - 1$ and $\dim Q' = \dim Q$, by always sampling $L \in \text{MGr}(\mathcal{E}', \ell_1, 2^{\ell_1} s)$ conditioned on $Q' \subseteq L \subseteq W$ and $Q + L \in \text{MGr}(\mathcal{E}', \ell_1 + b, 2^{\ell_1 - b} s)$, where $b = \dim Q - \dim Q'$. This corresponds exactly to [Equation \(6.23\)](#). Consequently, [Equation \(6.25\)](#) implies

$$\mathbb{E}_{Q' \sim \mathcal{Q}} \left[\text{the value of the probability in Equation (6.23)} \right] \geq \gamma/2 - 2^{-s/2} \geq \exp(-2q_0^5),$$

which implies $(\mathcal{E}', Q', f, W) \in \mathcal{R}_F[\mathcal{E}, \mathcal{U}, Q]$ for some subspace Q' that has nonzero probability under $\mathcal{Q}$.

To summarize, we have proven that (see the text before [Equation \(6.25\)](#))

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}', Q', f, W) \in \mathcal{R}_F[\mathcal{E}, \mathcal{U}, Q] \text{ for some } Q' \mid \mathcal{E}', \mathcal{U}' \right] \geq \gamma/2 \geq \exp(-2q_0^5).$$

This is the same as the desired conclusion, because when we sample $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+$ conditioned on $(\mathcal{E}', \mathcal{U}')$, the pair $(\mathcal{E}, \mathcal{U})$ is distributed independently of Q . $\square$

²⁰To bound the total variation distance, use [Proposition 6.22](#) and the fact that $\text{codim}_{V(\mathcal{E}')} W \leq q_0 \ll s$.

6.4.6 Consistency of Decodings

As mentioned earlier, we now show that any $(\mathcal{E}, \mathcal{U}, Q)$ that receives sufficiently many F -friendly messages *with different critical coordinates* would be F -attached to one of them.

Note that the conclusion of the following lemma is just an expanded way to say that $(\mathcal{E}, \mathcal{U}, Q)$ is F -attached to $(\mathcal{E}'_i, Q', f_i, W_i)$ for some $i \in [N]$.

Lemma 6.62. *Assume [Condition 3.12](#). Let $F[\cdot]$ be an Alice-table. Fix an Alice-packet $(\mathcal{E}, \mathcal{U})$ and a linear subspace $Q \in \text{Gr}(\mathcal{V}(\mathcal{E}), q_0)$, and a subspace $Q' \subseteq Q$ of codimension $\dim Q - \dim Q' = b \in \{0, 1\}$. Suppose we have the following objects:*

- (1) pairwise distinct indices $c_1, \dots, c_N \in [t]$, where $N \geq \exp(k^8)$;
- (2) for each $i \in [N]$, a c_i -critical descendant $\mathcal{E}'_i = (E'_{i,1}, \dots, E'_{i,t})$ of $\mathcal{E}$, such that

$$|E'_{1,c_1}| = |E'_{2,c_2}| = \dots = |E'_{N,c_N}|;$$

- (3) for each $i \in [N]$, a pair (f_i, W_i) such that $(\mathcal{E}, \mathcal{U}, Q)$ is F -friendly to $(\mathcal{E}'_i, Q', f_i, W_i)$.

Then there exist a linear subspace $W \subseteq \mathcal{V}(\mathcal{E})$ with $\text{codim}_{\mathcal{V}(\mathcal{E})}(W) \leq 2q_0$ and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q' \subseteq L \subseteq W \right] \geq \exp(-q_0^9).$$

Furthermore, for some $i \in [N]$ we have $W_i \subseteq W$ and $f|_{W_i} = f_i$.

Before starting the formal proof, we give an overview of the proof of [Lemma 6.62](#), which is inspired by the proof of [Lemma 3.9](#) in [\[DKK⁺25, Min22\]](#). For simplicity of presentation we ignore the issue of zoom-ins.

We know from the F -friendliness conditions that each $f_i : W_i \rightarrow \mathbb{F}_2$ agrees well with the table $F[\mathcal{E}, \mathcal{U}, \cdot]$ on the mixed-type-Grassmann locations, i.e. mixed-type subspaces L that are contained in $\mathcal{V}(\mathcal{E}')$. In order to patch these locally agreed functions together to some $f : W \rightarrow \mathbb{F}_2$, we use an ℓ_1 -vs.- $\ell_1/10$ -dimensional Grassmann agreement test. In each W_i , we plant a “local linearity test” by sampling $L_1, L_2 \in \text{MGr}(\mathcal{E}', \ell_1, 2^{\ell_1}s)$ conditioned on $L_1, L_2 \subseteq W_i$ and $\dim(L_1 \cap L_2) = \lfloor \ell_1/10 \rfloor$, and test if

$$F[\mathcal{E}, \mathcal{U}, L_1]|_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2]|_{L_1 \cap L_2}.$$

Each of these local linearity tests passes with noticeable probability, due to F -friendliness to $(\mathcal{E}', Q', f_i, W_i)$.

If the subspaces $W_i \subseteq \mathcal{V}(\mathcal{E})$ satisfy a sunflower condition (as per [Definition 3.10](#)), these local linearity tests, when aggregated together, will be noticeably similar to a “global linearity test” that samples $L_1, L_2 \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)$ conditioned on $L_1, L_2 \subseteq W$ and $\dim(L_1 \cap L_2) = \lfloor \ell_1/10 \rfloor$. Then, due to [Corollary E.3](#), we can decode from the table $F[\mathcal{E}, \mathcal{U}, \cdot]$ some global linear function $f : W \rightarrow \mathbb{F}_2$ that has good global agreement with $F[\mathcal{E}, \mathcal{U}, \cdot]$.

Of course, the subspaces $W_i \subseteq \mathcal{V}(\mathcal{E})$ do not necessarily satisfy the sunflower condition. Nevertheless, using [Lemma 3.11](#) we can find a sub-collection of these subspaces that form a sunflower, which is also good enough.

After being able to decode a global linear function $f : W \rightarrow \mathbb{F}_2$, we still have to show that it agrees with f_i for some $i \in [N]$. We consider the list of all global linear functions $f : W \rightarrow \mathbb{F}_2$ that has good agreement with $F[\mathcal{E}, \mathcal{U}, \cdot]$. A list-decoding argument will show that the size of the list is not large, and nearly all of the passing probability of the “global linearity test” above can be attributed to this list. This will imply that some function in the list does agree with some f_i .

Proof of Lemma 6.62. Without loss of generality, we assume $c_i = i$ for each $i \in [N]$, and let

$$|E'_{1,1}| = |E'_{2,2}| = \dots = |E'_{N,N}| = k'. \quad (6.26)$$

For each pair of distinct indices $i, j \in [N]$, we use $\mathcal{E}'_{i,j}$ to denote the “common thinning” of $\mathcal{E}'_i$ and $\mathcal{E}'_j$, obtained by replacing the i -th block of $\mathcal{E} = (E_1, \dots, E_t)$ with $E'_{i,i}$ and replacing the j -th block with $E'_{j,j}$. We then have $\mathcal{V}(\mathcal{E}'_i) \cap \mathcal{V}(\mathcal{E}'_j) = \mathcal{V}(\mathcal{E}'_{i,j})$. The proof is divided into the following six steps.

Step 1: sunflower argument. By Definition 6.59, we have $\text{codim}_{\mathcal{V}(\mathcal{E}'_i)} W_i \leq q_0$ for all $i \in [N]$.

By the pigeonhole principle, there exists an integer $w' \in \{0, 1, \dots, q_0\}$ such that $\text{codim}_{\mathcal{V}(\mathcal{E}'_i)} W_i = w'$ for at least $N_1 := \lceil N/(q_0 + 1) \rceil$ of the indices $i \in [N]$. Without loss of generality assume they are the first N_1 indices in $[N]$. Due to Equation (6.26), for all $i \in [N_1]$ we have

$$\text{codim}_{\mathcal{V}(\mathcal{E})} W_i = \text{codim}_{\mathcal{V}(\mathcal{E}'_i)} W_i + \text{codim}_{\mathcal{V}(\mathcal{E})} \mathcal{V}(\mathcal{E}'_i) = w' + 9k^2 - (k')^2 \quad (6.27)$$

Let $M = \lfloor \exp(k^3) \rfloor$ and let $m \leq M$ be a positive integer to be determined later. We apply Lemma 3.11 to the subspaces $W_1, \dots, W_{N_1} \subseteq \mathcal{V}(\mathcal{E})$, obtaining a subspace $W \subseteq \mathcal{V}(\mathcal{E})$ and indices $i_1, \dots, i_m \in [N_1]$ such that $(W, W_{i_1}, \dots, W_{i_m})$ forms a sunflower (see Definition 3.10; only the first m petals will be actually used). Without loss of generality, we assume the indices $i_1, \dots, i_m$ are $1, 2, \dots, m$. Note that by the definition of sunflower, we have $W_1, \dots, W_m \subseteq W$, and

$$\text{codim}_W W_1 = \dots = \text{codim}_W W_m = w_0$$

for some integer $w_0 \geq 0$. Denoting $w = \text{codim}_{\mathcal{V}(\mathcal{E})} W$, we deduce from Equation (6.27) that

$$w' + 9k^2 - (k')^2 = w_0 + w. \quad (6.28)$$

Furthermore, the definition of sunflower implies that for any pair of distinct indices $i, j \in [m]$, we have $\text{codim}_W W_i \cap W_j = 2w_0$. Since $W_i \cap W_j \subseteq \mathcal{V}(\mathcal{E}'_{i,j})$, it follows that

$$2w_0 + w = \text{codim}_{\mathcal{V}(\mathcal{E})} W_i \cap W_j = \text{codim}_{\mathcal{V}(\mathcal{E})} \mathcal{V}(\mathcal{E}'_{i,j}) + \text{codim}_{\mathcal{V}(\mathcal{E}'_{i,j})} W_i \cap W_j \geq 2(9k^2 - (k')^2). \quad (6.29)$$

Comparing Equations (6.28) and (6.29) yields $w \leq 2w'$, and hence $\text{codim}_{\mathcal{V}(\mathcal{E})} W \leq 2w' \leq 2q_0$.

Step 2: probability of lying in a petal. Write $d = \lfloor \ell_1/10 \rfloor$ and $D = 2\ell_1 - d$, and $h = D - \dim Q' = D - q_0 + b$. Throughout the rest of the proof, we suppose $L_+ \in \text{Gr}(\mathcal{V}(\mathcal{E}), D)$ is a random subspace conditioned on $Q' \subseteq L_+$, and $L_1, L_2 \in \text{Gr}(L_+, \ell_1)$ are then sampled independently conditioned on $Q' \subseteq L_1, L_2$. Note that with probability at least $1 - 2^{-d+q_0}$, we have $\dim(L_1 \cap L_2) = d$.

For each $i \in [m]$, we let Γ_i be the event

$$\left\{ Q + L_+ \in \text{MGr}(\mathcal{E}'_i, D + b, 2^{d-b}s) \right\} \cap \{L_+ \subseteq W_i\}.$$

Due to Equation (6.26), we know that the probability

$$\mathbb{P} \left[Q + L_+ \in \text{MGr}(\mathcal{E}'_i, D + b, 2^{d-b}s) \mid L_+ \subseteq \mathcal{V}(\mathcal{E}'_i) \right]$$

is the same for each $i \in [m]$.²¹ We use γ to denote this probability, and we trivially have $\gamma \geq \exp(-50\ell_1 k^2)$. Note that

$$\mathbb{P}[\Gamma_i] = \mathbb{P}[L_+ \subseteq \mathcal{V}(\mathcal{E}'_i)] \cdot \gamma \cdot \mathbb{P}_{L \in \text{MGr}(\mathcal{E}'_i, D+b, 2^{d-b}s)}[L \subseteq W_i \mid Q \subseteq L].$$

²¹This uses the fact that $Q \in \text{MGr}(\mathcal{E}'_i, q_0, 2^{2\ell_1 - q_0}s)$ for each $i \in [m]$. This fact holds because otherwise $(\mathcal{E}, \mathcal{U}, Q)$ could not be F -friendly to $(\mathcal{E}'_i, Q', f_i, W_i)$.

The first and third factors on the right-hand side are “zoom-out probabilities,” and are both easy to estimate (for the third, use [Proposition 6.26](#)), leading to the bounds

$$2^{-(w_0+w)h-3} \cdot \gamma \leq \mathbb{P}[\Gamma_i] \leq 2^{-(w_0+w)h+3} \cdot \gamma. \quad (6.30)$$

Furthermore, it is easy to see that for any pair of distinct indices $i, j \in [m]$, we have (the projections of L_+ to the i -th block and the j -th block are almost independent)

$$\gamma^2/2 \leq \mathbb{P}\left[Q + L_+ \in \text{MGr}(\mathcal{E}'_i, D + b, 2^{d-b}s) \cap \text{MGr}(\mathcal{E}'_j, D + b, 2^{d-b}s) \mid L_+ \subseteq \mathcal{V}(\mathcal{E}'_{i,j})\right] \leq 2\gamma^2. \quad (6.31)$$

By [Definition 6.24](#), the intersection of mixed-type Grassmann domains in [Equation \(6.31\)](#) is the same as $\text{MGr}_{i,j}(\mathcal{E}'_{i,j}, D + b, 2^{d-b}s)$. We write

$$\mathbb{P}\left[Q + L_+ \in \text{MGr}_{i,j}(\mathcal{E}'_{i,j}, D + b, 2^{d-b}s) \mid L_+ \subseteq \mathcal{V}(\mathcal{E}'_{i,j})\right] = \gamma_{i,j} \in \left[\frac{\gamma^2}{2}, 2\gamma^2\right].$$

Then we have

$$\mathbb{P}[\Gamma_i \cap \Gamma_j] = \mathbb{P}[L_+ \subseteq \mathcal{V}(\mathcal{E}'_{i,j})] \cdot \gamma_{i,j} \cdot \mathbb{P}_{L \in \text{MGr}(\mathcal{E}'_{i,j}, D+b, 2^{d-b}s)}[L \subseteq W_i \cap W_j \mid Q \subseteq L].$$

The first and third factors on the right-hand side are easy to estimate (for the third, use [Proposition 6.26](#)), leading to the bounds (recall [Equation \(6.29\)](#))

$$2^{-(2w_0+w)h-4} \cdot \gamma^2 \leq \mathbb{P}[\Gamma_i \cap \Gamma_j] \leq 2^{-(2w_0+w)h+4} \cdot \gamma^2. \quad (6.32)$$

Step 3: passing probability in a petal. For each $i \in [m]$, let Λ_i be the event

$$\Gamma_i \cap \{F[\mathcal{E}, \mathcal{U}, L_1] = f_i|_{L_1}\} \cap \{F[\mathcal{E}, \mathcal{U}, L_2] = f_i|_{L_2}\} \cap \{\dim(L_1 \cap L_2) = d\}.$$

We note that conditioned on Γ_i , the distribution of $Q + L_+$ is uniformly random over the set

$$\left\{L \in \text{MGr}(\mathcal{E}'_i, D + b, 2^{d-b}s) \mid Q \subseteq L \subseteq W_i\right\}.$$

By [Proposition 6.26](#), it follows that the distribution of $Q + L_1$ is 16-almost uniformly²² random over the set

$$\left\{L \in \text{MGr}(\mathcal{E}'_i, \ell_1 + b, 2^{\ell_1-b}s) \mid Q \subseteq L \subseteq W_i\right\}.$$

Using the assumption that $(\mathcal{E}, \mathcal{U}, Q)$ is F -friendly to $(\mathcal{E}'_i, Q', f_i, W_i)$, this implies

$$\mathbb{P}\left[F[\mathcal{E}, \mathcal{U}, L_1] = f_i|_{L_1} \mid \Gamma_i\right] \geq \exp(-2q_0^5)/16.$$

By Cauchy-Schwarz, we know that

$$\begin{aligned} & \mathbb{P}\left[F[\mathcal{E}, \mathcal{U}, L_1] = f_i|_{L_1} \text{ and } F[\mathcal{E}, \mathcal{U}, L_2] = f_i|_{L_2} \mid \Gamma_i\right] \\ &= \mathbb{E}_{L_+} \left[\mathbb{P}\left[F[\mathcal{E}, \mathcal{U}, L_1] = f_i|_{L_1} \mid L_+\right]^2 \mid \Gamma_i \right] \\ &\geq \mathbb{P}\left[F[\mathcal{E}, \mathcal{U}, L_1] = f_i|_{L_1} \mid \Gamma_i\right]^2 \geq \exp(-4q_0^5)/256. \end{aligned}$$

Therefore,

$$\mathbb{P}[\Lambda_i \mid \Gamma_i] \geq \exp(-4q_0^5)/256 - 2^{-d+q_0} \geq \exp(-q_0^6), \quad (6.33)$$

where we used [Condition 3.12](#) in the last transition.

²²Here we say a distribution over a finite set S is C -almost uniform if the probability of every element in the set lies in $[C^{-1}|S|^{-1}, C|S|^{-1}]$.

Step 4: inclusion-exclusion. For each $i \in [m]$, let Λ_i^* be the event

$$\Lambda_i \setminus \left(\bigcup_{j \in [m], j \neq i} \Gamma_j \right).$$

Combining Equations (6.30), (6.32) and (6.33), we get

$$\mathbb{P}[\Lambda_i^*] \geq \exp(-q_0^6) \cdot 2^{-(w_0+w)h-3} \gamma - (m-1) \cdot 2^{-(2w_0+w)h+4} \gamma^2.$$

Since the events $\Lambda_1^*, \dots, \Lambda_m^*$ are pairwise disjoint, we have

$$\mathbb{P} \left[\bigcup_{i=1}^m \Lambda_i^* \right] \geq 2^{-wh+4} \left(\exp(-q_0^6 - 10) \cdot m \cdot 2^{-w_0h} \gamma - m(m-1) 2^{-2w_0h} \gamma^2 \right).$$

We now choose $m = \lceil \exp(-q_0^6 - 11) \cdot 2^{w_0h} \gamma^{-1} \rceil \leq \exp(k^3)$. Plugging into the above equation yields

$$\mathbb{P} \left[\bigcup_{i=1}^m \Lambda_i^* \right] \geq 2^{-wh+4} \exp(-q_0^7). \quad (6.34)$$

For future reference, we also record the estimate (using Equations (6.30), (6.32) and (6.33))

$$\mathbb{P}[\Lambda_i^* | \Gamma_i] \geq \exp(-q_0^6) - (m-1) \cdot 2^{-w_0h+7} \gamma \geq \exp(-q_0^6)/2. \quad (6.35)$$

Note that

$$\bigcup_{i=1}^m \Lambda_i^* \subseteq \bigcup_{i=1}^m \{L_+ \subseteq W_i\} \subseteq \{L_+ \subseteq W\}.$$

Since $\mathbb{P}[L_+ \subseteq W] \leq 2^{-wh+1}$, Equation (6.34) implies that

$$\mathbb{P} \left[\bigcup_{i=1}^m \Lambda_i^* \mid L_+ \subseteq W \right] \geq \exp(-q_0^7). \quad (6.36)$$

In particular, by the definition of the events Λ_i , this means

$$\mathbb{P} \left[F[\mathcal{E}, \mathcal{U}, L_1] |_{L_1 \cap L_2} = F[\mathcal{E}, \mathcal{U}, L_2] |_{L_1 \cap L_2} \mid \dim(L_1 \cap L_2) = d \text{ and } L_+ \subseteq W \right] \geq \exp(-q_0^7).$$

In the above probability expression, the distribution of the pair (L_1, L_2) is identical to sampling from $\mathcal{G}(W, \ell_1, d)$ conditioned on $Q' \subseteq L_1, L_2$ (see Section 3.1 for the notation $\mathcal{G}(W, \ell_1, d)$). Therefore, due to Corollary E.3, there exists a linear function $g : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = g|_L \mid Q' \subseteq L \subseteq W \right] \geq \exp(-q_0^9). \quad (6.37)$$

Step 5: list-decoding. Let $g_1, \dots, g_p$ be the list of all linear functions $g : W \rightarrow \mathbb{F}_2$ satisfying (6.37), where p is a positive integer. By Lemma E.4, we know that $p \leq 2 \exp(q_0^9)$. We consider a “pruned” Grassmann table $F'[\cdot]$ defined as follows: for each $L \in \text{Gr}(W, \ell_1)$,

- if $F[\mathcal{E}, \mathcal{U}, L] = g_j|_L$ for some $j \in [p]$, then let $F'[L] = \text{nil}$;
- if $F[\mathcal{E}, \mathcal{U}, L] \neq g_j|_L$ for any $j \in [p]$, then let $F'[L] = F[\mathcal{E}, \mathcal{U}, L]$.

