

# Linear Space Streaming Lower Bounds for Approximating CSPs

Chi-Ning Chou\*    Alexander Golovnev†    Madhu Sudan‡    Ameya Velingker§  
 Santhoshini Velusamy¶

## Abstract

We consider the approximability of constraint satisfaction problems in the streaming setting. For every constraint satisfaction problem (CSP) on  $n$  variables taking values in  $\{0, \dots, q - 1\}$ , we prove that improving over the trivial approximability by a factor of  $q$  requires  $\Omega(n)$  space even on instances with  $O(n)$  constraints. We also identify a broad subclass of problems for which any improvement over the trivial approximability requires  $\Omega(n)$  space. The key technical core is an optimal,  $q^{-(k-1)}$ -inapproximability for the Max  $k$ -LIN-mod  $q$  problem, which is the Max CSP problem where every constraint is given by a system of  $k - 1$  linear equations mod  $q$  over  $k$  variables.

Our work builds on and extends the breakthrough work of Kapralov and Krachun (Proc. STOC 2019) who showed a linear lower bound on any non-trivial approximation of the Max-Cut problem in graphs. MaxCut corresponds roughly to the case of Max  $k$ -LIN-mod  $q$  with  $k = q = 2$ . For general CSPs in the streaming setting, prior results only yielded  $\Omega(\sqrt{n})$  space bounds. In particular no linear space lower bound was known for an approximation factor less than  $1/2$  for *any* CSP. Extending the work of Kapralov and Krachun to Max  $k$ -LIN-mod  $q$  to  $k > 2$  and  $q > 2$  (while getting optimal hardness results) is the main technical contribution of this work. Each one of these extensions provides non-trivial technical challenges that we overcome in this work.

---

\*Center for Computational Neuroscience, Flatiron Institute, New York, New York, USA. Research supported in part by the Simons Foundation, and by NSF grants DMS-2134157 and CCF-1565264, DARPA grant W911NF2010021, DOE grant DE-SC0022199. Email: [cchou@flatironinstitute.org](mailto:cchou@flatironinstitute.org).

†Department of Computer Science, Georgetown University. Supported in part by the NSF CAREER award (grant CCF2338730). Email: [alexgolovnev@gmail.com](mailto:alexgolovnev@gmail.com).

‡School of Engineering and Applied Sciences, Harvard University, Cambridge, Massachusetts, USA. Supported in part by a Simons Investigator Award and NSF Awards CCF 1715187 and CCF 2152413. Email: [madhu@cs.harvard.edu](mailto:madhu@cs.harvard.edu).

§This work was done while the author was at Google Research. Email: [ameyav@gmail.com](mailto:ameyav@gmail.com).

¶Toyota Technological Institute at Chicago, Illinois, USA. Supported in part by a Google Ph.D. Fellowship, a Simons Investigator Award to Madhu Sudan, and NSF Awards CCF 1715187, CCF 2152413, and CCF 2348475. Email: [santhoshinivelusamy@gmail.com](mailto:santhoshinivelusamy@gmail.com).

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Background . . . . .	3
1.2	Results . . . . .	3
1.3	Prior work . . . . .	4
1.4	Techniques and new contributions . . . . .	5
1.5	Organization of the rest of the paper . . . . .	9
<b>2</b>	<b>Preliminaries</b>	<b>9</b>
2.1	Total variation distance . . . . .	9
2.2	Concentration inequality . . . . .	10
2.3	Fourier analysis . . . . .	10
<b>3</b>	<b>Communication problems</b>	<b>14</b>
<b>4</b>	<b>Streaming problems and hardness</b>	<b>17</b>
4.1	Some examples . . . . .	20
<b>5</b>	<b>Lower bound on the communication complexity</b>	<b>21</b>
5.1	Proof of Theorem 3.5 . . . . .	24
5.2	Posterior sets and functions . . . . .	25
5.3	Fourier analytic conditions . . . . .	27
5.3.1	Three key definitions . . . . .	27
5.3.2	Three key lemmas . . . . .	29
5.4	Proof of Lemma 5.1 . . . . .	31
<b>6</b>	<b>Analysis of bounded functions</b>	<b>34</b>
6.1	Fourier coefficients of the posterior function . . . . .	34
6.2	Basic properties of large weakly-bounded sets . . . . .	36
6.3	Proof of the “posterior set” lemma . . . . .	39
6.4	Proof: boundedness implies near uniformity . . . . .	45
6.5	Proof of the “induction step” lemma . . . . .	51

# 1 Introduction

In this work we consider the *approximability of constraint satisfaction problems (CSPs) by streaming algorithms* with sublinear space. We give tight inapproximability results for a broad class of CSPs, while giving somewhat weaker bounds on the approximability of every CSP. We introduce these terms below.