We claim that

$$\mathbb{P} \left[F'[L_1] |_{L_1 \cap L_2} = F'[L_2] |_{L_1 \cap L_2} \mid \dim(L_1 \cap L_2) = d \text{ and } L_+ \subseteq W \right] \leq \exp(-q_0^8), \quad (6.38)$$

Suppose Equation (6.38) does not hold. Then by Corollary E.3, there would exist another linear function $g_0 : W \rightarrow \mathbb{F}_2$ (it cannot be among $g_1, \dots, g_p$ because otherwise the left-hand side of the following would be zero) satisfying

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F'[L] = g_0|_L \mid Q' \subseteq L \subseteq W \right] \geq \exp(-q_0^9),$$

and since $F'[\cdot]$ is a “pruning” of $F[\mathcal{E}, \mathcal{U}, \cdot]$, this g_0 would also satisfy Equation (6.37). That would make g_0 appear in the list $(g_1, \dots, g_p)$, which is a contradiction. Combining Equations (6.36) and (6.38) yields

$$\mathbb{P} \left[\left\{ F'[L_1] \neq F[\mathcal{E}, \mathcal{U}, L_1] \text{ or } F'[L_2] \neq F[\mathcal{E}, \mathcal{U}, L_2] \right\} \cap \bigcup_{i=1}^m \Lambda_i^* \mid L_+ \subseteq W \right] \geq \exp(-q_0^7) - \exp(-q_0^8),$$

and by the symmetry between L_1 and L_2 , this implies

$$\mathbb{P} \left[\left\{ F'[L_1] \neq F[\mathcal{E}, \mathcal{U}, L_1] \right\} \cap \bigcup_{i=1}^m \Lambda_i^* \mid L_+ \subseteq W \right] \geq \frac{1}{2} (\exp(-q_0^7) - \exp(-q_0^8)) \geq \exp(-q_0^8).$$

By the definition of F' , this means

$$\mathbb{P} \left[\left(\bigcup_{j=1}^p \left\{ F[\mathcal{E}, \mathcal{U}, L_1] = g_j|_{L_1} \right\} \right) \cap \left(\bigcup_{i=1}^m \Lambda_i^* \right) \mid L_+ \subseteq W \right] \geq \exp(-q_0^8). \quad (6.39)$$

Step 6: consistency. By Equation (6.39), there exists an index $j \in [p]$ such that

$$\mathbb{P} \left[\left\{ F[\mathcal{E}, \mathcal{U}, L_1] = g_j|_{L_1} \right\} \cap \bigcup_{i=1}^m \Lambda_i^* \mid L_+ \subseteq W \right] \geq \exp(-q_0^8)/p \geq \exp(-3q_0^9).$$

Without loss of generality assume this special index j is 1. Since the events $\Lambda_1^*, \dots, \Lambda_m^*$ are pairwise disjoint and all contained in the event $\{L_+ \subseteq W\}$, there exists an index $i \in [m]$ such that

$$\mathbb{P} \left[F[\mathcal{E}, \mathcal{U}, L_1] = g_1|_{L_1} \mid \Lambda_i^* \right] \geq \exp(-3q_0^9).$$

Without loss of generality assume this special index i is 1. By the definitions of Λ_1^* and Λ_1 , this is equivalent to

$$\mathbb{P} \left[f_1|_{L_1} = g_1|_{L_1} \mid \Lambda_1^* \right] \geq \exp(-3q_0^9).$$

Combining with Equation (6.35) yields

$$\mathbb{P} \left[f_1|_{L_1} = g_1|_{L_1} \mid \Gamma_1 \right] \geq \exp(-4q_0^9). \quad (6.40)$$

It remains to show that $f_1 = g_1|_{W_1}$. Assume on the contrary that $f_1 \neq g_1|_{W_1}$. We let $K = \ker(f_1 - g_1|_{W_1}) \subsetneq W_1$ be the hyperplane in W_1 on which f_1 agrees with $g_1|_{W_1}$. For any $L \in \text{MGr}(\mathcal{E}'_1, D + b, 2^{d-b}s)$ such that $Q \subseteq L \subseteq W_1$ but $L \not\subseteq K$, it is not hard to see (from how we sampled L_1 and L_+) that

$$\mathbb{P} \left[L_1 \subseteq K \mid Q + L_+ = L \right] \leq 2^{-(\ell_1 - q_0)}.$$

Furthermore, we know from Proposition 6.26 (and from the definition of Γ_1) that

$$\mathbb{P} \left[Q + L_+ \subseteq K \mid \Gamma_1 \right] \leq 2^{-(D - q_0) + 4}.$$

Therefore, by union bound we have

$$\mathbb{P} \left[L_1 \subseteq K \mid \Gamma_1 \right] \leq 2^{-(\ell_1 - q_0)} + 2^{-(D - q_0) + 4} \leq 2^{-\ell_1 + q_0 + 1}.$$

This directly contradicts Equation (6.40), and hence concludes the proof of this lemma. $\square$

6.4.7 Deriving Strategy for the Middle PCP

We are now ready to prove the soundness of $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$.

Proof of Lemma 6.33. Assume on the contrary that the value of $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$ is larger than δ . The goal is to obtain a strategy for

$$\text{Game2c}[H, k, \ell_2, t, 2^{2\ell_1 - q_0} s, q_0, \beta]$$

achieving a value larger than $2^{-q_2/4}$, which would contradict Lemma 5.22 and Proposition 6.30.

We first represent Alice's and Bob's strategies in Game3 by “folded tables.” Recall that in $\text{Game3}[H, k, \ell_1, \ell_2, t, s, \beta]$, the verifier samples $(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+$. We write

$$\tilde{F}[\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U})] : (L + \mathcal{N}(\mathcal{E}, \mathcal{U})) \rightarrow \mathbb{F}_2$$

for Alice's answer to the question $(\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U}))$, and write

$$\tilde{G}[\mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}'] : (L' + \bigoplus \mathcal{U}') \rightarrow \mathbb{F}_2$$

for Bob's answer to the question $(\mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}')$. By assumption, there exist such folded tables $\tilde{F}[\cdot]$ and $\tilde{G}[\cdot]$ such that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, L, *, \mathcal{E}', \mathcal{U}', L') \sim \mathcal{D}_{\text{in}}^+} \left[\tilde{F}[\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U})] \Big|_{L + \bigoplus \mathcal{U}} = \tilde{G}[\mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}'] \Big|_{L + \bigoplus \mathcal{U}} \right] > \delta. \quad (6.41)$$

Step 1: unfolded tables. We define an (unfolded) Alice-table (see Notation 6.38) $F^*[\cdot]$ as follows. For any Alice-packet $(\mathcal{E}, \mathcal{U})$ and any linear subspace $L \subseteq \mathcal{V}(\mathcal{E})$, if $(\mathcal{E}, \mathcal{U}, L)$ is an unfolded-Alice-question (see Notation 6.37), let

$$F^*[\mathcal{E}, \mathcal{U}, L] = \tilde{F}[\mathcal{E}, \mathcal{U}, L + \mathcal{N}(\mathcal{E}, \mathcal{U})] \Big|_L.$$

Otherwise, we let $F^*[\mathcal{E}, \mathcal{U}, L] = \text{nil}$.

Similarly, we define an (unfolded) Bob-table $G^*[\cdot]$ as follows. For any Bob-packet $(\mathcal{E}', \mathcal{U}')$ and any linear subspace $L' \subseteq \mathcal{V}(\mathcal{E}')$, if $(\mathcal{E}', \mathcal{U}', L')$ is an unfolded-Bob-question, let

$$G^*[\mathcal{E}', \mathcal{U}', L'] = \tilde{G}[\mathcal{E}', \mathcal{U}', L' + \bigoplus \mathcal{U}'] \Big|_{L'}.$$

Otherwise, we let $G^*[\mathcal{E}', \mathcal{U}', L'] = \text{nil}$.

We run the following iterative “pruning” procedure to obtain our final Alice-table $F[\cdot]$ and Bob-table $G[\cdot]$ used for decoding.

1. Initialize with $F := F^*$, $G := G^*$.
2. If there exists an unfolded-Alice-question $(\mathcal{E}, \mathcal{U}, L)$ such that $F[\mathcal{E}, \mathcal{U}, L] \neq \text{nil}$ but

$$\text{Vrf}_{F, G}(\mathcal{E}, \mathcal{U}, L, *, *, *) < 2^{-q_0},$$

update $F[\mathcal{E}, \mathcal{U}, L] = \text{nil}$. Similarly, if there exists an unfolded-Bob-question $(\mathcal{E}', \mathcal{U}', L')$ such that $G[\mathcal{E}', \mathcal{U}', L'] \neq \text{nil}$ but

$$\text{Vrf}_{F, G}(*, *, *, \mathcal{E}', \mathcal{U}', L') < 2^{-q_0},$$

update $G[\mathcal{E}', \mathcal{U}', L'] := \text{nil}$.

3. Repeat the preceding operations until for every unfolded-Alice-question $(\mathcal{E}, \mathcal{U}, L)$ such that $F[\mathcal{E}, \mathcal{U}, L] \neq \text{nil}$, we have $\text{Vrf}_{F,G}(\mathcal{E}, \mathcal{U}, L, *, *, *) \geq 2^{-q_0}$, and for every unfolded-Bob-question $(\mathcal{E}', \mathcal{U}', L')$ such that $G[\mathcal{E}', \mathcal{U}', L'] \neq \text{nil}$, we have $\text{Vrf}_{F,G}(*, *, *, \mathcal{E}', \mathcal{U}', L') \geq 2^{-q_0}$.

It is obvious that the procedure must terminate within a finite number of operations. Furthermore, by definitions, after termination the tables $F[\cdot], G[\cdot]$ are 2^{-q_0} -transferable with each other (see [Definition 6.53](#)).

We know from [Equation \(6.41\)](#) that $\text{Vrf}_{F^*, G^*} > \delta$. During the pruning procedure, the agreement probability can decrease by at most 2^{-q_0+1} , since when each unfolded question of Alice or Bob is pruned, its conditional contribution to the agreement is at most 2^{-q_0} . As a result, we get

$$\text{Vrf}_{F,G} \geq \text{Vrf}_{F^*, G^*} - 2^{-q_0+1} \geq \delta/2, \quad (6.42)$$

under [Condition 3.12](#).

Step 2: strategy for Game2c. Let $\vec{\tau} = (\tau_0, \dots, \tau_{2q_0})$ be as in [Condition 3.12](#). We now derive strategies for the provers in $\text{Game2c}[H, k, \ell_2, t, 2^{2\ell_1 - q_0}s, q_0, \beta]$ from the tables $F[\cdot]$ and $G[\cdot]$. The strategy for Alice is as follows.

1. Receive the question $(\mathcal{E}, \mathcal{A}, \mathcal{U})$. Let $Q = \sigma(\mathcal{A}_{[q_0]})$. If $\dim Q < q_0$, return an arbitrary answer and abort.
2. Pick a random subspace $Q' \subseteq Q$ with $\dim Q - \dim Q' \in \{0, 1\}$. If $\text{LIST}_{Q'}^{\vec{\tau}}(F) = \emptyset$ (see [Definition 3.8](#)), return an arbitrary answer and abort.
3. Pick a random element $(f, W) \in \text{LIST}_{Q'}^{\vec{\tau}}(F)$, and randomly extend f to a linear function $\tilde{f} : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$. If $\tilde{f}|_{\mathcal{N}(\mathcal{E}, \mathcal{U})}$ is not SNR-satisfying, return an arbitrary answer and abort. Otherwise, return $\tilde{f}$.

Before describing Bob's strategy, we first prepare a table of "distinguished answers" for Bob. For each Bob-packet $(\mathcal{E}', \mathcal{U}')$ and each subspace $Q \subseteq \mathcal{V}(\mathcal{E}')$ of dimension at most q_0 , if $(\mathcal{E}', \mathcal{U}', Q)$ is answerable with respect to $G[\cdot]$ (see [Definition 6.55](#)), pick a distinguished element of the list $\mathcal{S}_G[\mathcal{E}', \mathcal{U}', Q]$, and denote this element by $\mathcal{S}_G^*[\mathcal{E}', \mathcal{U}', Q]$. Now the strategy for Bob is:

1. Receive the question $(\mathcal{E}', \mathcal{A}, \mathcal{U}')$. Let $Q = \sigma(\mathcal{A}_{[q_0]})$.
2. If $(\mathcal{E}', \mathcal{U}', Q)$ is not answerable (see [Definition 6.55](#)) with respect to $G[\cdot]$, return an arbitrary answer. Otherwise, let $(f, W) = \mathcal{S}_G^*[\mathcal{E}', \mathcal{U}', Q]$, randomly extend f to a linear function $\tilde{f} : \mathcal{V}(\mathcal{E}') \rightarrow \mathbb{F}_2$, and return $\tilde{f}$.

Step 3: SNR-satisfaction. In this step, the goal is to show that in the strategy for Alice constructed in Step 2, for any (f, W) in Alice's list $\text{LIST}_{Q'}^{\vec{\tau}}(F)$, there exists an extension $\tilde{f} : \mathcal{V}(\mathcal{E}) \rightarrow \mathbb{F}_2$ such that $\tilde{f}|_{\mathcal{N}(\mathcal{E}, \mathcal{U})}$ is SNR-satisfying. Suppose such an extension does not exist for a pair $(f, W) \in \text{LIST}_{Q'}^{\vec{\tau}}(F)$. It follows that $f|_{\mathcal{N}(\mathcal{E}, \mathcal{U}) \cap W}$ does not have an SNR-satisfying extension to $\mathcal{N}(\mathcal{E}, \mathcal{U})$. Then for any linear subspace $\tilde{L} \subseteq \mathcal{V}(\mathcal{E})$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[L + \mathcal{N}(\mathcal{E}, \mathcal{U}) = \tilde{L} \mid Q' \subseteq L \subseteq W \right] > 0, \quad (6.43)$$

we must have

$$\tilde{F}[\mathcal{E}, \mathcal{U}, \tilde{L}]|_{W \cap \tilde{L}} \neq f|_{W \cap \tilde{L}}. \quad (6.44)$$

We claim that this implies

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q' \subseteq L \subseteq W \text{ and } L + \mathcal{N}(\mathcal{E}, \mathcal{U}) = \tilde{L} \right] \leq 2^{-(\ell_1 - q_0) + 3}. \quad (6.45)$$

Then taking expectation over $\tilde{L}$ yields

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \mid Q' \subseteq L \subseteq W \right] \leq 2^{-(\ell_1 - q_0) + 3},$$

contradicting the condition that $(f, W) \in \text{LIST}_{Q'}^{\vec{\tau}}(F)$.

We now show that [Equations \(6.43\)](#) and [\(6.44\)](#) together imply [Equation \(6.45\)](#). Indeed, [Equation \(6.43\)](#) implies that

$$\dim \left(W \cap \tilde{L} / (W \cap \mathcal{N}(\mathcal{E}, \mathcal{U}) + Q') \right) \leq \ell_1 - \dim Q',$$

which in turn (combined with [Equation \(6.43\)](#)) implies

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[L + \mathcal{N}(\mathcal{E}, \mathcal{U}) = \tilde{L} \mid Q' \subseteq L \subseteq W \cap \tilde{L} \right] \geq \prod_{i=1}^{\infty} (1 - 2^{-i}) \geq \frac{1}{4}. \quad (6.46)$$

If [Equation \(6.45\)](#) does not hold, then due to [Equation \(6.46\)](#) we have

$$\mathbb{P}_{L \in \text{Gr}(\mathcal{V}(\mathcal{E}), \ell_1)} \left[F[\mathcal{E}, \mathcal{U}, L] = f|_L \text{ and } L + \mathcal{N}(\mathcal{E}, \mathcal{U}) = \tilde{L} \mid Q' \subseteq L \subseteq W \cap \tilde{L} \right] \geq 2^{-(\ell_1 - q_0) + 1},$$

which easily contradicts [Equation \(6.44\)](#).

Step 4: good and excellent tuples. Fix an arbitrary Bob-packet $(\mathcal{E}', \mathcal{U}')$ and a subspace $Q \subseteq \mathcal{V}(\mathcal{E}')$ such that $(\mathcal{E}', \mathcal{U}', Q)$ is answerable with respect to $G[\cdot]$. Recall from Step 2 that a distinguished element $(f, W) = \mathcal{S}_G^*[\mathcal{E}', \mathcal{U}', Q]$ is chosen from the list $\mathcal{S}_G[\mathcal{E}', \mathcal{U}', Q]$. Now imagine that for any Alice-packet $(\mathcal{E}, \mathcal{U})$ such that $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *)$ has nonzero probability under $\mathcal{D}_{\text{in}}^+$,

$$(\mathcal{E}', \mathcal{U}', Q) \text{ sends the message } (\mathcal{E}', Q', f, W) \text{ to } (\mathcal{E}, \mathcal{U}, Q)$$

for any $Q' \subseteq Q$ with $\dim Q - \dim Q' \in \{0, 1\}$ (so there are 2^{q_0} messages sent to the same $(\mathcal{E}, \mathcal{U}, Q)$, because there are 2^{q_0} possibilities of Q'). We say that $(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}')$ is a *good tuple* if

$$(\mathcal{E}', \mathcal{U}', Q) \text{ sends } (\mathcal{E}, \mathcal{U}, Q) \text{ a message that } (\mathcal{E}, \mathcal{U}, Q) \text{ is } F\text{-friendly to.}$$

We say that $(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}')$ is an *excellent tuple* if

$$(\mathcal{E}', \mathcal{U}', Q) \text{ sends } (\mathcal{E}, \mathcal{U}, Q) \text{ a message that } (\mathcal{E}, \mathcal{U}, Q) \text{ is } F\text{-attached to.}$$

We claim that for any possible sample $(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}$, if $(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}')$ is an excellent tuple, where $Q = \sigma(\mathcal{A}_{[q_0]})$, then the strategies in Step 2 succeed with probability at least $\exp(-\ell_1^2)$ on the question pair $((\mathcal{E}, \mathcal{A}, \mathcal{U}), (\mathcal{E}', \mathcal{A}, \mathcal{U}'))$. Indeed, if $(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}')$ is an excellent tuple, then by [Definition 6.60](#), for some $Q' \subseteq Q$ with $\dim Q - \dim Q' \in \{0, 1\}$, there exists a pair $(f_0, W_0) \in \text{LIST}_{Q'}^{\vec{\tau}}(F)$ such that $W \subseteq W_0$ and $f_0|_W = f$. Then

- with probability (at least) 2^{-q_0} , Alice chooses the correct Q' ;

- with probability (at least) $\left| \text{LIST}_{Q'}^{\vec{\tau}}(F) \right|^{-1}$, Alice chooses the correct (f_0, W_0) ;
- since $\text{codim}_{\mathcal{V}(\mathcal{E})} W_0 \leq 2q_0$, with probability at least 2^{-2q_0} , Alice chooses an extension of f_0 to $\mathcal{V}(\mathcal{E})$ that has an SNR-satisfying restriction on $\mathcal{N}(\mathcal{E}, \mathcal{U})$ (that such an extension exists is argued in Step 3 of this proof);
- since $\text{codim}_{\mathcal{V}(\mathcal{E}')} W \leq q_0$, with probability at least 2^{-q_0} , Bob chooses an extension of f to $\mathcal{V}(\mathcal{E}')$ that is consistent with Alice's choice.