## 1.1 Background

We consider the general class of constraint satisfaction problems with finite constraints over finite-valued variables. A *problem* in this class, denoted  $\text{Max-CSP}(\mathcal{F})$ , is given by positive integers  $q$  and  $k$  and a family of functions  $\mathcal{F} \subseteq \{f : \mathbb{Z}_q^k \rightarrow \{0, 1\}\}$ . An *instance* of the problem consists of  $m$  constraints placed on  $n$  variables that take values in the set  $\mathbb{Z}_q = \{0, \dots, q-1\}$ , where each constraint is given by a function  $f \in \mathcal{F}$  and  $k$  distinct indices of variables  $j_1, \dots, j_k \in [n]$ . Given an instance  $\Psi$  of  $\text{Max-CSP}(\mathcal{F})$ , the goal is to compute the *value*  $\text{val}_\Psi$  defined to be the maximum, over all assignments to  $n$  variables, of the fraction of constraints satisfied by the assignment. For  $\alpha \in [0, 1]$ , the goal of the  $\alpha$ -approximate version of the problem is to compute an estimate  $\eta$  such that  $\alpha \cdot \text{val}_\Psi \leq \eta \leq \text{val}_\Psi$ .

In this work we consider the space complexity of approximating  $\text{Max-CSP}(\mathcal{F})$  by a single pass (potentially randomized) streaming algorithm that is presented the instance  $\Psi$  one constraint at a time. We consider “non-trivial” approximation algorithms for  $\text{Max-CSP}(\mathcal{F})$ , where we first dismiss two notions of “triviality”. First note that since we only consider space restrictions but not time restrictions, one can sample  $O(n)$  constraints of  $\Psi$  and solve the  $\text{Max-CSP}(\mathcal{F})$  problem on the sampled constraints optimally to get a  $(1 - \varepsilon)$ -approximation algorithm for every constant  $\varepsilon > 0$  in  $\tilde{O}(n)$  space. Thus for this paper we view non-trivial algorithms to be those that run in  $o(n)$  space.<sup>1</sup> The other form of “triviality” we dismiss is in the approximation factor. Given a family  $\mathcal{F}$ , let  $\rho_{\min}(\mathcal{F})$  denote the infimum, over all instances  $\Psi$  of  $\text{Max-CSP}(\mathcal{F})$ , of the value  $\text{val}_\Psi$ . Note that the algorithm that outputs the constant  $\rho_{\min}(\mathcal{F})$  is a  $(O(1)$ -space!)  $\rho_{\min}(\mathcal{F})$ -approximation algorithm for  $\text{Max-CSP}(\mathcal{F})$ . Thus we consider  $\rho_{\min}(\mathcal{F})$  to be the “trivial” approximation factor for a family  $\mathcal{F}$ . With these two notions of “triviality” in mind, we define  $\text{Max-CSP}(\mathcal{F})$  to be  $\alpha$ -*approximable* (in the streaming setting) if  $\alpha$  is the largest constant such that there exists an  $\alpha$ -approximation algorithm for  $\text{Max-CSP}(\mathcal{F})$  using  $o(n)$  space. We simply say that  $\text{Max-CSP}(\mathcal{F})$  is *approximable* (in the streaming setting) if it is  $\alpha$ -approximable for some  $\alpha > \rho_{\min}(\mathcal{F})$ . We define a problem to be *approximation-resistant* (in the streaming setting) otherwise.