In total, the probability that the verifier in **Game2c** accepts on the question pair $((\mathcal{E}, \mathcal{A}, \mathcal{U}), (\mathcal{E}', \mathcal{A}, \mathcal{U}'))$ is at least

$$2^{-4q_0} \left| \text{LIST}_{Q'}^{\vec{\tau}}(F) \right|^{-1} \geq \exp(-\ell_1^2),$$

where the size of $\text{LIST}_{Q'}^{\vec{\tau}}(F)$ is bounded by [Lemma 3.9](#).

It remains to show that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, \mathcal{E}', \mathcal{U}', \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\left(\mathcal{E}, \mathcal{U}, \sigma(\mathcal{A}_{[q_0]}), \mathcal{E}', \mathcal{U}' \right) \text{ is excellent} \right] \geq \exp(-9\ell_1^2). \quad (6.47)$$

Once that is shown, it would follow that the verifier in **Game2c** $[H, k, \ell_2, t, 2^{2\ell_1 - q_0}s, q_0, \beta]$ accepts with probability at least

$$\exp(-9\ell_1^2) \cdot \exp(-\ell_1^2) > 2^{-q_2/4},$$

and we would be done.

Step 5: finding attached messages. Combining [Corollary 6.58](#) and [Lemma 6.61](#), and the definition of good tuples, we know that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}') \text{ is good} \right] \geq \exp(-8\ell_1^2).$$

To show [Equation \(6.47\)](#), it suffices to show that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}') \text{ is good but not excellent} \right] \leq t^{-1/2}.$$

In fact, in the remainder of the proof, we fix an arbitrary Alice-packet $(\mathcal{E}, \mathcal{U})$ and show that

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}') \text{ is good but not excellent} \mid \mathcal{E}, \mathcal{U} \right] \leq t^{-1/2}. \quad (6.48)$$

For any $(\mathcal{E}, \mathcal{U}, Q)$ and any integer $k' \in \{k, k+1, \dots, 3k\}$, we let $\mathcal{C}(\mathcal{E}, \mathcal{U}, Q, k') \subseteq [t]$ denote the set of indices $c \in [t]$ such that there exists a c -critical Bob-packet $(\mathcal{E}', \mathcal{U}')$ with:

- $|E'_c| = k'$, where E'_c is the critical block of $\mathcal{E}' = (E'_1, \dots, E'_t)$; and
- $(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}')$ is good but not excellent.

We also define $\mathcal{C}(\mathcal{E}, \mathcal{U}, Q) = \bigcup_{k' \in \{k, \dots, 3k\}} \mathcal{C}(\mathcal{E}, \mathcal{U}, Q, k')$.

Roughly speaking, $\mathcal{C}(\mathcal{E}, \mathcal{U}, Q)$ is the set of critical coordinates for which $(\mathcal{E}, \mathcal{U}, Q)$ receives some message that it is F -friendly to but not F -attached to. This set cannot be too large, because otherwise, [Lemma 6.62](#) could help find one of these messages that $(\mathcal{E}, \mathcal{U}, Q)$ is F -attached to, leading to a contradiction. More formally, for an arbitrary $(\mathcal{E}, \mathcal{U}, Q)$ and thinning size $k' \in \{k, \dots, 3k\}$, suppose

that $|\mathcal{C}(\mathcal{E}, \mathcal{U}, Q, k')| \geq 2^{q_0} \exp(k^8)$. Then by the pigeonhole principle, for some Q' and on at least $\exp(k^8)$ distinct critical indices, $(\mathcal{E}, \mathcal{U}, Q)$ receives messages of the form $(\mathcal{E}', Q', f, W)$ with the same thinning size k' , and it is F -friendly to but not F -attached to them. This contradicts [Lemma 6.62](#). Therefore, we conclude that

$$|\mathcal{C}(\mathcal{E}, \mathcal{U}, Q)| \leq \sum_{k'=k}^{3k} |\mathcal{C}(\mathcal{E}, \mathcal{U}, Q, k')| \leq (2k+1) \cdot 2^{q_0} \exp(k^8) \leq \exp(2k^8). \quad (6.49)$$

Step 6: finishing the proof. We are now ready to prove [Equation \(6.48\)](#). When we sample $(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+$ conditioned on $(\mathcal{E}, \mathcal{U})$, let $c \in [t]$ be the critical coordinate that we use as an auxiliary random variable in the sampling procedure. If we condition only on $(\mathcal{E}, \mathcal{U})$, [Proposition 6.10](#) shows that the critical coordinate c is uniformly distributed over $[t]$, and [Equation \(6.49\)](#) could be directly used to bound the probability of being good but not excellent. In reality ([Equation \(6.48\)](#)), we also need to condition on Q . The intuition is that conditioning on Q does not bias the distribution of c by too much. Formally, we do the following calculation.

By definitions, we have

$$\begin{aligned} & \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, Q, \mathcal{E}', \mathcal{U}', *) \sim \mathcal{D}_{\text{in}}^+} \left[(\mathcal{E}, \mathcal{U}, Q, \mathcal{E}', \mathcal{U}') \text{ is good but not excellent} \mid \mathcal{E}, \mathcal{U} \right] \\ & \leq \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[c \in \mathcal{C}(\mathcal{E}, \mathcal{U}, \sigma(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \quad (\text{seeing } Q \text{ as } \sigma(\mathcal{A}_{[q_0]})) \\ & = \sum_{j=1}^t \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[c = j \text{ and } j \in \mathcal{C}(\mathcal{E}, \mathcal{U}, \sigma(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \right] \\ & = \frac{1}{t} \sum_{j=1}^t \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[j \in \mathcal{C}(\mathcal{E}, \mathcal{U}, \sigma(\mathcal{A}_{[q_0]})) \mid \mathcal{E}, \mathcal{U} \text{ and } \{c = j\} \right] \quad (\text{the marginal of } c \text{ is uniform}) \\ & = \frac{1}{t} \sum_{B \in \mathcal{V}(\mathcal{E})^{q_0}} \sum_{j=1}^t \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[j \in \mathcal{C}(\mathcal{E}, \mathcal{U}, \text{span}(B)) \text{ and } \rho(\mathcal{A}_{[q_0]}) = B \mid \mathcal{E}, \mathcal{U} \text{ and } \{c = j\} \right] \\ & \leq \frac{\exp(2k^8)}{t} \sum_{B \in \mathcal{V}(\mathcal{E})^{q_0}} \max_{j \in [t]} \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\rho(\mathcal{A}_{[q_0]}) = B \mid \mathcal{E}, \mathcal{U} \text{ and } \{c = j\} \right]. \quad (\text{using Equation (6.49)}) \end{aligned}$$

It suffices to prove the following upper bound

$$\sum_{B \in \mathcal{V}(\mathcal{E})^{q_0}} \max_{j \in [t]} \mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\rho(\mathcal{A}_{[q_0]}) = B \mid \mathcal{E}, \mathcal{U} \text{ and } \{c = j\} \right] \leq 2^{9q_0 k^2}.$$

Let $N := 2^{9q_0 k^2}$. It is easy to see that the number of valid B is at most N^t . Also, for every fixed $j \in [t]$ and $B \in \mathcal{V}(\mathcal{E})^{q_0}$, we have

$$\mathbb{P}_{(\mathcal{E}, \mathcal{U}, *, *, \mathcal{A}) \sim \mathcal{D}_{\text{in}}} \left[\rho(\mathcal{A}_{[q_0]}) = B \mid \mathcal{E}, \mathcal{U} \text{ and } \{c = j\} \right] \leq N^{-t+1}$$

since the projections of $\rho(\mathcal{A}_{[q_0]})$ on the non-critical blocks are independent and uniformly random. Combining the two facts, we obtain the desired estimate. $\square$

7 Acknowledgments

We thank Mark Braverman, Irit Dinur, Guy Kindler, Subhash Khot, Ran Raz, Muli Safra for several discussions and collaborations that led to this work.

References

- [ABS15] Sanjeev Arora, Boaz Barak, and David Steurer. Subexponential algorithms for Unique Games and related problems. *Journal of the ACM*, 62(5):42:1–42:25, 2015.
- [ACC06] Sanjeev Arora, Eden Chlamtac, and Moses Charikar. New approximation guarantee for chromatic number. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 215–224. ACM, 2006.
- [AKK⁺08] Sanjeev Arora, Subhash A. Khot, Alexandra Kolla, David Steurer, Madhur Tulsiani, and Nisheeth K. Vishnoi. Unique Games on expanding constraint graphs are easy. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 21–28. ACM, 2008.
- [ALM⁺98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.
- [AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: a new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.
- [BBKO21] Libor Barto, Jakub Bulín, Andrei Krokhin, and Jakub Opršal. Algebraic approach to promise constraint satisfaction. *Journal of the ACM*, 68(4):28:1–28:66, 2021.
- [BHL26] Nikhil Bansal, Neng Huang, and Euiwoong Lee. Improved SDP-based algorithm for coloring 3-colorable graphs, 2026.
- [BK97] Avrim Blum and David Karger. An $\tilde{O}(n^{3/14})$ -coloring algorithm for 3-colorable graphs. *Information Processing Letters*, 61(1):49–53, 1997.
- [BKS19] Boaz Barak, Pravesh K. Kothari, and David Steurer. Small-set expansion in Shortcode graph and the 2-to-2 Conjecture. In *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:12. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019.
- [Chl07] Eden Chlamtac. Approximation algorithms using hierarchies of semidefinite programming relaxations. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, pages 691–701. IEEE Computer Society, 2007.
- [CMM06] Moses Charikar, Konstantin Makarychev, and Yury Makarychev. Near-optimal algorithms for Unique Games. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 205–214. ACM, 2006.
- [DGKR05] Irit Dinur, Venkatesan Guruswami, Subhash Khot, and Oded Regev. A new multilayered PCP and the hardness of hypergraph vertex cover. *SIAM Journal on Computing*, 34(5):1129–1146, 2005.
- [DH13] Irit Dinur and Prahladh Harsha. Composition of low-error 2-query PCPs using decodable PCPs. *SIAM Journal on Computing*, 42(6):2452–2486, 2013.

- [DHK15] Irit Dinur, Prahladh Harsha, and Guy Kindler. Polynomially low error PCPs with polyloglog n queries via modular composition. In *Proceedings of the 47th Annual ACM Symposium on Theory of Computing*, pages 267–276. ACM, 2015.
- [DKK⁺21] Irit Dinur, Subhash Khot, Guy Kindler, Dor Minzer, and Muli Safra. On non-optimally expanding sets in Grassmann graphs. *Israel Journal of Mathematics*, 243(1):377–420, 2021.
- [DKK⁺25] Irit Dinur, Subhash Khot, Guy Kindler, Dor Minzer, and Muli Safra. Towards a proof of the 2-to-1 Games Conjecture. *Theory of Computing*, 21(11):1–50, 2025.
- [DMR09] Irit Dinur, Elchanan Mossel, and Oded Regev. Conditional hardness for approximate coloring. *SIAM Journal on Computing*, 39(3):843–873, 2009.
- [DRS05] Irit Dinur, Oded Regev, and Clifford Smyth. The hardness of 3-uniform hypergraph coloring. *Combinatorica*, 25(5):519–535, 2005.
- [DS05] Irit Dinur and Samuel Safra. On the hardness of approximating minimum vertex cover. *Annals of Mathematics*, 162(1):439–485, 2005.
- [EKL23] David Ellis, Guy Kindler, and Noam Lifshitz. An analogue of Bonami’s lemma for functions on spaces of linear maps, and 2-2 games. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 656–660. ACM, 2023.
- [Fei98] Uriel Feige. A threshold of $\ln n$ for approximating set cover. *Journal of the ACM*, 45(4):634–652, 1998.
- [FGL⁺96] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM*, 43(2):268–292, 1996.
- [GK04] Venkatesan Guruswami and Sanjeev Khanna. On the hardness of 4-coloring a 3-colorable graph. *SIAM Journal on Discrete Mathematics*, 18(1):30–40, 2004.
- [Gol23] Louis Golowich. From Grassmannian to simplicial high-dimensional expanders. In *64th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2023)*, pages 1639–1648. IEEE Computer Society, 2023.
- [GS20] Venkatesan Guruswami and Sai Sandeep. d -to-1 hardness of coloring 3-colorable graphs with $O(1)$ colors. In *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 62:1–62:12. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.
- [GW95] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42(6):1115–1145, 1995.
- [Hås01] Johan Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001.
- [HMRW14] Moritz Hardt, Raghu Meka, Prasad Raghavendra, and Benjamin Weitz. Computational limits for matrix completion. In *Proceedings of the 27th Conference on Learning Theory*, volume 35 of *Proceedings of Machine Learning Research*, pages 703–725. PMLR, 2014.

- [HMS23] Yahli Hecht, Dor Minzer, and Muli Safra. NP-hardness of almost coloring almost 3-colorable graphs. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2023)*, volume 275 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 51:1–51:12. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.
- [Hol09] Thomas Holenstein. Parallel repetition: simplification and the no-signaling case. *Theory of Computing*, 5(8):141–172, 2009.
- [Kho02a] Subhash Khot. Hardness results for coloring 3-colorable 3-uniform hypergraphs. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 23–32. IEEE Computer Society, 2002.
- [Kho02b] Subhash Khot. On the power of Unique 2-prover 1-round games. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity*, page 25. IEEE Computer Society, 2002.
- [Kho10a] Subhash Khot. Inapproximability of NP-complete problems, discrete Fourier analysis, and geometry. In *Proceedings of the International Congress of Mathematicians*, volume 4, pages 2676–2697. Hindustan Book Agency, 2010.
- [Kho10b] Subhash Khot. On the Unique Games Conjecture (invited survey). In *Proceedings of the 25th Annual IEEE Conference on Computational Complexity*, pages 99–121. IEEE Computer Society, 2010.
- [Kho14] Subhash Khot. Hardness of approximation. In *Proceedings of the International Congress of Mathematicians (ICM 2014)*, volume 1, pages 711–728. Kyung Moon Sa, 2014.
- [KKMO07] Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O’Donnell. Optimal inapproximability results for MAX-CUT and other 2-variable CSPs? *SIAM Journal on Computing*, 37(1):319–357, 2007.
- [KLS00] Sanjeev Khanna, Nathan Linial, and Shmuel Safra. On the hardness of approximating the chromatic number. *Combinatorica*, 20(3):393–415, 2000.
- [KMMS25] Subhash Khot, Dor Minzer, Dana Moshkovitz, and Muli Safra. Small-set expansion in the Johnson graph. *Theory of Computing*, 21(2):1–43, 2025.
- [KMS98] David R. Karger, Rajeev Motwani, and Madhu Sudan. Approximate graph coloring by semidefinite programming. *Journal of the ACM*, 45(2):246–265, 1998.
- [KMS23] Subhash Khot, Dor Minzer, and Muli Safra. Pseudorandom sets in Grassmann graph have near-perfect expansion. *Annals of Mathematics*, 198(1):1–92, 2023.
- [KMS25] Subhash Khot, Dor Minzer, and Muli Safra. On independent sets, 2-to-2 games and Grassmann graphs. *Theory of Computing*, 21(10):1–55, 2025.
- [KO22] Andrei Krokhin and Jakub Opršal. An invitation to the promise constraint satisfaction problem. *ACM SIGLOG News*, 9(3):30–59, 2022.
- [KOWŽ23] Andrei Krokhin, Jakub Opršal, Marcin Wrochna, and Stanislav Živný. Topology and adjunction in promise constraint satisfaction. *SIAM Journal on Computing*, 52(1):38–79, 2023.

- [KR08] Subhash Khot and Oded Regev. Vertex cover might be hard to approximate to within $2 - \epsilon$. *Journal of Computer and System Sciences*, 74(3):335–349, 2008.
- [KS13] Subhash Khot and Muli Safra. A two-prover one-round game with strong soundness. *Theory of Computing*, 9(28):863–887, 2013.
- [KS14] Subhash Khot and Rishi Saket. Hardness of finding independent sets in 2-colorable and almost 2-colorable hypergraphs. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1607–1625. Society for Industrial and Applied Mathematics, 2014.
- [KS17] Subhash Khot and Rishi Saket. Hardness of coloring 2-colorable 12-uniform hypergraphs with $2^{(\log n)^{\Omega(1)}}$ colors. *SIAM Journal on Computing*, 46(1):235–271, 2017.
- [KT17] Ken-ichi Kawarabayashi and Mikkel Thorup. Coloring 3-colorable graphs with less than $n^{1/5}$ colors. *Journal of the ACM*, 64(1):4:1–4:23, 2017.
- [KTY24] Ken-ichi Kawarabayashi, Mikkel Thorup, and Hirotaka Yoneda. Better coloring of 3-colorable graphs. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 331–339. ACM, 2024.
- [KV15] Subhash A. Khot and Nisheeth K. Vishnoi. The Unique Games Conjecture, integrality gap for cut problems and embeddability of negative-type metrics into ℓ_1 . *Journal of the ACM*, 62(1):8:1–8:39, 2015.
- [Min22] Dor Minzer. *On Monotonicity Testing and the 2-to-2 Games Conjecture*, volume 49 of *ACM Books*. Association for Computing Machinery, 2022.
- [MR10] Dana Moshkovitz and Ran Raz. Two-query PCP with subconstant error. *Journal of the ACM*, 57(5):29:1–29:29, 2010.
- [MZ26] Dor Minzer and Kai Zhe Zheng. Near optimal alphabet-soundness tradeoff PCPs. *Journal of the ACM*, 73(4), 2026.
- [Rag08] Prasad Raghavendra. Optimal algorithms and inapproximability results for every CSP? In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 245–254. ACM, 2008.
- [Rao11] Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM Journal on Computing*, 40(6):1871–1891, 2011.
- [Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.
- [Tre12] Luca Trevisan. On Khot’s Unique Games Conjecture. *Bulletin of the American Mathematical Society*, 49(1):91–111, 2012.
- [TSSW00] Luca Trevisan, Gregory B. Sorkin, Madhu Sudan, and David P. Williamson. Gadgets, approximation, and linear programming. *SIAM Journal on Computing*, 29(6):2074–2097, 2000.
- [Wig83] Avi Wigderson. Improving the performance guarantee for approximate graph coloring. *Journal of the ACM*, 30(4):729–735, 1983.

[Zuc07] David Zuckerman. Linear degree extractors and the inapproximability of Max Clique and chromatic number. *Theory of Computing*, 3(6):103–128, 2007.

A Basic Linear Algebra

In this appendix, we collect some basic linear algebraic facts about bilinear maps. Recall from [Section 3.1](#) that given an $\mathbb{F}_2$ -vector space V and a bilinear map $f : V \otimes V \rightarrow \mathbb{F}_2$, we use T_f to denote the associated linear map from V to V^* . The rank of f is defined to be the rank of T_f . The first proposition below analyzes how the rank of f changes after being restricted to a subspace $U \otimes U \subseteq V \otimes V$.