## 1.2 Results

Our first main result in this paper gives a sufficient condition for a problem to be approximation resistant in the streaming setting. We say that  $f : \mathbb{Z}_q^k \rightarrow \{0, 1\}$  is a *wide* constraint if there exists  $\mathbf{a} \in \mathbb{Z}_q^k$  such that for every  $i \in \mathbb{Z}_q$  we have  $f(\mathbf{a} + i^k) = 1$  where  $i^k = (i, i, \dots, i)$  and addition is performed in the group  $\mathbb{Z}_q^k$ . We say that a family  $\mathcal{F}$  is *wide* if every function  $f \in \mathcal{F}$  is wide.

**Theorem 1.1.** *For every  $q, k$  and every wide family  $\mathcal{F}$ ,  $\text{Max-CSP}(\mathcal{F})$  is approximation-resistant.*

Many natural CSPs are wide, including Max  $q$ -colorability and Boolean problems such as Max  $k$ -SAT. Others, such as Max  $k$ -LIN-mod  $q$  and the “Unique Games” problem, contain wide subfamilies with the same “trivial” approximation factor, and thus [Theorem 1.1](#) implies these are

---

<sup>1</sup>We note that there is a gap between the  $o(n)$  space we allow and the  $O(n \log n)$  space that is trivial, but we are not able to get sharp enough lower bounds to address this gap.

also approximation resistant. We elaborate on some of these examples in [Section 4.1](#). However, clearly wideness does not capture all CSPs. For general CSPs, while we do not pin down the approximability exactly, we do manage to pin it down up to a multiplicative factor of  $q$ .

**Theorem 1.2.** *For every  $q, k$  and every family  $\mathcal{F}$ , if  $\mathcal{F}$  is  $\alpha$ -approximable then  $\alpha \in [\rho_{\min}(\mathcal{F}), q \cdot \rho_{\min}(\mathcal{F})]$ .*

Both [Theorems 1.1](#) and [1.2](#) follow from our more detailed [Theorem 4.3](#). In [Section 4.1](#) we give a few examples illustrating how our theorems give tight lower bounds for some commonly studied CSPs including Max  $q$ -coloring, Unique Games, and Max Linear Systems.

Neither of the theorems above gives a complete classification of the approximability of CSPs in sublinear space. Contrasting with [\[CGSV21a\]](#) one may have hoped that all lower bounds in [\[CGSV21a\]](#) might simply extend, from ruling out  $o(\sqrt{n})$ -space sketching algorithms, to ruling out  $o(n)$ -space sketching algorithms. However subsequent work has shown that this hope is not realizable. Specifically Saxena, Singer, Sudan and Velusamy [\[SSSV23\]](#) have shown that the Max Dicut problem allows an  $\tilde{O}(\sqrt{n})$ -space sketching algorithm that gets a .485 which beats the  $4/9$ -approximation upper bound for  $o(\sqrt{n})$ -space algorithms, from the work of Chou, Golovnev and Velusamy [\[CGV20\]](#). Indeed there seems to be broader class of problems that might allow such improvements in  $o(n)$ -space. This is hinted at in the work of Singer [\[Sin23\]](#) who shows that for every  $k \geq 2$ , there is a  $\tilde{O}(n^{1-1/k})$ -space algorithm for *bounded-degree* instances of the Max  $k$ -AND problem that beats the approximability upper bound given in Boyland, Hwang, Prasad, Singer and Velusamy [\[BHP<sup>+</sup>22\]](#) for  $o(\sqrt{n})$ -space sketching algorithms. (A CSP instance has bounded degree if each variable appears in  $O(1)$  constraints. Note that all lower bounds in this paper and prior works are proven for bounded degree instances.) And for the Max Dicut problem on bounded degree instances, Saxena, Singer, Sudan and Velusamy [\[SSSV25\]](#) gave  $1/2 - \varepsilon$  approximation algorithms, for every  $\varepsilon > 0$ , using  $o(n)$  space. Their result was recently generalized to arbitrary instances by Azarmehr, Behnezhad, Ferante, and Sanneian [\[ABFS25\]](#). Thus the class of problems for which linear space upper bounds on the approximability match the performance of polylogarithmic space sketching algorithms is a strict subclass of all MaxCSPs. Finding where exactly this boundary lies remains a wide open question.