Proposition A.1. Let V be a finite dimensional $\mathbb{F}_2$ -vector space and let $U \subseteq V$ be a linear subspace. For any bilinear form $f : V \otimes V \rightarrow \mathbb{F}_2$, we have

$$\text{rank}(f) - 2 \text{codim } U \leq \text{rank}(f|_{U \otimes U}) \leq \text{rank}(f).$$

Proof. Let $\iota : U \hookrightarrow V$ be the embedding map, and let $g = f|_{U \otimes U}$. Then we have the commutative diagram

$$\begin{array}{ccccc} U & \xrightarrow{\iota} & V & \xrightarrow{T_f} & V^* & \xrightarrow{\iota^\dagger} & U^* \\ & & & \searrow & & \nearrow & \\ & & & T_g & & & \end{array}$$

Both composing with ι on the right and composing with $\iota^\dagger$ on the left reduce the rank by at most $\text{codim } U$, so we have

$$\text{rank}(T_f) - 2 \text{codim } U \leq \text{rank}(T_g) \leq \text{rank}(T_f),$$

as desired. □

The next two corollaries of [Proposition A.1](#) are both used in [Lemma 4.27](#).

Corollary A.2. Let V be a finite dimensional $\mathbb{F}_2$ -vector space and let $U \subseteq V$ be a linear subspace. Suppose $f : V \otimes V \rightarrow \mathbb{F}_2$ is a bilinear form such that $\text{rank}(f|_{U \otimes U}) = \text{rank}(f)$. Then for any $v \in V$, there exists $u \in U$ such that

$$f(v \otimes x) = f(u \otimes x) \quad \text{for all } x \in V.$$

In other words, letting $g = f|_{U \otimes U}$, we have $h|_U \in \text{image}(T_g)$ for each $h \in \text{image}(T_f)$.

Proof. Let $\iota : U \hookrightarrow V$ be the embedding map. Since $\text{rank}(f|_{U \otimes U}) = \text{rank}(f)$, it follows from the proof of [Proposition A.1](#) that

$$\text{image}(T_f \circ \iota) = \text{image}(T_g),$$

which is exactly the desired conclusion. □

Corollary A.3. For any positive integers n, r and any symmetric bilinear form $f : \mathbb{F}_2^n \otimes \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ with rank r , there exists an r -element subset $S \subseteq [n]$ such that the restriction of f to $\mathbb{F}_2^S \otimes \mathbb{F}_2^S$ has rank r .

Proof. Since $\dim \ker(T_f) = n - r$, there exists an r -element subset $S \subseteq [n]$ such that

$$\mathbb{F}_2^S + \ker(T_f) = \mathbb{F}_2^n. \tag{A.1}$$

Let $\iota : \mathbb{F}_2^S \rightarrow \mathbb{F}_2^n$ be the embedding map. To show that the restriction of f to $\mathbb{F}_2^S \otimes \mathbb{F}_2^S$ has rank r , it suffices to show that

$$\text{rank}(\iota^\dagger \circ T_f \circ \iota) = \text{rank}(T_f).$$

The symmetry of f implies

$$(T_f \circ \iota)^\dagger = \iota^\dagger \circ T_f,$$

so it suffices to show that $\text{rank}(T_f \circ \iota) = \text{rank}(T_f)$. But this is immediate due to [Equation \(A.1\)](#). $\square$

The next lemma is a standard decomposition of bilinear forms into symmetric rank-1 forms. It is used also in [Lemma 4.27](#).

Lemma A.4. *Let V be a finite dimensional $\mathbb{F}_2$ -vector space, and let r be a positive integer. For any symmetric bilinear form $f : V \otimes V \rightarrow \mathbb{F}_2$ with rank r , there exist a nonnegative integer $k \leq 3r/2$ and k vectors $v_1, \dots, v_k \in V$ such that*

$$f(x \otimes y) = \sum_{i=1}^k f(x \otimes v_i) f(y \otimes v_i) \quad \text{for all } x, y \in V.$$

In other words, any symmetric bilinear form of rank r has a tensor decomposition (see [Definition 4.13](#)) into at most $3r/2$ linear functionals.

Proof. We proceed by induction on r . The conclusion clearly holds for $r = 0$. In the rest of the proof, assume $r \geq 1$ and the conclusion is true for all smaller values of r . Consider the following two cases.

Case 1: there exists a vector $v \in V$ such that $f(v \otimes v) = 1$. Define a subspace

$$U = \{u \in V \mid f(u \otimes v) = 0\} \subseteq V.$$

It is clear that $\ker(T_f) \subseteq U$, and since $v \notin U$ we also have $\dim U \leq \dim V - 1$. Therefore,

$$\text{rank}(f|_{U \otimes U}) \leq \dim U - \dim \ker(T_f) \leq \dim V - \dim \ker(T_f) - 1 = \text{rank}(f) - 1.$$

Define a linear map $\pi : V \rightarrow V$ by letting $\pi(x) = x - f(x \otimes v)v$ for all $x \in V$. It is clear that

$$f(\pi(x) \otimes v) = f(x \otimes v) - f(x \otimes v)^2 = 0 \quad \text{for all } x \in V,$$

and hence the image of π is contained in U . Furthermore, for each $x, y \in V$ we have

$$\begin{aligned} f(\pi(x) \otimes \pi(y)) &= f(x \otimes y) - 2f(x \otimes v)f(y \otimes v) + f(x \otimes v)f(y \otimes v)f(v \otimes v) \\ &= f(x \otimes y) - f(x \otimes v)f(y \otimes v). \end{aligned} \tag{A.2}$$

Applying the induction hypothesis to the bilinear form $f(\pi(\cdot) \otimes \pi(\cdot))$ (which has rank at most $r - 1$ because $\text{image}(\pi) \subseteq U$ and $\text{rank}(f|_{U \otimes U}) \leq r - 1$), we get k vectors $v_1, \dots, v_k \in V$ with $k \leq 3(r - 1)/2$ such that

$$f(\pi(x) \otimes \pi(y)) = \sum_{i=1}^k f(x \otimes v_i) f(y \otimes v_i) \quad \text{for all } x, y \in V. \tag{A.3}$$

Combining [Equations \(A.2\) and \(A.3\)](#), we get

$$f(x \otimes y) = f(x \otimes v)f(y \otimes v) + \sum_{i=1}^k f(x \otimes v_i) f(y \otimes v_i) \quad \text{for all } x, y \in V,$$

as desired (noting that $k + 1 \leq 3r/2$).

Case 2: $f(v \otimes v) = 0$ holds for all $v \in V$. Since $\text{rank}(f) \geq 1$, there exist $v, w \in V$ such that $f(v \otimes w) = 1$. It follows from the case assumption that v and w are linearly independent. Define a subspace

$$U = \{u \in V \mid f(u \otimes v) = f(u \otimes w) = 0\} \subseteq V.$$

The rest of the argument is entirely analogous to Case 1. Since $U \cap \text{span}\{v, w\} = \{0\}$ we have $\dim U \leq \dim V - 2$. Due to $\ker(T_f) \subseteq U$, we then have $\text{rank}(f|_{U \otimes U}) \leq r - 2$. Define a linear map $\pi : V \rightarrow V$ by letting

$$\pi(x) = x - f(x \otimes v)w - f(x \otimes w)v \quad \text{for all } x \in V.$$

Similarly to Case 1, it is easy to verify that

$$f(\pi(x) \otimes v) = f(\pi(x) \otimes w) = 0 \quad \text{for all } x \in V,$$

and hence the image of π is contained in U . Furthermore, for each $x, y \in V$ one gets

$$\begin{aligned} & f(\pi(x) \otimes \pi(y)) \\ &= f(x \otimes y) - f(x \otimes v)f(y \otimes w) - f(x \otimes w)f(y \otimes v) \\ &= f(x \otimes y) - f(x \otimes v)f(y \otimes v) - f(x \otimes w)f(y \otimes w) - f(x \otimes (v + w))f(y \otimes (v + w)). \end{aligned}$$

As in Case 1, we then apply the induction hypothesis to decompose $f(\pi(x) \otimes \pi(y))$ into the sum of at most $3(r - 2)/2$ terms of the form $f(x \otimes v_i)f(y \otimes v_i)$. Thus $f(x \otimes y)$ can be written as the sum of at most $3(r - 2)/2 + 3 = 3r/2$ such terms, as desired. $\square$

The next lemma is the key to the success of the “local tensor tests” in our middle PCP, and it is used in [Lemma 5.16](#). In words, it asserts that if a bilinear form f has rank at least $2 + 2\text{codim}W$, then (1) restricting it to $W \otimes W$ drops the rank by at most $2\text{codim}W$, and (2) with high probability, restricting it to a random subspace $U \subseteq W$ of sufficiently large dimension does not drop the rank to at most 1.

Lemma A.5. *Let V be a finite dimensional $\mathbb{F}_2$ -vector space, and let $Q, W \subseteq V$ be linear subspaces such that $Q \subseteq W$. Denote $q = \dim Q$. Let ℓ be a positive integer such that $q + 2 \leq \ell \leq \dim W$. Then for any bilinear form $f : V \otimes V \rightarrow \mathbb{F}_2$ such that $\text{rank}(f) \geq 2 + 2\text{codim}W$, we have*

$$\mathbb{P}_{U \in \text{Gr}(W, \ell)} [\text{rank}(f|_{U \otimes U}) \leq 1 \mid Q \subseteq U] \leq 2^{4 - (\ell - q)/2}.$$

Proof. Let $g = f|_{W \otimes W}$. By [Proposition A.1](#), the assumption that $\text{rank}(f) \geq 2 + 2\text{codim}W$ implies $\text{rank}(g) \geq 2$. It suffices to work with the restricted map g in the rest of the proof.

Let $\ell' = \lfloor (\ell - q)/2 \rfloor \geq 1$. To pick a uniformly random $U \in \text{Gr}(W, \ell)$ that contains Q , we first pick uniformly random subspaces $U_1, U_2 \in \text{Gr}(W, \ell')$ independently, and then pick a uniformly random $U \in \text{Gr}(W, \ell)$ conditioned on $Q, U_1, U_2 \subseteq U$. Since we always have

$$\text{rank}(f|_{U \otimes U}) = \text{rank}(g|_{U \otimes U}) \geq \text{rank}(g|_{U_1 \otimes U_2}),$$

it suffices to show that

$$\mathbb{P}_{U_1, U_2 \in \text{Gr}(W, \ell')} [\text{rank}(g|_{U_1 \otimes U_2}) \leq 1] \leq 2^{3 - \ell'}.$$

As in the proof of [Proposition A.1](#), we let $\iota_{U_1} : U_1 \hookrightarrow W$ and $\iota_{U_2} : U_2 \hookrightarrow W$ be the two canonically defined embedding maps. Then we have

$$\text{rank}(g|_{U_1 \otimes U_2}) = \text{rank}(\iota_{U_2}^\dagger \circ T_g \circ \iota_{U_1}).$$

Note that

$$\text{rank}(T_g \circ \iota_{U_1}) = \dim(U_1 + \ker(T_g)) - \dim \ker(T_g).$$

Therefore, denoting $w = \dim W$ and $r = \text{rank}(g) = w - \dim \ker(T_g)$, we can calculate

$$\begin{aligned} & \mathbb{P}_{U_1 \in \text{Gr}(W, \ell')} [\text{rank}(T_g \circ \iota_{U_1}) \leq 1] \\ &= \mathbb{P}_{U_1 \in \text{Gr}(W, \ell')} [\dim(U_1 + \ker(T_g)) - \dim \ker(T_g) \leq 1] \\ &\leq \sum_{K \in \text{Gr}(W, w-r+1), K \supseteq \ker(T_g)} \mathbb{P}_{U_1 \in \text{Gr}(W, \ell')} [U_1 \subseteq K] \\ &\leq (2^r - 1) \cdot \begin{bmatrix} w - r + 1 \\ \ell' \end{bmatrix}_2 \begin{bmatrix} w \\ \ell' \end{bmatrix}_2^{-1} \\ &= (2^r - 1) \cdot \prod_{i=0}^{\ell'-1} \frac{2^{w-r-i+1} - 1}{2^{w-i} - 1} \\ &\leq 2^r \cdot (2^{-r+1})^{\ell'} \leq 2^{-\ell'+2}. \end{aligned} \quad (\text{using } r \geq 2 \text{ and } \ell' \geq 1)$$

Similarly, since

$$\text{rank}(\iota_{U_2}^\dagger \circ T_g \circ \iota_{U_1}) = \dim(U_2 + \ker(\iota_{U_1}^\dagger \circ T_g^\dagger)) - \dim \ker(\iota_{U_1}^\dagger \circ T_g^\dagger),$$

an analogous calculation shows

$$\mathbb{P}_{U_2 \in \text{Gr}(W, \ell')} [\text{rank}(\iota_{U_2}^\dagger \circ T_g \circ \iota_{U_1}) \leq 1] \leq 2^{-\ell'+2} \quad \text{whenever} \quad \dim \ker(\iota_{U_1}^\dagger \circ T_g^\dagger) \leq \dim W - 2.$$

But $\dim \ker(\iota_{U_1}^\dagger \circ T_g^\dagger) \leq \dim W - 2$ happens exactly when $\text{rank}(T_g \circ \iota_{U_1}) \geq 2$, the probability of which has already been shown to be at least $1 - 2^{-\ell'+2}$. Therefore, we conclude that

$$\mathbb{P}_{U_1, U_2 \in \text{Gr}(W, \ell')} [\text{rank}(\iota_{U_2}^\dagger \circ T_g \circ \iota_{U_1}) \leq 1] \leq 2 \cdot 2^{-\ell'+2} = 2^{-\ell'+3},$$

as desired. $\square$

B From Sub-4-to-1 to Exact 4-to-1 Games

In this appendix, we show that the hardness of approximating sub-4-to-1 games implies the exact 4-to-1 games theorem.

Proof of Theorem 1.6 assuming Theorem 3.3. Fix an arbitrary parameter $\varepsilon \in (0, 1)$ and a positive integer r . Write $k = \lceil 4/\varepsilon \rceil$ and $r' = kr$. We will prove Theorem 1.6 by constructing a polynomial-time reduction from $\text{GapS-4-to-1}_r(1, \varepsilon/2)$ to $\text{Gap-4-to-1}_{r'}(1, \varepsilon)$.

Given a sub-4-to-1 game instance Ψ with underlying graph $(L \sqcup R, E)$, alphabets Σ_L, Σ_R and constraints $\{\Phi_e \subseteq \Sigma_L \times \Sigma_R\}_{e \in E}$, we construct a 4-to-1 game instance Ψ' as follows:

1. Let Ψ' have the same constraint graph $(L \sqcup R, E)$ as Ψ , except that each edge in E is replaced by k parallel copies.
2. The left-alphabet of Ψ' is $\Sigma'_L = \Sigma_L \times (\mathbb{Z}/k\mathbb{Z})$, and the right-alphabet of Ψ' is $\Sigma'_R = \Sigma_R \times (\mathbb{Z}/k\mathbb{Z})$.

3. For each edge $e = (u, v) \in E$, according to [Definition 3.1](#), there exists a partition $\Sigma_L = \Sigma_{L,1} \sqcup \dots \sqcup \Sigma_{L,t}$ into sets of size 4 and a partition $\Sigma_R = \Sigma_{R,1} \sqcup \dots \sqcup \Sigma_{R,t}$ into singleton sets such that

$$\Phi_e = \bigcup_{i=1}^t \Gamma_{L,i} \times \Gamma_{R,i}, \quad \text{for some subsets } \Gamma_{L,i} \subseteq \Sigma_{L,i} \text{ and } \Gamma_{R,i} \subseteq \Sigma_{R,i}. \quad (\text{B.1})$$

For each $j, \ell \in \mathbb{Z}/k\mathbb{Z}$ and $i \in [t]$, we let

$$\Sigma_{L,i,j}^{(\ell)} = (\Gamma_{L,i} \times \{j\}) \cup ((\Sigma_{L,i} \setminus \Gamma_{L,i}) \times \{j + \ell\}) \subseteq \Sigma_L \times (\mathbb{Z}/k\mathbb{Z}) = \Sigma'_L, \quad (\text{B.2})$$

$$\Sigma_{R,i,j}^{(\ell)} = (\Gamma_{R,i} \times \{j\}) \cup ((\Sigma_{R,i} \setminus \Gamma_{R,i}) \times \{j - \ell\}) \subseteq \Sigma_R \times (\mathbb{Z}/k\mathbb{Z}) = \Sigma'_R. \quad (\text{B.3})$$

We then define a constraint $\Phi'_{e,\ell} \subseteq \Sigma'_L \times \Sigma'_R$

$$\Phi'_{e,\ell} = \bigcup_{i=1}^t \bigcup_{j \in \mathbb{Z}/k\mathbb{Z}} \Sigma_{L,i,j}^{(\ell)} \times \Sigma_{R,i,j}^{(\ell)}. \quad (\text{B.4})$$

Since for each $i \in [t]$, the sets $\Sigma_{L,i,1}^{(\ell)}, \dots, \Sigma_{L,i,k}^{(\ell)}$ have size $|\Sigma_{L,i}| = 4$ and form a partition of $\Sigma_{L,i} \times (\mathbb{Z}/k\mathbb{Z})$, and similarly the sets $\Sigma_{R,i,1}^{(\ell)}, \dots, \Sigma_{R,i,k}^{(\ell)}$ have size $|\Sigma_{R,i}| = 1$ and form a partition of $\Sigma_{R,i} \times (\mathbb{Z}/k\mathbb{Z})$, it is clear that $\Phi'_{e,\ell}$ is a 4-to-1 constraint.

4. For each edge $e \in E$, we put in Ψ' the k constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$. The total number of constraints in Ψ' is therefore equal to $k|E|$.

It is easy to see that Ψ' can be constructed from Ψ in polynomial time. We then show the completeness and soundness of the reduction.

Completeness: if $\text{val}(\Psi) = 1$, there exist assignment maps $A_L : L \rightarrow \Sigma_L$ and $A_R : R \rightarrow \Sigma_R$ that satisfy all constraints Φ_e , for $e \in E$. Then it is clear that the map $A'_L : L \rightarrow \Sigma'_L$ defined by $A'_L(u) = (A_L(u), 1)$ and the map $A'_R : R \rightarrow \Sigma'_R$ defined by $A'_R(v) = (A_R(v), 1)$ jointly satisfy all constraints $\Phi'_{e,\ell}$, for $e \in E$ and $\ell \in \mathbb{Z}/k\mathbb{Z}$. Consequently, we have $\text{val}(\Psi') = 1$.

Soundness: suppose we have assignment maps $A'_L : L \rightarrow \Sigma'_L$ and $A'_R : R \rightarrow \Sigma'_R$ given by

$$A'_L(u) = (A_L(u), K_L(u)) \quad \text{and} \quad A'_R(v) = (A_R(v), K_R(v)).$$

For any edge $e = (u, v) \in E$, we claim that if $(A_L(u), A_R(v)) \notin \Phi_e$, then at most 2 of the k constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ are satisfied by (A'_L, A'_R) . This means

$$\text{val}_{\Psi'}(A'_L, A'_R) \leq \text{val}_{\Psi}(A_L, A_R) + 2/k \leq \text{val}_{\Psi}(A_L, A_R) + \varepsilon/2,$$

and by the arbitrariness of (A'_L, A'_R) it follows that

$$\text{val}(\Psi') \leq \text{val}(\Psi) + \varepsilon/2,$$

as desired.