### 1.3 Prior work

There have been a number of works in the broad area of approximations for streaming constraint satisfaction problems and lower bound techniques for those [\[GKK<sup>+</sup>09, VY11, KKS15, AKL16, KKS17, GVV17, GT19, KK19, CGV20, AKSY20, AN21, CGSV21a, SSV21\]](#). Among these our work is the *first work to aim to get tight inapproximability results for a broad class of CSPs for almost linear space single-pass streaming algorithms*. Previous works either did not get tight approximation factors or were aimed at specific problems or only got  $\Omega(\sqrt{n})$ -space lower bounds, though some do target multi-pass streaming algorithms [\[AKSY20, AN21\]](#) — which we do not do here. We describe the state of the art prior to our work below. (More detailed descriptions of prior works can be found in [\[CGSV21a\]](#).)

On the front of general lower bounds, Chou, Golovnev, Sudan and Velusamy [\[CGSV21a\]](#) explored the same set of CSP problems as we do, i.e,  $\text{Max-CSP}(\mathcal{F})$  for arbitrary  $q, k$  and  $\mathcal{F}$ . Their focus is on looser space lower bounds: specifically, they focus on problems that require  $n^{\Omega(1)}$  space vs. those where  $n^{o(1)}$  space suffices. They give a complete dichotomy for sketching algorithms, a special class of streaming algorithms. They also give sufficient conditions for approximation resistance with respect to sub-polynomial space general streaming algorithms. [Theorem 2.9](#) in their paper shows that families  $\mathcal{F}$  where the satisfying assignments of every function in the class support

a one-wise independent distribution are approximation resistant. This theorem is incomparable with our [Theorem 1.1](#) in that they give approximation resistance for a broader collection of problems (all wide families support one-wise independence) but the space lower bound is weaker — they give an  $\Omega(\sqrt{n})$  lower bound and we get  $\Omega(n)$  lower bounds for wide families. [\[CGSV21a\]](#) does not give an analogue of our [Theorem 1.2](#), though such a result (with the weaker  $\Omega(\sqrt{n})$  space lower bound) can be derived from their theorems equally easily. Indeed, our [Section 4](#) is based on their work.

Turning to linear space lower bounds, the breakthrough work here is due to Kapralov and Krachun [\[KK19\]](#), who show that approximating Max Cut (which translates in our setting to  $\text{Max-CSP}(\mathcal{F})$  for  $\mathcal{F} = \{\oplus_2\}$  where  $\oplus_2 : \{0, 1\}^2 \rightarrow \{0, 1\}$  is the binary XOR function) to within a factor  $\frac{1}{2} + \varepsilon$  requires  $\Omega(n)$  space for every  $\varepsilon > 0$ . Indeed, our work builds on their work and we compare our techniques later. Prior to the work of Kapralov and Krachun, there was a weaker result due to Kapralov, Khanna, Sudan and Velingker [\[KKS17\]](#) showing that there exists  $\varepsilon > 0$  such that  $(1 - \varepsilon)$ -approximation for Max Cut requires linear space. Finally, Chou, Golovnev and Velusamy [\[CGV20\]](#) get a tight inapproximability for Max Exact 2-SAT (corresponding to  $\text{Max-CSP}(\mathcal{F})$  for  $\mathcal{F} = \{\vee_2\}$ , where  $\vee_2 : \{0, 1\}^2 \rightarrow \{0, 1\}$  is the binary OR function) for linear space algorithms, by a reduction from Max Cut.

Thus, prior to our work it was conceivable (though of course extremely unlikely) that every  $\text{Max-CSP}(\mathcal{F})$  allowed a  $1/2$ -approximating streaming algorithm using  $o(n)$  space. Our work is the first to prove inapproximability  $\alpha \leq 1/2$  for any  $\text{Max-CSP}(\mathcal{F})$ . Indeed, we get inapproximabilities going to 0 either as  $q \rightarrow \infty$  (e.g., for the Unique Games problem) or as  $k \rightarrow \infty$  (e.g., for the Max  $k$ -equality problem with  $q = 2$  as defined later in [Section 1.4](#)).