We now fix an edge $e = (u, v) \in E$ such that $(A_L(u), A_R(v)) \notin \Phi_e$, and show that at most 2 of the k constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ are satisfied by (A'_L, A'_R) . Let the subsets

$$\Gamma_{L,i}, \Sigma_{L,i} \subseteq \Sigma_L, \quad \Gamma_{R,i}, \Sigma_{R,i} \subseteq \Sigma_R, \quad \Sigma_{L,i,j}^{(\ell)} \subseteq \Sigma'_L, \quad \text{and} \quad \Sigma_{R,i,j}^{(\ell)} \subseteq \Sigma'_R$$

be as defined in [Equations \(B.1\) to \(B.3\)](#). We divide into the following five cases.

Case 1: $(A_L(u), A_R(v)) \notin \Sigma_{L,i} \times \Sigma_{R,i}$ for any $i \in [t]$. In this case, it is easy to see from [Equations \(B.2\) to \(B.4\)](#) that whichever values $K_L(u)$ and $K_R(v)$ take, we always have

$$(A'_L(u), A'_R(v)) \notin \bigcup_{\ell=1}^k \Phi'_{e,\ell}.$$

Therefore, none of the constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ are satisfied by (A'_L, A'_R) .

Case 2: $(A_L(u), A_R(v)) \in (\Sigma_{L,i} \setminus \Gamma_{L,i}) \times \Gamma_{R,i}$ for some $i \in [t]$. In this case, $(A'_L(u), A'_R(v)) \in \Phi'_{e,\ell}$ if and only if $K_L(u) = K_R(v) + \ell$, and hence exactly one of the constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ is satisfied by (A'_L, A'_R) .

Case 3: $(A_L(u), A_R(v)) \in \Gamma_{L,i} \times (\Sigma_{R,i} \setminus \Gamma_{R,i})$ for some $i \in [t]$. This case is symmetric to the previous case, and exactly one of the constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ is satisfied by (A'_L, A'_R) .

Case 4: $(A_L(u), A_R(v)) \in (\Sigma_{L,i} \setminus \Gamma_{L,i}) \times (\Sigma_{R,i} \setminus \Gamma_{R,i})$ for some $i \in [t]$. In this case, we have $(A'_L(u), A'_R(v)) \in \Phi'_{e,\ell}$ if and only if $K_L(u) - \ell = K_R(v) + \ell$, and hence at most two of the constraints $\Phi'_{e,1}, \dots, \Phi'_{e,k}$ are satisfied by (A'_L, A'_R) .

Case 5: $(A_L(u), A_R(v)) \in \Gamma_{L,i} \times \Gamma_{R,i}$ for some $i \in [t]$. This case cannot happen because if it does then (A_L, A_R) satisfies Φ_e , violating the assumption. $\square$

C Approximate Coloring of Hypergraphs

In this appendix, we present a proof of the “starting point” theorem (restated below) used in our reduction to 4-to-1 games. The proof of this theorem is essentially due to [\[DGKR05, DRS05\]](#), and we claim no originality here. The inclusion of the proof here is purely for the sake of expositional completeness.

Theorem 3.4 ([\[DRS05\]](#)). *For every fixed positive integer $c \geq 2$, there exists a constant $\varepsilon \geq \exp(-\exp(O(c^3)))$ such that given a 3-uniform hypergraph H , it is **NP**-hard to distinguish between the following cases:*

- (1) *Yes case: H is 2-colorable.*
- (2) *No case: in every c -coloring of H , at least ε fraction of the edges are monochromatic.*

To prove [Theorem 3.4](#), we need to use the PCP theorem of [\[ALM⁺98, AS98\]](#) and the parallel repetition theorem of [\[Raz98\]](#). More specifically, we apply the parallel repetition theorem to the equation-vs.-variable game associated to 3SAT5 instances.²³ This step is standard in the hardness of approximation literature, and we state the result ([Theorem C.2](#)) below without proof.

Definition C.1. Let d_0 and d_1 be positive integers. A (d_0, d_1) -biregular projection label cover instance $\Psi = (V_0, V_1, E, \Sigma_0, \Sigma_1, (\pi_e)_{e \in E})$ consists of the following data:

- (1) two vertex sets V_0 and V_1 ;
- (2) a set E of edges between V_0 and V_1 such that in the bipartite graph $(V_0 \sqcup V_1, E)$, every vertex in V_0 has degree d_0 and every vertex in V_1 has degree d_1 ;

²³By 3SAT5, we mean 3SAT instances where each variable is contained in exactly 5 clauses; see [\[Fei98, Proposition 2.1.2\]](#).

(3) two finite alphabets Σ_0, Σ_1 ; and

(4) a collection of constraints $(\pi_e)_{e \in E}$, where each π_e is a map from Σ_0 to Σ_1 .

The value of Ψ , denoted by $\text{val}(\Psi)$, is the maximum value of

$$\frac{1}{|E|} \sum_{(v_0, v_1) \in E} \mathbb{1} [\pi_{(v_0, v_1)}(A_0(v_0)) = A_1(v_1)]$$

achievable by assignment maps $A_0 : V_0 \rightarrow \Sigma_0$ and $A_1 : V_1 \rightarrow \Sigma_1$.

Theorem C.2 ([ALM⁺98, AS98, Raz98]). *There exists an absolute constant $\gamma \in (0, 1)$ such that for every fixed positive integer u , given a $(3^u, 5^u)$ -biregular projection label cover instance $\Psi = (V_0, V_1, E, \Sigma_0, \Sigma_1, (\pi_e)_{e \in E})$ such that $|\Sigma_0| = 7^u$ and $|\Sigma_1| = 2^u$, it is **NP**-hard to distinguish between the case $\text{val}(\Psi) = 1$ and the case $\text{val}(\Psi) \leq 2^{-\gamma u}$.*

Assuming [Theorem C.2](#), we now present a proof of [Theorem 3.4](#).

Proof of Theorem 3.4. We proceed by a reduction from [Theorem C.2](#). Let $\gamma \in (0, 1)$ be as in [Theorem C.2](#), and let $u = \lceil 40\gamma^{-2}c \rceil$. We fix a $(3^u, 5^u)$ -biregular projection label cover instance $\Psi = (V_0, V_1, E, \Sigma_0, \Sigma_1, (\pi_e)_{e \in E})$ with $|\Sigma_0| = 7^u$ and $|\Sigma_1| = 2^u$; we will show how to map it to a 3-uniform hypergraph H while linking the value of Ψ to the colorability of H .

The proof is divided into 8 steps. We first construct the hypergraph H in Steps 1 and 2. The completeness of the reduction is proved in Step 3, while Steps 4 to 8 will be devoted to proving the soundness of the reduction. Except for Step 6, the proof is almost identical to the one in [DRS05].²⁴ Throughout the proof, we let $\ell = 2c^2$.

Step 1: multi-layered label cover. Following the ideas of [DGKR05, DRS05], the first step is to perform a “multi-layered” parallel repetition on Ψ . For each $i \in [\ell]$, let $\mathcal{V}_i$ and R_i be the cartesian products

$$\mathcal{V}_i = V_1^{i-1} \times V_0^{\ell-i} \quad \text{and} \quad R_i = \Sigma_1^{i-1} \times \Sigma_0^{\ell-i}.$$

The $(\ell - 1)$ -tuples $\mathbf{v} = (v_1, \dots, v_{\ell-1}) \in \mathcal{V}_i$ will be the “blown-up vertices” in the i -th layer, and R_i can be viewed as their alphabets. For each $i, j \in [\ell]$ such that $i < j$, let $\mathcal{E}_{i,j}$ be the collection of pairs

$$(\mathbf{v}, \mathbf{v}') = ((v_1, \dots, v_{\ell-1}), (v'_1, \dots, v'_{\ell-1})) \in \mathcal{V}_i \times \mathcal{V}_j$$

such that:

- (1) $v_s = v'_s$ for all $s \in \{1, 2, \dots, i-1\} \cup \{j, j+1, \dots, \ell-1\}$; and
- (2) $(v_s, v'_s) \in E$ for all $s \in \{i, i+1, \dots, j-1\}$.

Given such a pair $(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}$, we define a projection map $\pi_{(\mathbf{v}, \mathbf{v}')} : R_i \rightarrow R_j$ by

$$\pi_{(\mathbf{v}, \mathbf{v}')}(\sigma_1, \dots, \sigma_{\ell-1}) = (\sigma_1, \dots, \sigma_{i-1}, \pi_{(v_i, v'_i)}(\sigma_i), \dots, \pi_{(v_{j-1}, v'_{j-1})}(\sigma_{j-1}), \sigma_j, \dots, \sigma_{\ell-1}),$$

for all $\sigma_1, \dots, \sigma_{i-1} \in \Sigma_1$ and $\sigma_i, \dots, \sigma_{\ell-1} \in \Sigma_0$.

For each $i, j \in [\ell]$ such that $i < j$, we have

$$|\mathcal{E}_{i,j}| = |\mathcal{V}_j| \cdot (5^u)^{j-i} = (5^u)^{j-i} \cdot |V_1|^{j-1} |V_0|^{\ell-j} = 5^{u(j-i)} \cdot (5/3)^{u(\ell-j)} \cdot |V_1|^{\ell-1}, \quad (\text{C.1})$$

where we used the $(3^u, 5^u)$ -biregularity of Ψ and its consequence $|V_0|/|V_1| = 5^u/3^u$.

²⁴The arguments in Steps 1, 5 and 8 are due to [DGKR05].

Step 2: construction of H . Following [DRS05], we construct the hypergraph H by composing the multi-layered label cover from Step 1 with an inner gadget based on the Kneser graph.

For each $i \in [\ell]$, we let $r_i = \lceil (|R_i| - c)/2 \rceil$. The vertex set of H is the disjoint union of cartesian products $\bigsqcup_{i=1}^{\ell} (\mathcal{V}_i \times \binom{R_i}{r_i})$, and the hyperedges of H are the collection of unordered triples $\{(\mathbf{v}, S_1), (\mathbf{v}, S_2), (\mathbf{v}', S_3)\}$ such that:

- (1) $\mathbf{v} \in \mathcal{V}_i$ and $\mathbf{v}' \in \mathcal{V}_j$ for some $i, j \in [\ell]$ such that $i < j$;
- (2) $(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}$;
- (3) $S_1, S_2 \in \binom{R_i}{r_i}$ and $S_3 \in \binom{R_j}{r_j}$; and
- (4) $S_1 \cap S_2 = \emptyset$ and $\pi_{(\mathbf{v}, \mathbf{v}')} (R_i \setminus (S_1 \cup S_2)) \subseteq S_3$.

Using Equation (C.1), we can upper-bound the number of edges in H by

$$\sum_{i,j \in [\ell], i < j} |\mathcal{E}_{i,j}| \cdot 2^{|R_i|} \cdot 2^{|R_j|} \leq 8^{7^{u(\ell-1)}} \ell^2 \cdot \max_{i,j \in [\ell], i < j} |\mathcal{E}_{i,j}| \leq 5^{u(\ell-1)} 8^{7^{u(\ell-1)}} \ell^2 \cdot |V_1|^{\ell-1}. \quad (\text{C.2})$$

It is clear that H can be constructed from Ψ in polynomial time. It suffices to prove the following statements:

- (1) Completeness: if $\text{val}(\Psi) = 1$, then H is 2-colorable.
- (2) Soundness: if under some c -coloring of H , less than $\exp(-\exp(\Omega(c^3)))$ fraction of edges of H are monochromatic, then $\text{val}(\Psi) > 2^{-\gamma^u}$.

The first statement will be proved in Step 3, and the second will be proved in Steps 4 to 8.

Step 3: completeness. In this step, we assume $\text{val}(\Psi) = 1$ and show that H is 2-colorable.

Suppose $A_0 : V_0 \rightarrow \Sigma_0$ and $A_1 : V_1 \rightarrow \Sigma_1$ are assignments that together satisfy every constraint of Ψ . Then for any $i \in [\ell]$, we can define a lifted assignment map $\tilde{A}_i : \mathcal{V}_i \rightarrow R_i$ by letting

$$\tilde{A}_i(\mathbf{v}) = (A_1(v_1), \dots, A_1(v_{i-1}), A_0(v_i), \dots, A_0(v_{\ell-1})), \quad \text{for all } \mathbf{v} = (v_1, \dots, v_{\ell-1}) \in \mathcal{V}_i.$$

For any vertex $(\mathbf{v}, S) \in \mathcal{V}_i \times \binom{R_i}{r_i}$, we color it red if $\tilde{A}_i(\mathbf{v}) \in S$, and otherwise color it blue.

Now, for any hyperedge $\{(\mathbf{v}, S_1), (\mathbf{v}, S_2), (\mathbf{v}', S_3)\}$ included in H (see Step 2), we have:

- (1) The vertices $(\mathbf{v}, S_1)$ and $(\mathbf{v}, S_2)$ cannot be both red, because $S_1 \cap S_2 = \emptyset$.
- (2) Let $i, j \in [\ell]$ be the indices such that $\mathbf{v} \in \mathcal{V}_i$ and $\mathbf{v}' \in \mathcal{V}_j$. If $(\mathbf{v}, S_1)$ and $(\mathbf{v}, S_2)$ are both colored blue, then $\tilde{A}_i(\mathbf{v}) \in R_i \setminus (S_1 \cup S_2)$ and hence

$$\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{A}_i(\mathbf{v})) \in S_3, \quad \text{due to} \quad \pi_{(\mathbf{v}, \mathbf{v}')} (R_i \setminus (S_1 \cup S_2)) \subseteq S_3.$$

By the definitions of $\pi_{(\mathbf{v}, \mathbf{v}')}$ and $\tilde{A}_i, \tilde{A}_j$, we have $\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{A}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}')$. Therefore, if $(\mathbf{v}, S_1)$ and $(\mathbf{v}, S_2)$ are both colored blue, then $(\mathbf{v}', S_3)$ must be colored red.

In conclusion, the hyperedge $\{(\mathbf{v}, S_1), (\mathbf{v}, S_2), (\mathbf{v}', S_3)\}$ cannot be monochromatic under the proposed coloring. This means that H is 2-colorable as long as $\text{val}(\Psi) = 1$.

Step 4: finding the leading color. In the rest of the proof, we fix a c -coloring of H , denoted by the map

$$f : \bigsqcup_{i=1}^{\ell} (\mathcal{V}_i \times \binom{R_i}{r_i}) \rightarrow [c].$$

We suppose that at most ε fraction of edges of H are monochromatic under f , for some $\varepsilon \in (0, 1)$ to be specified later.

For each $i \in [\ell]$ and each $\mathbf{v} \in \mathcal{V}_i$, we apply [DRS05, Lemma 2.2] to the vertices in the set $\left\{ (\mathbf{v}, S) \mid S \in \binom{R_i}{r_i} \right\}$ to find a color $c_{\mathbf{v}} \in [c]$ such that:

- (1) The fraction of sets $S \in \binom{R_i}{r_i}$ such that $f(\mathbf{v}, S) = c_{\mathbf{v}}$ is at least $|R_i|^{-c-1}$.
- (2) There exist disjoint sets $S_1, S_2 \in \binom{R_i}{r_i}$ such that $f(\mathbf{v}, S_1) = f(\mathbf{v}, S_2) = c_{\mathbf{v}}$. The set $R_i \setminus (S_1 \cup S_2)$ will be denoted by $B(\mathbf{v})$ and used later in the proof.

For each $i \in [\ell]$, let $c^{(i)} \in [c]$ be a color that maximizes the number of tuples $\mathbf{v} \in \mathcal{V}_i$ with $c_{\mathbf{v}} = c^{(i)}$. Since $\ell = 2c^2$, by the pigeonhole principle there exists a color $c^* \in [c]$ such that $c^{(i)} = c^*$ for at least $2c$ distinct indices $i \in [\ell]$. Pick exactly $2c$ indices among them, and let I be the set of these $2c$ indices.

Step 5: locating two critical layers. Observe that the bipartite graph $(\mathcal{V}_i \sqcup \mathcal{V}_{i+1}, \mathcal{E}_{i,i+1})$ is bi-regular for all $i \in [\ell - 1]$, due to the bi-regularity of Ψ . Consider the following random walk:

1. Start at a uniformly random element $\mathbf{v}^{(1)} \in \mathcal{V}_1$.
2. For each $i \in [\ell - 1]$, let $\mathbf{v}^{(i+1)}$ be a uniformly random element of $\mathcal{V}_{i+1}$ conditioned on $(\mathbf{v}^{(i)}, \mathbf{v}^{(i+1)}) \in \mathcal{E}_{i,i+1}$.

Due to the bi-regularity of the bipartite graphs $(\mathcal{V}_i \sqcup \mathcal{V}_{i+1}, \mathcal{E}_{i,i+1})$, this random walk produces a random sequence $(\mathbf{v}^{(1)}, \dots, \mathbf{v}^{(\ell)}) \in \mathcal{V}_1 \times \dots \times \mathcal{V}_{\ell}$ that is marginally uniform over each $\mathcal{V}_i$. Furthermore, by the definition of the edge sets $\mathcal{E}_{i,j}$, it is easy to see that for any $i, j \in [\ell]$ such that $i < j$, the distribution of the pair $(\mathbf{v}^{(i)}, \mathbf{v}^{(j)})$ is uniform over $\mathcal{E}_{i,j}$.

For each $i \in [\ell]$, let Γ_i be the event that $c_{\mathbf{v}^{(i)}} = c^{(i)}$. By the marginal uniformity and the choice of the $c^{(i)}$'s we have $\mathbb{P}[\Gamma_i] \geq c^{-1}$. By the inclusion-exclusion principle, we have

$$\begin{aligned} 1 &\geq \mathbb{P} \left[\bigcup_{i \in I} \Gamma_i \right] \geq \sum_{i \in I} \mathbb{P}[\Gamma_i] - \sum_{i, j \in I, i < j} \mathbb{P}[\Gamma_i \cap \Gamma_j] \\ &\geq |I| \cdot c^{-1} - \binom{|I|}{2} \cdot \max_{i, j \in I, i < j} \mathbb{P}[\Gamma_i \cap \Gamma_j]. \end{aligned}$$

Therefore, there exist $i, j \in I$ with $i < j$ such that

$$\mathbb{P}[\Gamma_i \cap \Gamma_j] \geq \binom{|I|}{2}^{-1} \cdot (c^{-1}|I| - 1) = \binom{2c}{2}^{-1} \geq \frac{1}{2c^2}.$$

By the uniformity of $(\mathbf{v}^{(i)}, \mathbf{v}^{(j)})$ over $\mathcal{E}_{i,j}$, this means that

$$\mathbb{P}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}} \left[c_{\mathbf{v}} = c^{(i)} \text{ and } c_{\mathbf{v}'} = c^{(j)} \right] \geq \frac{1}{2c^2}.$$

Since $i, j \in I$, by the definition of I , the above is equivalent to

$$\mathbb{P}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}} [c_{\mathbf{v}} = c_{\mathbf{v}'} = c^*] \geq \frac{1}{2c^2}. \quad (\text{C.3})$$

In the remainder of the proof, we fix the indices i and j identified above (satisfying Equation (C.3)).

Step 6: discarding monochromatic edges. We let $\mathcal{E}^*$ be the collection of all pairs $(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}$ such that:

- (1) $c_{\mathbf{v}} = c_{\mathbf{v}'} = c^*$; and
- (2) no hyperedge of H of the form $\{(\mathbf{v}, S_1), (\mathbf{v}, S_2), (\mathbf{v}', S_3)\}$ is colored monochromatically by f .

By Equation (C.2), the total number of monochromatic edges of H under the coloring f is at most

$$\varepsilon \cdot 5^{u(\ell-1)} 8^{7^{u(\ell-1)}} \ell^2 \cdot |V_1|^{\ell-1} \leq \varepsilon \cdot 5^{u(\ell-1)} 8^{7^{u(\ell-1)}} \ell^2 \cdot |\mathcal{E}_{i,j}| \leq \frac{1}{4c^2} |\mathcal{E}_{i,j}|,$$

where we chose a sufficiently small $\varepsilon = \exp(-\exp(O(c^3)))$ that justifies the last transition. It then follows from Equation (C.3) and the definition of $\mathcal{E}^*$ that

$$|\mathcal{E}^*| \geq \frac{1}{2c^2} |\mathcal{E}_{i,j}| - \frac{1}{4c^2} |\mathcal{E}_{i,j}| = \frac{1}{4c^2} |\mathcal{E}_{i,j}|. \quad (\text{C.4})$$

Step 7: strategy for the multi-layered label cover. The goal of this step is to decode from f a “good” assignment map for the two critical layers (identified in Step 5) of the ℓ -layered label cover instance (constructed in Step 1).

For each $\mathbf{v}' \in \mathcal{V}_j$, let $N^*(\mathbf{v}')$ be the collection of tuples $\mathbf{v} \in \mathcal{V}_i$ such that $(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*$.

In this paragraph, we define a deterministic map $\tilde{A}_j : \mathcal{V}_j \rightarrow R_j$ using the coloring f . Fix a tuple $\mathbf{v}' \in \mathcal{V}_j$. If $c_{\mathbf{v}'} \neq c^*$, we assign $\tilde{A}_j(\mathbf{v}')$ arbitrarily. Otherwise, for each $\mathbf{v} \in N^*(\mathbf{v}')$, we denote

$$B(\mathbf{v}, \mathbf{v}') := \pi_{(\mathbf{v}, \mathbf{v}')} (B(\mathbf{v})).$$

Recall from Step 4 that, the set $R_i \setminus B(\mathbf{v}) \subseteq R_i$ can be decomposed as the disjoint union of two sets $S_1, S_2 \in \binom{R_i}{r_i}$ such that $f(\mathbf{v}, S_1) = f(\mathbf{v}, S_2) = c^*$. For each $S \in \binom{R_j}{r_j}$ such that $B(\mathbf{v}, \mathbf{v}') \subseteq S$, by the construction in Step 2, the hyperedge

$$\{(\mathbf{v}, S_1), (\mathbf{v}, S_2), (\mathbf{v}', S)\}$$

is included in H . By the definition of $\mathcal{E}^*$, this hyperedge cannot be monochromatic under the coloring f , and therefore $f(\mathbf{v}', S) \neq c^*$. However, recall also from Step 4 that the fraction of $S \in \binom{R_j}{r_j}$ such that $f(\mathbf{v}', S) = c^*$ is at least $|R_j|^{-c-1}$. Therefore, at least an $|R_j|^{-c-1}$ fraction of $S \in \binom{R_j}{r_j}$ contain none of the sets $B(\mathbf{v}, \mathbf{v}')$, where $\mathbf{v}$ ranges in $N^*(\mathbf{v}')$. We can then apply Lemma C.3 to find²⁵ an element of R_j that is contained in $B(\mathbf{v}, \mathbf{v}')$ for at least

$$\eta = \frac{6^{-c}}{c(c+1) \ln |R_j|}$$

fraction of the tuples $\mathbf{v} \in N^*(\mathbf{v}')$. Define $\tilde{A}_j(\mathbf{v}')$ to be such an element of R_j .

We now define a random assignment map $\tilde{\mathcal{A}}_i : \mathcal{V}_i \rightarrow R_i$ by picking each $\tilde{\mathcal{A}}_i(\mathbf{v})$ independently and uniformly at random from $B(\mathbf{v})$. By the definition of $B(\mathbf{v})$ (in Step 4), we have $|B(\mathbf{v})| \leq |R_i| - 2r_i \leq c$. Therefore, we have

$$\mathbb{E}_{\tilde{\mathcal{A}}_i} \left[\mathbb{P}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*} \left[\pi_{(\mathbf{v}, \mathbf{v}')} (\tilde{\mathcal{A}}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}') \right] \right]$$

²⁵Note that for any $\mathbf{v} \in N^*(\mathbf{v}')$, we have $|B(\mathbf{v}, \mathbf{v}')| = |\pi_{(\mathbf{v}, \mathbf{v}')} (B(\mathbf{v}))| \leq |B(\mathbf{v})| \leq |R_i| - 2r_i \leq c$.

$$\begin{aligned}
&= \mathbb{E}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*} \left[\mathbb{P}_{\tilde{\mathcal{A}}_i} \left[\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{\mathcal{A}}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}') \right] \right] \\
&\geq \eta \cdot \mathbb{E}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*} \left[\mathbb{P}_{\tilde{\mathcal{A}}_i} \left[\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{\mathcal{A}}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}') \right] \mid \tilde{A}_j(\mathbf{v}') \in B(\mathbf{v}, \mathbf{v}') \right] \quad (\text{by the choice of } \tilde{\mathcal{A}}_i(\mathbf{v}')) \\
&\geq \eta \cdot \mathbb{E}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*} \left[\frac{1}{|B(\mathbf{v})|} \right] \geq \frac{\eta}{c}. \quad (\text{by the definition of } B(\mathbf{v}, \mathbf{v}'))
\end{aligned}$$

Therefore, there exists a deterministic instantiation $\tilde{A}_i : \mathcal{V}_i \rightarrow R_i$ of $\tilde{\mathcal{A}}_i$ such that

$$\mathbb{P}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}^*} \left[\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{A}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}') \right] \geq \frac{\eta}{c}.$$

By Equation (C.4), it follows that

$$\mathbb{P}_{(\mathbf{v}, \mathbf{v}') \in \mathcal{E}_{i,j}} \left[\pi_{(\mathbf{v}, \mathbf{v}')}(\tilde{A}_i(\mathbf{v})) = \tilde{A}_j(\mathbf{v}') \right] \geq \frac{\eta}{4c^3}. \quad (\text{C.5})$$

In the rest of the proof, we fix $\tilde{A}_i$ to be an instantiation of $\tilde{\mathcal{A}}_i$ that satisfies Equation (C.5).

Step 8: strategy for the original label cover. We define a random pair of (correlated) embedding maps $\varphi_0 : V_0 \hookrightarrow \mathcal{V}_i$ and $\varphi_1 : V_1 \hookrightarrow \mathcal{V}_j$ as follows:

1. For each $s \in \{1, 2, \dots, i-1\}$, let $v_s = v'_s$ be a uniformly random element of V_1 .
2. For each $s \in \{i+1, i+2, \dots, j-1\}$, pick a pair $(v_s, v'_s) \in E$ uniformly at random.
3. For each $s \in \{j, j+1, \dots, \ell-1\}$, let $v_s = v'_s$ be a uniformly random element of V_0 .
4. For each $w \in V_0$, let $\varphi_0(w) = (v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_{\ell-1}) \in \mathcal{V}_i$.
5. For each $w' \in V_1$, let $\varphi_1(w') = (v'_1, \dots, v'_{i-1}, w', v'_{i+1}, \dots, v'_{\ell-1}) \in \mathcal{V}_j$.

If we first sample the random maps φ_0, φ_1 and then independently sample a pair $(w, w') \in E$, it is clear that $(\varphi_0(w), \varphi_1(w'))$ is uniformly distributed over $\mathcal{E}_{i,j}$. Therefore, it follows from Equation (C.5) that

$$\mathbb{E}_{(\varphi_0, \varphi_1)} \left[\mathbb{P}_{(w, w') \in E} \left[\pi_{(\varphi_0(w), \varphi_1(w'))} \left(\tilde{A}_i(\varphi_0(w)) \right) = \tilde{A}_j(\varphi_1(w')) \right] \right] \geq \frac{\eta}{4c^3}. \quad (\text{C.6})$$

We now define a random pair of (correlated) assignment maps $\mathcal{A}_0 : V_0 \rightarrow \Sigma_0$ and $\mathcal{A}_1 : V_1 \rightarrow \Sigma_1$ as follows:

1. Sample the pair of embedding maps φ_0, φ_1 as described earlier.
2. For each $w \in V_0$, let $\mathcal{A}_0(w)$ be the i -th coordinate of $\tilde{A}_i(\varphi_0(w))$.
3. For each $w' \in V_1$, let $\mathcal{A}_1(w')$ be the i -th coordinate of $\tilde{A}_j(\varphi_1(w'))$.

By the definition of $\pi_{(\varphi_0(w), \varphi_1(w'))}$ in Step 1, it follows from Equation (C.6) that

$$\mathbb{E}_{(\mathcal{A}_0, \mathcal{A}_1)} \left[\mathbb{P}_{(w, w') \in E} \left[\pi_{(w, w')}(\mathcal{A}_0(w)) = \mathcal{A}_1(w') \right] \right] \geq \frac{\eta}{4c^3}.$$

Therefore, there exists a deterministic instantiation (A_0, A_1) of the random pair of maps $(\mathcal{A}_0, \mathcal{A}_1)$ that satisfies at least $\eta/(4c^3)$ fraction of the constraints in Ψ . Thus we have

$$\text{val}(\Psi) \geq \frac{\eta}{4c^3} \geq \frac{6^{-c}}{4c^4(c+1)\ln|R_j|} \geq \frac{6^{-c}}{4c^4(c+1)(\ell-1)\ln(7^u)} \geq \frac{1}{2^{20c} \cdot u} > 2^{-\gamma u},$$

where we used $u \geq 40\gamma^{-2}c$ in the last transition. $\square$

The following combinatorial lemma (adapted from [DRS05, Claim 4.5]) is used in Step 7 of the preceding proof.

Lemma C.3. *Fix a positive integer c . Let R be a nonempty finite set with $|R| \geq 6c$, and let r be an integer such that $|R|/3 \leq r \leq 2|R|/3$. Suppose $B_1, \dots, B_m \subseteq R$ are a sequence of subsets such that $|B_i| \leq c$ for each $i \in [m]$. If at least an $|R|^{-c-1}$ fraction of r -element subsets $S \in \binom{R}{r}$ contain none of the sets $B_1, \dots, B_m$, then there exists an element $a \in R$ contained in at least*

$$\frac{6^{-c}}{c(c+1)\ln|R|}$$

fraction of the sets $B_1, \dots, B_m$.

Proof. Let

$$\eta := \max_{a \in R} \frac{|\{i \in [m] \mid a \in B_i\}|}{m}.$$

Without loss of generality, suppose $B_1, \dots, B_q$ are a maximum pairwise disjoint subfamily among the sets $B_1, \dots, B_m$, for some integer $q \in [m]$. By maximality, every B_i contains some element of

$$U := B_1 \cup \dots \cup B_q.$$

Therefore

$$m \leq \sum_{a \in U} |\{i \in [m] \mid a \in B_i\}| \leq |U| \cdot \eta m \leq cq \cdot \eta m,$$

and hence $\eta \geq 1/(cq)$.

Next we upper-bound q using the assumptions in the lemma. Let S be chosen uniformly at random from $\binom{R}{r}$. For each $j \in [q]$, we have

$$\mathbb{P}_{S \in \binom{R}{r}} [B_j \subseteq S] = \binom{|R| - |B_j|}{r - |B_j|} / \binom{|R|}{r} = \prod_{t=0}^{|B_j|-1} \frac{r-t}{|R|-t} \geq \left(\frac{1}{6}\right)^{|B_j|} \geq 6^{-c},$$

where we used the assumptions $r \geq |R|/3$ and $|B_j| \leq c \leq |R|/6$ in the third transition.

Because the sets $B_1, \dots, B_q$ are pairwise disjoint, the events $\{B_j \subseteq S\}$, for $j \in [q]$, are negatively correlated under the uniform distribution over $\binom{R}{r}$. Hence

$$\mathbb{P}_{S \in \binom{R}{r}} [B_j \not\subseteq S \text{ for all } j \in [q]] \leq \prod_{j=1}^q \mathbb{P}_{S \in \binom{R}{r}} [B_j \not\subseteq S] \leq (1 - 6^{-c})^q.$$

Therefore, by the assumption in the lemma, we have

$$|R|^{-c-1} \leq \mathbb{P}_{S \in \binom{R}{r}} [B_i \not\subseteq S \text{ for all } i \in [m]] \leq \mathbb{P}_{S \in \binom{R}{r}} [B_j \not\subseteq S \text{ for all } j \in [q]] \leq (1 - 6^{-c})^q.$$

Taking logarithms gives

$$q \leq \frac{(c+1) \ln |R|}{-\ln(1-6^{-c})} \leq 6^c(c+1) \ln |R|.$$

Combining this with $\eta \geq 1/(cq)$, we obtain the desired inequality

$$\eta \geq \frac{6^{-c}}{c(c+1) \ln |R|}. \quad \square$$

D Grassmann Decoding Theorems

In this appendix, we explain how the Grassmann decoding theorems ([Theorems 3.5](#) and [3.6](#)) used in this paper can be derived from the slightly different versions in the existing literature.

D.1 The Expansion Theorem

To prove Grassmann decoding theorems, the standard approach is to first establish some small-set expansion properties of the Grassmann graph. It is observed in [[KMS25](#), [DKK⁺25](#)] that small vertex sets may not expand very well in the Grassmann graph, and the correct approach is to consider sets that remain small even after zoom-ins and zoom-outs. This is formalized in the next definition.

Definition D.1. Let n, ℓ, q be nonnegative integers such that $n - q \geq \ell \geq q + 1$, and let $\varepsilon \in (0, 1)$. Suppose $\mathcal{L} \subseteq \text{Gr}(\mathbb{F}_2^n, \ell)$ is a set of subspaces. We say that $\mathcal{L}$ is (q, ε) -pseudorandom if for any subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$ and $W \in \text{Gr}(\mathbb{F}_2^n, n - q)$ such that $Q \subseteq W$, we have

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L} \mid Q \subseteq L \subseteq W] \leq \varepsilon.$$

To facilitate Fourier analysis, it is useful to “lift” the Grassmann graph to a Cayley graph over an Abelian group. The “short-code graph” is a Cayley graph that serves this purpose very well, with the matrix space $\mathbb{F}_2^{n \times \ell}$ as the additive group and the rank-1 matrices as the generating set. The counterpart of [Definition D.1](#) in the short-code graph is given as follows.

Definition D.2. Let n, ℓ, q be nonnegative integers such that $n - q \geq \ell \geq q + 1$, and let $\varepsilon \in (0, 1)$. A function $f : \mathbb{F}_2^{n \times \ell} \rightarrow \{0, 1\}$ is said to be (q, ε) -pseudorandom if for any matrices

$$Y_1 \in \mathbb{F}_2^{\ell \times q}, \quad Z_1 \in \mathbb{F}_2^{n \times q}, \quad Y_2 \in \mathbb{F}_2^{q \times n} \quad \text{and} \quad Z_2 \in \mathbb{F}_2^{q \times \ell},$$

such that $\left\{ X \in \mathbb{F}_2^{n \times \ell} \mid XY_1 = Z_1 \text{ and } Y_2X = Z_2 \right\}$ is nonempty, we have

$$\mathbb{E}_{X \in \mathbb{F}_2^{n \times \ell}} [f(X) \mid XY_1 = Z_1 \text{ and } Y_2X = Z_2] \leq \varepsilon.$$

It is not hard to relate [Definitions D.1](#) and [D.2](#) together; we use the following lemma from [[MZ26](#)].

Lemma D.3 ([[MZ26](#), Lemma A.18]). *Let n, ℓ, q be nonnegative integers such that $n - q \geq \ell \geq q + 1$, and let $\varepsilon \in (0, 1)$. Suppose $\mathcal{L} \subseteq \text{Gr}(\mathbb{F}_2^n, \ell)$ is (q, ε) -pseudorandom (in the sense of [Definition D.1](#)). Define a function $f : \mathbb{F}_2^{n \times \ell} \rightarrow \{0, 1\}$ by*

$$f(X) = \begin{cases} 1, & \text{if } \text{rank}(X) = \ell \text{ and } \text{col}(X) \in \mathcal{L}, \\ 0, & \text{otherwise.} \end{cases}$$

Then f is $(q, 4\varepsilon)$ -pseudorandom (in the sense of [Definition D.2](#)).

The adjacency matrix of the short-code graph is represented by the following linear operator.

Definition D.4. Given a function $f : \mathbb{F}_2^{n \times \ell} \rightarrow \mathbb{R}$, we let $\mathcal{T}f : \mathbb{F}_2^{n \times \ell} \rightarrow \mathbb{R}$ be the function defined by

$$\mathcal{T}f(X) = \mathbb{E}_{Y_1 \in \mathbb{F}_2^{n \times 1}, Y_2 \in \mathbb{F}_2^{1 \times \ell}} [f(X + Y_1 Y_2)]. \quad (\text{D.1})$$

We are now ready to state the main expansion theorem from [KMS23, EKL23], which shows that pseudorandom sets have good expansion in the short-code graph.

Lemma D.5 ([EKL23, Theorem 69]). *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q \geq \ell \geq q + 1$. Then any $(q, 2^{-Cq^2})$ -pseudorandom function $f : \mathbb{F}_2^{n \times \ell} \rightarrow \{0, 1\}$ satisfies²⁶*

$$\langle f, \mathcal{T}f \rangle \leq 2^{-q+1} \mathbb{E}[f].$$

We then transfer the expansion theorem from the short-code graph to the Grassmann graph.

Lemma D.6. *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Then any $(q, 2^{-Cq^2})$ -pseudorandom subset $\mathcal{L} \subseteq \text{Gr}(\mathbb{F}_2^n, \ell)$ satisfies*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}] \leq 2^{-q+2} \cdot \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}].$$

Proof. If $q = 0$ the conclusion obviously holds. We assume $q \geq 1$, and let C be the constant from Lemma D.5. Suppose $\mathcal{L} \subseteq \text{Gr}(\mathbb{F}_2^n, \ell)$ is $(q, 2^{-(C+2)q^2})$ -pseudorandom. Define a function $f : \mathbb{F}_2^{n \times \ell} \rightarrow \{0, 1\}$ from $\mathcal{L}$ as in Lemma D.3. By Lemma D.3 we know that f is $(q, 2^{-Cq^2})$ -pseudorandom (in the sense of Definition D.2).

If $X \in \mathbb{F}_2^{n \times \ell}$, $Y_1 \in \mathbb{F}_2^{n \times 1}$ and $Y_2 \in \mathbb{F}_2^{1 \times \ell}$ are independent and uniformly random, then conditioned on the event

$$\{\text{rank}(X) = \ell\} \cap \{Y_1 \notin \text{col}(X)\} \cap \{Y_2 \neq 0\}, \quad (\text{D.2})$$

the pair $(\text{col}(X), \text{col}(X + Y_1 Y_2))$ is a uniformly random edge of the Grassmann graph $\text{Gr}(\mathbb{F}_2^n, \ell)$. Note that the probability of the event Equation (D.2) is at least $1 - 2^{\ell-n} - 2^{\ell-n} - 2^{-\ell} \geq 1/2$. Therefore, we have

$$\mathbb{P}_{X \in \mathbb{F}_2^{n \times \ell}, Y_1 \in \mathbb{F}_2^{n \times 1}, Y_2 \in \mathbb{F}_2^{1 \times \ell}} [f(X) = f(X + Y_1 Y_2) = 1] \geq \frac{1}{2} \cdot \mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}] \quad (\text{D.3})$$

Since the left-hand side of Equation (D.3) is exactly $\langle f, \mathcal{T}f \rangle$, using Lemma D.5 we can conclude that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}] \leq 2 \langle f, \mathcal{T}f \rangle \leq 2^{-q+2} \cdot \mathbb{E}[f] \leq 2^{-q+2} \cdot \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}]. \quad \square$$

D.2 From Expansion to Decoding

We now use an argument, originally due to [BKS19], to deduce the decoding statement from the expansion statement.

²⁶Here the inner product $\langle f, \mathcal{T}f \rangle$ should be interpreted as $\mathbb{E}_{X \in \mathbb{F}_2^{n \times \ell}} [f(X) \mathcal{T}f(X)]$.

Theorem D.7. *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right] \geq 2^{-q+4}. \quad (\text{D.4})$$

Then there exist a linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ and subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, $W \in \text{Gr}(\mathbb{F}_2^n, n - q)$ such that $Q \subseteq W$ and

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \subseteq W \right] \geq 2^{-Cq^2}.$$

Proof. For each linear functional $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, let $\mathcal{L}_f$ denote the set of subspaces $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$ such that $F[L] = f|_L$. We have

$$\mathbb{E}_{f \in (\mathbb{F}_2^n)^*} \left[\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}_f] \right] = \mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{f \in (\mathbb{F}_2^n)^*} [f|_L = F[L]] \right] \leq 2^{-\ell}. \quad (\text{D.5})$$

Furthermore,

$$\mathbb{E}_{f \in (\mathbb{F}_2^n)^*} \left[\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}_f] \right] = \mathbb{E}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{f \in (\mathbb{F}_2^n)^*} [f|_{L_1} = F[L_1] \text{ and } f|_{L_2} = F[L_2]] \right]. \quad (\text{D.6})$$

Note that for any edge (L_1, L_2) of the Grassmann graph $\text{Gr}(\mathbb{F}_2^n, \ell)$ such that

$$F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2},$$

we have

$$\mathbb{P}_{f \in (\mathbb{F}_2^n)^*} [f|_{L_1} = F[L_1] \text{ and } f|_{L_2} = F[L_2]] = 2^{-\ell-1}.$$

Therefore, combining [Equations \(D.4\) and \(D.6\)](#) yields

$$\mathbb{E}_{f \in (\mathbb{F}_2^n)^*} \left[\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}_f] \right] \geq 2^{-\ell-1} \cdot 2^{-q+4} = 2^{-q-\ell+3}. \quad (\text{D.7})$$

Combining [Equations \(D.5\) and \(D.7\)](#), we know that there exists a linear functional $f \in (\mathbb{F}_2^n)^*$ such that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}_f] > 2^{-q+2} \cdot \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}_f].$$

It then follows from [Lemma D.6](#) that $\mathcal{L}_f$ is not $(q, 2^{-Cq^2})$ -pseudorandom, which is exactly the desired conclusion. $\square$

We now restate and prove the precise decoding result stated in [Section 3.3.2](#). It is almost identical to [Theorem D.7](#), except that we require the feasible zoom-ins Q to be abundant.

Theorem 3.5 ([KMS23, EKL23]). *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right] \geq 2^{-q+5}. \quad (3.1)$$

Then for at least $2^{-q-\ell^2}$ fraction of subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, there exist a subspace $W \in \text{Gr}(\mathbb{F}_2^n, n - q)$ containing Q and a linear map $f : W \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \subseteq W \right] \geq 2^{-Cq^2}.$$

Proof. We take C to be the same constant as in [Theorem D.7](#). Let $\mathcal{Q}$ be the collection of subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$ that satisfy the desired property, and we will prove that

$$|\mathcal{Q}| \geq 2^{-q-\ell^2} |\text{Gr}(\mathbb{F}_2^n, q)|.$$

In the rest of the proof, we assume on the contrary that $|\mathcal{Q}| < 2^{-q-\ell^2} |\text{Gr}(\mathbb{F}_2^n, q)|$.

We define a table $F'[\cdot]$, where $F'[L] \in L^* \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, as follows:

$$F'[L] = \begin{cases} \mathbf{nil}, & \text{if } Q \subseteq L \text{ for some } Q \in \mathcal{Q}, \\ F[L], & \text{otherwise.} \end{cases}$$

We thus have

$$\begin{aligned} \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [F[L] \neq F'[L]] &\leq \sum_{Q \in \mathcal{Q}} \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [Q \subseteq L] = |\mathcal{Q}| \cdot \begin{bmatrix} n-q \\ \ell-q \end{bmatrix}_2 \begin{bmatrix} n \\ \ell \end{bmatrix}_2^{-1} \\ &= |\mathcal{Q}| \cdot \begin{bmatrix} n \\ q \end{bmatrix}_2^{-1} \begin{bmatrix} \ell \\ q \end{bmatrix}_2 \leq 2^{-q-\ell^2} \cdot 2^{\ell^2} = 2^{-q}. \end{aligned}$$

Therefore, it follows from the assumption [Equation \(3.1\)](#) that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [F'[L_1]|_{L_1 \cap L_2} = F'[L_2]|_{L_1 \cap L_2}] \geq 2^{-q+5} - 2 \cdot 2^{-q} \geq 2^{-q+4}.$$

Applying [Theorem D.7](#) to the table F' yields subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, $W \in \text{Gr}(\mathbb{F}_2^n, n-q)$ such that $Q \subseteq W$ and

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [F'[L] = f|_L \mid Q \subseteq L \subseteq W] \geq 2^{-Cq^2}. \quad (\text{D.8})$$

By the definition of $\mathcal{Q}$, this implies that $Q \in \mathcal{Q}$. However, as $F'[L] = \mathbf{nil}$ for any L containing a member of $\mathcal{Q}$, the left-hand side of [Equation \(D.8\)](#) must be 0, which is a contradiction. $\square$

We now move on to the second decoding theorem we need. The following lemma says that if a function F on the vertices of the Grassmann graph is locally constant on its edges, then it is globally constant inside some zoom-in/zoom-out combination.

Lemma D.8. *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose Σ is a finite set and $F[\cdot]$ is a table where $F[L] \in \Sigma \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [F[L_1] = F[L_2] \neq \mathbf{nil}] \geq 2^{-q+3}. \quad (\text{D.9})$$

Then there exist an element $\sigma \in \Sigma$ and subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, $W \in \text{Gr}(\mathbb{F}_2^n, n-q)$ such that $Q \subseteq W$ and

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [F[L] = \sigma \mid Q \subseteq L \subseteq W] \geq 2^{-Cq^2}.$$

Proof. For each element $\sigma \in \Sigma$, let $\mathcal{L}_\sigma$ denote the set of subspaces $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$ such that $F[L] = \sigma$. We have

$$\mathbb{E}_{\sigma \in \Sigma} \left[\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}_\sigma] \right] = \mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{\sigma \in \Sigma} [\sigma = F[L]] \right] \leq \frac{1}{|\Sigma|}. \quad (\text{D.10})$$

Furthermore, due to the assumption of the lemma, we have

$$\begin{aligned} \mathbb{E}_{\sigma \in \Sigma} \left[\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}_\sigma] \right] &= \mathbb{E}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{\sigma \in \Sigma} [\sigma = F[L_1] = F[L_2]] \right] \\ &= \frac{1}{|\Sigma|} \cdot \mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [F[L_1] = F[L_2] \neq \text{nil}] \geq \frac{2^{-q+3}}{|\Sigma|}. \end{aligned} \quad (\text{D.11})$$

Therefore, combining [Equations \(D.10\) and \(D.11\)](#), we know that there exists an element $\sigma \in \Sigma$ such that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [L_1, L_2 \in \mathcal{L}_\sigma] > 2^{-q+2} \cdot \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [L \in \mathcal{L}_\sigma].$$

It then follows from [Lemma D.6](#) that $\mathcal{L}_\sigma$ is not $(q, 2^{-Cq^2})$ -pseudorandom, which is exactly the desired conclusion. $\square$

Our second decoding theorem (restated below) is a similar variant of [Lemma D.8](#) with “abundant zoom-ins.”

Theorem 3.6. *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, q be nonnegative integers such that $n - q - 3 \geq \ell \geq q + 3$. Suppose Σ is a finite set and $F[\cdot]$ is a table where $F[L] \in \Sigma \cup \{\text{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell)} [F[L_1] = F[L_2] \neq \text{nil}] \geq 2^{-q+4}. \quad (3.2)$$

Then for at least $2^{-q-\ell^2}$ fraction of subspaces $Q \in \text{Gr}(\mathbb{F}_2^n, q)$, there exist an element $\sigma \in \Sigma$ and a subspace $W \in \text{Gr}(\mathbb{F}_2^n, n - q)$ containing Q such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [F[L] = \sigma \mid Q \subseteq L \subseteq W] \geq 2^{-Cq^2}.$$

Proof. One can use [Lemma D.8](#) to prove [Theorem 3.6](#) in an entirely analogous way to how [Theorem D.7](#) is used to prove [Theorem 3.5](#). $\square$

E Linearity Testing and List Decoding Bounds

In this appendix, we briefly explain how to prove [Lemma 3.9](#). The core of the proof is an ℓ -vs.- b -dimensional Grassmann agreement test, whose soundness is given by the following lemma from [\[KMS25, Theorem B.1\]](#) (see also [\[DKK⁺25, Lemma 3.1\]](#)).

Lemma E.1 ([\[KMS25, DKK⁺25\]](#)). *There is an absolute constant $C > 0$ such that the following holds. Let n, ℓ, b be positive integers such that $n \geq 2\ell$ and $40 \leq b \leq \ell/4$. Suppose $F[\cdot]$ is a table where $F[L] \in L^*$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell, b)} [F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2}] \geq \varepsilon,$$

for some parameter $\varepsilon \in [2^{4-b/4}, 1]$. Then there exists a linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [F[L] = f|_L] \geq C^{-1}\varepsilon^3.$$

The following lemma is a slight variant where some entries are allowed to be `nil`.

Lemma E.2. *There is an absolute constant $C \geq 40$ such that the following holds. Let n, ℓ, b be positive integers such that $n \geq 2\ell$ and $C \leq b \leq \ell/4$. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\mathbf{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell, b)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \right] \geq \varepsilon, \quad (\text{E.1})$$

for some parameter $\varepsilon \in [2^{4-b/4}, 1]$. Then there exists a linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \right] \geq C^{-1} \varepsilon^3.$$

Proof. We define a random table $F'[\cdot]$ as follows: for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$,

- (1) if $F[L] \neq \mathbf{nil}$, let $F'[L] = F[L]$;
- (2) if $F[L] = \mathbf{nil}$, pick a uniformly random linear functional $h \in L^*$ and let $F'[L] = h$.

Therefore, for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$ the entry $F'[L]$ always takes value in the space L^* .

For any fixed linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, the random variables

$$Z_f(L) = \mathbf{1} \left[F'[L] = f|_L \text{ and } F[L] = \mathbf{nil} \right] \quad \text{for } L \in \text{Gr}(\mathbb{F}_2^n, \ell)$$

take values in $\{0, 1\}$, have expected values at most $2^{-\ell}$, and are mutually independent. Therefore, by Chernoff bound we have

$$\begin{aligned} \mathbb{P}_{F'} \left[\frac{1}{|\text{Gr}(\mathbb{F}_2^n, \ell)|} \sum_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} Z_f(L) \geq 2^{1-\ell} \right] &\leq \exp \left(-\frac{1}{3} \cdot 2^{-\ell} \cdot |\text{Gr}(\mathbb{F}_2^n, \ell)| \right) \\ &\leq \exp \left(-\frac{1}{3} \cdot 2^{\ell(n-\ell-1)} \right) < 2^{-n}, \end{aligned}$$

where in the last transition we used the condition that $n \geq 2\ell \geq 320$. By a union bound over all linear maps $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, it follows that with nonzero probability over F' we have

$$\mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} [Z_f(L)] \leq 2^{1-\ell}.$$

In other words, there exists a realization of the random table $F'[\cdot]$, which we denote by $F_0[\cdot]$, such that

- (1) for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, we have $F_0[L] \in L^*$;
- (2) for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, we have $F_0[L] = F[L]$ whenever $F[L] \neq \mathbf{nil}$;
- (3) $\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F_0[L] = f|_L \text{ and } F[L] = \mathbf{nil} \right] \leq 2^{1-\ell}$ for any linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$.

Since $F_0[\cdot]$ only replaces the $\mathbf{nil}$ values in $F[\cdot]$, it is clear that [Equation \(E.1\)](#) also holds for F_0 , i.e.

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell, b)} \left[F_0[L_1]|_{L_1 \cap L_2} = F_0[L_2]|_{L_1 \cap L_2} \right] \geq \varepsilon,$$

and hence we may apply [Lemma E.1](#) to obtain a linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F_0[L] = f|_L \right] \geq C_0^{-1} \varepsilon^3,$$

for some absolute constant $C_0 > 0$. Combining this with the second and third properties of $F_0[\cdot]$ listed above, it follows that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \right] \geq C_0^{-1} \varepsilon^3 - 2^{1-\ell} \geq (2C_0)^{-1} \varepsilon^3,$$

where the last transition holds as long as $\varepsilon^3 \cdot 2^\ell$ is sufficiently large. $\square$

The next corollary is a version of [Lemma E.2](#) that also takes zoom-ins into account.

Corollary E.3. *There is an absolute constant $C \geq 40$ such that the following holds. Fix positive integers n, ℓ, b and a nonnegative integer q such that $n \geq 2\ell$ and $C(q+1) \leq b \leq \ell/4$. Let $Q \in \text{Gr}(\mathbb{F}_2^n, q)$ be a subspace. Suppose $F[\cdot]$ is a table where $F[L] \in L^* \cup \{\text{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$, such that*

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell, b)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \mid Q \subseteq L_1, L_2 \right] \geq \varepsilon, \quad (\text{E.2})$$

for some parameter $\varepsilon \in [2^{-b/8}, 1]$. Then there exists a linear map $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \right] \geq C^{-1} \cdot 2^{-3q} \varepsilon^3.$$

Proof. Since there are exactly 2^q linear functionals $Q \rightarrow \mathbb{F}_2$, there exists a linear functional $h \in Q^*$ such that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(\mathbb{F}_2^n, \ell, b)} \left[F[L_1]|_{L_1 \cap L_2} = F[L_2]|_{L_1 \cap L_2} \text{ and } F[L_1]|_Q = h \mid Q \subseteq L_1, L_2 \right] \geq 2^{-q} \varepsilon, \quad (\text{E.3})$$

Let $Q^c \in \text{Gr}(\mathbb{F}_2^n, n-q)$ be a linear subspace such that $Q \cap Q^c = \{0\}$. Define a table $F'[\cdot]$ as follows: for each $L \in \text{Gr}(Q^c, \ell-q)$,

- (1) if $F[L+Q] \neq \text{nil}$ and $F[L+Q]|_Q = h$, let $F'[L] = F[L+Q]|_L$;
- (2) if $F[L+Q] = \text{nil}$ or $F[L+Q]|_Q \neq h$, let $F'[L] = \text{nil}$.

It then follows from [Equation \(E.3\)](#) that

$$\mathbb{P}_{(L_1, L_2) \sim \mathcal{G}(Q^c, \ell-q, b-q)} \left[F'[L_1]|_{L_1 \cap L_2} = F'[L_2]|_{L_1 \cap L_2} \right] \geq 2^{-q} \varepsilon.$$

Applying [Lemma E.2](#) to the table $F'[\cdot]$ and then translating the conclusion back to $F[\cdot]$ yields the desired result. $\square$

We now explain how to prove [Lemma 3.9](#). The proof of [Lemma 3.9](#) (with `nil` entries disallowed) in [\[DKK⁺25\]](#) runs a sunflower argument (similar to the proof of [Lemma 6.62](#)) to show that if we have too many $(f_i, W_i) \in \text{LIST}_Q^{\vec{\tau}}(F)$ with W_i 's having the same codimension, then a subcollection of them can be “patched together” into a $(f, W) \in \text{LIST}_Q^{\vec{\tau}}(F)$ with $\text{codim } W$ smaller than the codimension of W_i 's. Since this contradicts the maximality requirement in [Definition 3.8](#), one can conclude that $\text{LIST}_Q^{\vec{\tau}}(F)$ does not contain too many pairs with the same zoom-out dimension. Since there are only $(w+1)$ possible zoom-out dimensions, the size of the list itself can consequently be bounded.

In order to allow `nil` entries, the only change one has to make to the proof is to use [Corollary E.3](#) instead of [Lemma E.1](#) as the linearity-test input. We also record the following lemma that is used both in the proof of [Lemma 3.9](#) and in the proof of [Lemma 6.62](#).

Lemma E.4 ([KMS25, Theorem 2.6]). *There is an absolute constant $C \geq 40$ such that the following holds. Fix positive integers n, ℓ, b , a nonnegative integer q and a parameter $\eta \in (0, 1)$ such that*

$$n \geq 2\ell, \quad C(q+1) \leq b \leq \ell/4, \quad \text{and} \quad \eta \geq 2^{-b/8}.$$

Let $Q \in \text{Gr}(\mathbb{F}_2^n, q)$ be a subspace. Suppose $F[\cdot]$ is a table where $F[L] \in L^ \cup \{\text{nil}\}$ for each $L \in \text{Gr}(\mathbb{F}_2^n, \ell)$. Then there are at most $2/\eta$ different linear functions $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that*

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[F[L] = f|_L \mid Q \subseteq L \right] \geq \eta. \quad (\text{E.4})$$

Proof. Let $f_1, \dots, f_m : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be the pairwise distinct linear functions satisfying Equation (E.4). Let

$$\mu = \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell), i \in [m]} \left[F[L] = f_i|_L \mid Q \subseteq L \right] \geq \eta.$$

To prove $m \leq 2/\eta$, assume on the contrary that $m > 2/\eta$. We note that for any distinct indices $i, j \in [m]$, since f_i and f_j are distinct linear functions, we have

$$\mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[f_i|_L = f_j|_L \mid Q \subseteq L \right] = \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[L \subseteq \ker(f_i - f_j) \mid Q \subseteq L \right] \leq 2^{q-\ell}.$$

Therefore, we have

$$\begin{aligned} \mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{i \in [m]} \left[F[L] = f_i|_L \right]^2 \mid Q \subseteq L \right] &= \mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{i, j \in [m]} \left[F[L] = f_i|_L = f_j|_L \right] \mid Q \subseteq L \right] \\ &\leq \frac{\mu}{m} + \frac{m-1}{m} \cdot 2^{q-\ell} \leq \frac{\mu\eta}{2} + 2^{q-\ell} < \mu^2. \end{aligned}$$

On the other hand, by Cauchy-Schwarz we have

$$\mathbb{E}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell)} \left[\mathbb{P}_{i \in [m]} \left[F[L] = f_i|_L \right]^2 \mid Q \subseteq L \right] \geq \mathbb{P}_{L \in \text{Gr}(\mathbb{F}_2^n, \ell), i \in [m]} \left[F[L] = f_i|_L \mid Q \subseteq L \right]^2 = \mu^2,$$

leading to a contradiction. $\square$

F Covering Properties

Several covering-property-type statements were left unproved in Sections 4 to 6. In this section, we complete their proofs.

F.1 Covering in the Outer PCP

We first prove Proposition 4.7 (restated below), which analyzes the distribution of E' in a sample $(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$ conditioned on $(A_{\text{in}}, A_{\text{mid}})$.

Proposition 4.7. Let E be a tripled set. Fix nonnegative integers q_1, q_2 and a parameter $\beta \in [0, 1)$. Fix arbitrary tuples

$$A_1 \in (\mathbb{F}_2^E)^{q_1} \quad \text{and} \quad A_2 \in (\mathbb{F}_2^E)^{q_2}.$$

Sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$. Then the resulting marginal distribution of E' is independent over triples of E . Furthermore, each triple of E is entirely included in E' with conditional probability at least $1 - 4^{q_1+q_2}\beta$.

Proof. We write $q = q_1 + q_2$. Without loss of generality, we assume

$$E = [3k] \quad \text{and} \quad \text{Triples}(E) = \{\{3i - 2, 3i - 1, 3i\} \mid i \in [k]\}$$

for some positive integer k .

Let $P \subseteq E$ be the union of the supports of all vectors appearing in the fixed advice sequences A_1 and A_2 . For each $i \in [k]$, let

$$P_i = \{j \in \{1, 2, 3\} \mid 3i - 3 + j \in P\}.$$

Consider a sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}([3k], q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$. Under this conditioning, the marginal distribution of E' is independent over the triples of E : for every $i \in [k]$,

- (1) if $|P_i| \geq 2$, then $3i - 2, 3i - 1$ and $3i$ are all included in E' with probability 1;
- (2) if P_i is a singleton set $\{j\}$, then $3i - 2, 3i - 1$ and $3i$ are all included in E' with probability $1 - \eta_1$, and with probability η_1 only $3i - 3 + j$ is included in E' , where

$$\eta_1 = \frac{(\beta/3)(1 - 2^{-q})}{(\beta/3)(1 - 2^{-q}) + (1 - \beta)(1 - 2^{-q})2^{-2q}} = \frac{2^{2q}\beta}{2^{2q}\beta + 3(1 - \beta)} \leq 2^{2q}\beta; \quad (\text{F.1})$$

- (3) if $P_i = \emptyset$, then $3i - 2, 3i - 1$ and $3i$ are all included in E' with probability $1 - \eta_0$, and with probability η_0 only (a uniformly random) one of them is included in E' , where

$$\eta_0 = \frac{\beta \cdot 2^{-q}}{\beta \cdot 2^{-q} + (1 - \beta)2^{-3q}} = \frac{2^{2q}\beta}{2^{2q}\beta + (1 - \beta)} \leq 2^{2q}\beta. \quad (\text{F.2})$$

In each of the above three cases, the triple $\{3i - 2, 3i - 1, 3i\}$ is included entirely in E' with probability at least $1 - 2^{2q}\beta = 1 - 4^{q_1+q_2}\beta$. $\square$

Building on the proof of [Proposition 4.7](#), we can now prove the main covering property needed for the middle PCP ([Proposition 4.8](#), restated below), which asserts that the distribution of A_{mid} is close to uniform over Alice's space even when conditioned on A_{in} (similar arguments appeared in [\[KS13, KMS25\]](#)).

Proposition 4.8. Let E be a tripled set. Fix nonnegative integers q_1, q_2 and a parameter $\beta \in [0, 4^{-q_1-q_2})$. Fix an arbitrary tuple $A_1 \in (\mathbb{F}_2^E)^{q_1}$. Sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\}$. Then the resulting marginal distribution of A_{mid} has total variation distance at most $4^{q_1+q_2}\beta\sqrt{|E|/3}$ to the uniform distribution over $(\mathbb{F}_2^E)^{q_2}$.

Proof. As in the proof of [Proposition 4.7](#), we assume

$$E = [3k] \quad \text{and} \quad \text{Triples}(E) = \{\{3i - 2, 3i - 1, 3i\} \mid i \in [k]\}$$

for some positive integer k . Let $P \subseteq E$ be the union of the supports of all vectors appearing in the fixed advice sequence A_1 . For each $i \in [k]$, let $P_i = \{j \in \{1, 2, 3\} \mid 3i - 3 + j \in P\}$. We organize the proof into the following two steps.

Step 1: description of the distribution. Similarly to [Equations \(F.1\) and \(F.2\)](#), we let

$$\eta_1 = \frac{2^{2q_1} \beta}{2^{2q_1} \beta + 3(1 - \beta)} \leq 2^{2q_1} \beta \quad \text{and} \quad \eta_0 = \frac{2^{2q_1} \beta}{2^{2q_1} \beta + (1 - \beta)} \leq 2^{2q_1} \beta.$$

Let $\mathcal{D}_0$ be the uniform distribution over

$$(\mathbb{F}_2^{q_2})^3 = \left\{ (x^{(1)}, x^{(2)}, x^{(3)}) \mid x^{(1)}, x^{(2)}, x^{(3)} \text{ are vectors in } \mathbb{F}_2^{q_2} \right\}.$$

For each $j \in [3]$, let $\mathcal{D}_j$ be the uniform distribution over the subset

$$\left\{ (x^{(1)}, x^{(2)}, x^{(3)}) \in (\mathbb{F}_2^{q_2})^3 \mid x^{(i)} = 0 \text{ for all } i \in [3] \setminus \{j\} \right\} \subseteq (\mathbb{F}_2^{q_2})^3.$$

For each $i \in [k]$, we define a distribution $\mathcal{D}^{(i)}$ over $(\mathbb{F}_2^{q_2})^3$ as follows (according to the conditional distribution of $E' \cap \{3i - 2, 3i - 1, 3i\}$ described in the proof of [Proposition 4.7](#)):

- (1) if $|P_i| \geq 2$, let $\mathcal{D}^{(i)} = \mathcal{D}_0$;
- (2) if P_i is a singleton set $\{j\}$, let $\mathcal{D}^{(i)}$ be the mixture $(1 - \eta_1)\mathcal{D}_0 + \eta_1\mathcal{D}_j$;
- (3) if $P_i = \emptyset$, let $\mathcal{D}^{(i)}$ be the mixture $(1 - \eta_0)\mathcal{D}_0 + \frac{1}{3}\eta_0\mathcal{D}_1 + \frac{1}{3}\eta_0\mathcal{D}_2 + \frac{1}{3}\eta_0\mathcal{D}_3$.

It is straightforward to verify that in each of the above three cases, for any tuple $X \in (\mathbb{F}_2^{q_2})^3$ we have

$$\left| \sqrt{\mathcal{D}^{(i)}(X)/\mathcal{D}_0(X)} - 1 \right| \leq \left| \mathcal{D}^{(i)}(X)/\mathcal{D}_0(X) - 1 \right| \leq 2^{2q_2} \max\{\eta_0, \eta_1\} \leq 2^{2q_2+2q_1} \beta. \quad (\text{F.3})$$

Now consider a sample

$$(E', A_{\text{in}}, A_{\text{mid}}) \sim \mathcal{J}_{\text{out}}([3k], q_1, q_2, \beta)$$

conditioned on the event $\{A_{\text{in}} = A_1\}$. The conditional distribution of E' is as described in the proof of [Proposition 4.7](#) and does not depend on q_2 . It is then easy to see from the proof of [Proposition 4.7](#) that the conditional distribution of A_{mid} is the output distribution of the following process:

- 1. For each $i \in [k]$, sample a tuple of three vectors $(x^{(3i-2)}, x^{(3i-1)}, x^{(3i)}) \sim \mathcal{D}^{(i)}$.
- 2. Form the $3k$ -by- q_2 matrix $X \in \mathbb{F}_2^{3k \times q_2}$ whose i -th row is $x^{(i)}$ for each $i \in [3k]$. Let $\mathcal{M}_P$ denote the resulting distribution of X .
- 3. Output the q_2 columns of X .

Step 2: tensorization of Hellinger affinity. It now suffices to show that $\mathcal{M}_P$ is close to uniform over $\mathbb{F}_2^{3k \times q_2}$ (the space of $3k$ -by- q_2 matrices).

For each $i \in [k]$, by [Equation \(F.3\)](#) we have that the squared Hellinger distance between $\mathcal{D}^{(i)}$ and $\mathcal{D}_0$ is

$$\frac{1}{2} \cdot \mathbb{E}_{X \sim \mathcal{D}_0} \left[\left(\sqrt{\mathcal{D}^{(i)}(X)/\mathcal{D}_0(X)} - 1 \right)^2 \right] \leq 2^{4q_1+4q_2-1} \beta^2,$$

and therefore

$$\sum_{X \in (\mathbb{F}_2^{q_2})^3} \sqrt{\mathcal{D}^{(i)}(X)\mathcal{D}_0(X)} = 1 - \frac{1}{2} \sum_{X \in (\mathbb{F}_2^{q_2})^3} \left(\sqrt{\mathcal{D}^{(i)}(X)} - \sqrt{\mathcal{D}_0(X)} \right)^2 \geq 1 - 2^{4q_1+4q_2-1} \beta^2.$$

Consider the distributions

$$\prod_{i=1}^k \mathcal{D}^{(i)} = \mathcal{M}_P \quad \text{and} \quad \prod_{i=1}^k \mathcal{D}_0 = \mathcal{D}_0^{\otimes k}.$$

over $\mathbb{F}_2^{3k \times q_2}$. By the tensorization we have

$$\begin{aligned} \sum_{X \in \mathbb{F}_2^{3k \times q_2}} \sqrt{\mathcal{M}_P(X) \mathcal{D}_0^{\otimes k}(X)} &= \prod_{i=1}^k \sum_{X \in (\mathbb{F}_2^{q_2})^3} \sqrt{\mathcal{D}^{(i)}(X) \mathcal{D}_0(X)} \\ &\geq (1 - 2^{4q_1+4q_2-1} \beta^2)^k \geq 1 - 2^{4q_1+4q_2-1} \beta^2 k. \end{aligned}$$

Consequently, the squared Hellinger distance between $\mathcal{M}_P$ and $\mathcal{D}_0^{\otimes k}$ is

$$\frac{1}{2} \sum_{X \in \mathbb{F}_2^{3k \times q_2}} \left(\sqrt{\mathcal{M}_P(X)} - \sqrt{\mathcal{D}_0^{\otimes k}(X)} \right)^2 \leq 2^{4q_1+4q_2-1} \beta^2 k,$$

and hence by Cauchy-Schwarz,²⁷ the total variation distance between $\mathcal{M}_P$ and $\mathcal{D}_0^{\otimes k}$ is

$$\frac{1}{2} \sum_{X \in \mathbb{F}_2^{3k \times q_2}} \left| \mathcal{M}_P(X) - \mathcal{D}_0^{\otimes k}(X) \right| \leq \sqrt{2} \cdot \sqrt{2^{4q_1+4q_2-1} \beta^2 k} = 2^{2q_1+2q_2} \beta \sqrt{k}. \quad \square$$

F.2 Covering in the Middle PCP

In the middle PCP, we introduced a new joint distribution $\mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$ based on the “thinning with advice” distribution $\mathcal{J}_{\text{out}}(E, q_1, q_2, \beta)$. Specifically, in addition to the tuple $(E', A_{\text{in}}, A_{\text{mid}})$ sampled in the latter joint distribution, a subspace $U \subseteq \mathbb{F}_2^{E'}$ is generated. Since the way we generated U in $\mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$ can be viewed as sampling “advice vectors” and taking their span, the following proposition follows rather easily from [Proposition 4.8](#).

Proposition 5.4. Let E be a tripled set. Fix a parameter $\beta \in [0, 1)$ and nonnegative integers q_1, q_2, ℓ such that $|E| \geq \ell \geq q_2$. Fix arbitrary tuples

$$A_1 \in (\mathbb{F}_2^E)^{q_1} \quad \text{and} \quad A_2 \in (\mathbb{F}_2^E)^{q_2} \quad \text{such that} \quad \dim \text{span}(A_2) = q_2.$$

Sample

$$(E', A_{\text{in}}, A_{\text{mid}}, U) \sim \mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$$

conditioned on the event $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$. Then the resulting marginal distribution of U has total variation distance at most

$$4^{q_1+\ell} \beta \sqrt{|E|/3} + 2^{\ell-|E|}$$

to the uniform distribution over the set $\{U \in \text{Gr}(\mathbb{F}_2^E, \ell) \mid \text{span}(A_2) \subseteq U\}$.

Proof. We write $q = q_1 + q_2$ and $\ell' = \ell - q_2$.

According to [Definition 5.1](#), when $(E', A_{\text{in}}, A_{\text{mid}}, U)$ is sampled from $\mathcal{J}_{\text{mid}}(E, q_1, q_2, \beta, \ell)$, a vector sequence $A' \in (\mathbb{F}_2^{E'})^{\ell'}$ is generated, and then U is taken to be the sum $\text{span}(A_{\text{mid}}) + \text{span}(A')$. Let

$$A_{\text{in}} \uplus A_{\text{mid}} \in (\mathbb{F}_2^{E'})^{q_1+q_2}$$

²⁷For any two probability vectors $p, q \in \mathbb{R}^n$, we have $\|p - q\|_1 \leq \|\sqrt{p} - \sqrt{q}\|_2 \cdot \|\sqrt{p} + \sqrt{q}\|_2 \leq 2\|\sqrt{p} - \sqrt{q}\|_2$.

denote the concatenation of the two vector sequences A_{in} and A_{mid} . Note that before any conditioning, the distribution of $(E', A_{\text{in}} \uplus A_{\text{mid}}, A')$ is identical to $\mathcal{J}_{\text{out}}(E, q, \ell', \beta)$. Therefore, it follows from [Proposition 4.8](#) that after conditioning on $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$,

$$\text{the distribution of } A' \text{ is } \left(4^{q+\ell'} \beta \sqrt{|E|/3}\right)\text{-close to uniform over } (\mathbb{F}_2^E)^{\ell'}. \quad (\text{F.4})$$

Since $\dim \text{span}(A_2) = q_2$, it is easy to see that

$$\mathbb{P}_{A \in (\mathbb{F}_2^E)^{\ell'}} [\dim(\text{span}(A_2) + \text{span}(A)) = \ell] \geq 1 - 2^{\ell-|E|}. \quad (\text{F.5})$$

Furthermore, if $A \in (\mathbb{F}_2^E)^{\ell'}$ is a uniformly random vector sequence, then the distribution of $(\text{span}(A_2) + \text{span}(A))$ conditioned on the event

$$\{\dim(\text{span}(A_2) + \text{span}(A)) = \ell\}$$

is uniform over the set $\{U \in \text{Gr}(\mathbb{F}_2^E, \ell) \mid \text{span}(A_2) \subseteq U\}$. Therefore, it follows from [Equations \(F.4\)](#) and [\(F.5\)](#) that conditioned on $\{A_{\text{in}} = A_1\} \cap \{A_{\text{mid}} = A_2\}$, the distribution of $U = (\text{span}(A_{\text{mid}}) + \text{span}(A'))$ has total variation distance at most

$$4^{q+\ell'} \beta \sqrt{|E|/3} + 2^{\ell-|E|} = 4^{q_1+\ell} \beta \sqrt{|E|/3} + 2^{\ell-|E|}$$

to the uniform distribution over $\{U \in \text{Gr}(\mathbb{F}_2^E, \ell) \mid \text{span}(A_2) \subseteq U\}$. $\square$

F.3 Covering in the Inner PCP

We finish by stating the following general probabilistic fact that establishes the covering property achieved by the lazy parallel repetition step. It is essentially the same as [Claim 2.5](#), but stated more generally in a way that is suitable for us.

Proposition F.1. Fix positive integers k, t and finite sets $\mathcal{A}_1, \dots, \mathcal{A}_t$ with $|\mathcal{A}_j| = k$ for each $j \in [t]$. Suppose that for each $j \in [t]$ there is a probability distribution μ_j over $\mathcal{A}_j$ and a surjective map $\pi_j : \mathcal{A}_j \rightarrow \mathcal{B}_j$ onto some finite set $\mathcal{B}_j$. Let $\pi : \prod_{j=1}^t \mathcal{A}_j \rightarrow \prod_{j=1}^t \mathcal{B}_j$ be the coordinate-wise map defined by

$$\pi(a_1, \dots, a_t) = (\pi_1(a_1), \dots, \pi_t(a_t)) \quad \text{for all } (a_1, \dots, a_t) \in \prod_{j=1}^t \mathcal{A}_j.$$

Define a probability distribution μ on $\prod_{j=1}^t \mathcal{A}_j$ to be the output distribution of the following process:

1. Sample a uniformly random index $c \in [t]$.
2. Sample $a_c \sim \mu_c$. For each $j \in [t] \setminus \{c\}$, sample a_j uniformly at random from $\mathcal{A}_j$.
3. Output $(a_1, \dots, a_t)$.

For each $b \in \prod_{j=1}^t \mathcal{B}_j$, let $\text{dist}(b)$ be the total variation distance between

- (1) the distribution of $a \sim \mu$ conditioned on the event $\{\pi(a) = b\}$ (if $\mathbb{P}_{a \sim \mu}[\pi(a) = b] = 0$, let $\text{dist}(b) = 1$), and
- (2) the uniform distribution over the subset $\pi^{-1}(\{b\}) \subseteq \prod_{j=1}^t \mathcal{A}_j$.

Then we have

$$\mathbb{E}_{a \sim \mu} [\text{dist}(\pi(a))] \leq \sqrt{\frac{k}{4t}}.$$

Proof. For each $j \in [t]$, let $f_j : \mathcal{A}_j \rightarrow [0, +\infty)$ be the probability density function of μ_j ; that is, let $f_j(a) = k \cdot \mu_j(\{a\})$ for all $a \in \mathcal{A}_j$. It is then easy to see that the probability density function of μ is given by

$$f(a_1, \dots, a_t) := \frac{1}{t} \sum_{j=1}^t f_j(a_j), \quad \text{for all } (a_1, \dots, a_t) \in \prod_{j=1}^t \mathcal{A}_j.$$

For each $j \in [t]$, let $g_j : \mathcal{B}_j \rightarrow [0, +\infty)$ be defined by

$$g_j(b_j) = \begin{cases} \mathbb{E}_{a_j \in \pi_j^{-1}(\{b_j\})} [f_j(a_j)], & \text{if } \pi_j^{-1}(\{b_j\}) \neq \emptyset, \\ 0, & \text{otherwise.} \end{cases}$$

For each $b \in \prod_{j=1}^t \mathcal{B}_j$, let

$$g(b) = \frac{1}{t} \sum_{j=1}^t g_j(b_j) = \mathbb{E}_{a \in \pi^{-1}(\{b\})} [f(a)].$$

For any $b \in \prod_{j=1}^t \mathcal{B}_j$ that lies in the support of g , the total variation distance between the distribution of $a \sim \mu$ conditioned on $\{\pi(a) = b\}$ and the uniform distribution over $\pi^{-1}(\{b\})$ is

$$\begin{aligned} \frac{1}{2} \cdot \mathbb{E}_{a \in \pi^{-1}(\{b\})} \left[\left| \frac{f(a)}{g(b)} - 1 \right| \right] &\leq \frac{1}{2g(b)} \sqrt{\text{Var}_{a \in \pi^{-1}(\{b\})} [f(a)]} && \text{(by Cauchy-Schwarz)} \\ &= \frac{1}{2t \cdot g(b)} \sqrt{\sum_{j=1}^t \text{Var}_{a_j \in \pi_j^{-1}(b_j)} [f_j(a_j)]} \\ &\quad \text{(using the fact that } \pi^{-1}(\{b\}) \text{ is a product set)} \\ &\leq \frac{1}{2t \cdot g(b)} \sqrt{\sum_{j=1}^t k \cdot \mathbb{E}_{a_j \in \pi_j^{-1}(b_j)} [f_j(a_j)]} && (f_j \text{ is upper-bounded by } k) \\ &\leq \frac{1}{2} \sqrt{\frac{k}{t \cdot g(b)}} && \text{(by the definition of } g(b)) \end{aligned}$$

Let ν be the distribution of $\pi(a)$ when a is sampled uniformly from $\prod_{j=1}^t \mathcal{A}_j$. We then have

$$\mathbb{E}_{a \sim \mu} [\text{dist}(\pi(a))^2] = \mathbb{E}_{b \sim \nu} [g(b) \cdot \text{dist}(b)^2] \leq \mathbb{E}_{b \sim \nu} \left[\frac{k}{4t} \right] = \frac{k}{4t},$$

and hence $\mathbb{E}_{a \sim \mu} [\text{dist}(\pi(a))] \leq \sqrt{k/(4t)}$ by Cauchy-Schwarz. □