The main contribution of our work is to extend the techniques of [\[KK19\]](#) to problems beyond Max Cut. Indeed the bulk of our proof takes the tour-de-force proof in [\[KK19\]](#) and finds the correct replacements in our setting. In the process, we arguably even present cleaner abstractions of their work. We elaborate on this further in the next section but first comment on why we feel the extensions are not straightforward given [\[KK19\]](#). First we note that the exact class of problems we are able to deal with in [Theorem 1.1](#) is not the fullest extension one may hope for. At the very least we have expected to cover the same set of problems as [\[CGSV21a, Theorem 2.9\]](#), i.e., families supporting one-wise independent distributions, but this remains open. Indeed to get our extensions we have to formulate a new communication problem which generalizes the one in [\[KK19\]](#) and is different from the many variations considered in [\[CGSV21b\]](#) and [\[CGSV21a\]](#). In particular we are forced to work with a less expressive set of communication problems that already forces a “linear-algebraic” restriction on the core problems we work with. (We do believe a slight extension of our results to “families containing one-wise independent cosets of  $\mathbb{Z}_q^k$ ” should be more feasible.) Having identified the right set of problems, carrying out the proof of Kapralov and Krachun is still non-trivial. In particular one has to be careful to ensure that the improvement in the exponent of the space bound (from  $n^{1/2}$  to  $n$ ) is by a full factor of 2 and not a factor of  $k/(k - 1)$ , which is what one natural extension would lead to! We comment on these improvements in greater detail in the following.

## 1.4 Techniques and new contributions

There are two lines of previous work that seem relevant to this work and we discuss our technical contributions relative to those here. We start with quick comparison with the previous work [\[CGSV21a\]](#) that gives  $\Omega(\sqrt{n})$  lower bounds for a broader subset of problems than those addressed in this paper. We then move on to the work [\[KK19\]](#) which is much closer to our work and needs more detailed comparison.

**Comparison with [CGSV21a].** While there is some obvious overlap in the set of problems considered in [CGSV21a] and this paper (and also in the set of authors) we claim that, beyond this aspect, the overlap in techniques is minimal. Both papers do use lower bounds on communication problems to establish lower bounds on streaming CSPs (which is standard in the context of streaming lower bounds). But the exact set of communication problems is different, and the tools used to establish the lower bounds are also different. In particular, [CGSV21a] create roughly a new communication problem for every  $\gamma, \beta$  and  $\mathcal{F}$  and the main technical contributions there are lower bounds for these problems achieved mainly through a rich set of reductions among these communication problems. In our work we essentially work with one communication problem (once we fix  $k$  and  $q$ ) and the core of our work is proving a lower bound for this problem. (This lower bound is based on extending [KK19] and we will elaborate on this later.) We use this one problem to get hardness for many different  $\gamma, \beta$  and  $\mathcal{F}$  — this part is arguably related to the work of [CGSV21a] but we feel this is the obvious part of their work as well as our work. Finally, turning to the communication problems, the natural communication problems used to analyze streaming complexity involves one way communication among a large constant number of players. The exact problem of this type that we focus on is different from the ones considered in [CGSV21a] due to a concept we call “folding”. Folding makes our problems too restrictive to work for [CGSV21a] (i.e., would prevent them for addressing every  $(\gamma, \beta) - \text{Max-CSP}(\mathcal{F})$ ), whereas we do not know how to get our lower bounds without folding. We also note that [CGSV21a] derive their multiplayer lower bounds from lower bounds for a corresponding 2-player game and all their reductions work only for these 2-player games, which are inherently limited to yielding  $\Theta(\sqrt{n})$  space lower bounds.

We now turn to the more significant comparison, with [KK19]. We start with a quick review of the main steps of [KK19] and then describe our analysis and conclude with a summary of the differences/new contributions relative to [KK19].

**Summary of [KK19].** Kapralov and Krachun [KK19] work with a distributional  $T$ -player one-way communication game for some constant  $T$ . The game also has a parameter  $\alpha > 0$ . In instances of length  $n$  of this game,  $T$  players  $P_1, \dots, P_T$  get partial matchings  $M_1, \dots, M_T$  on the vertex set  $[n]$  along with respective binary labels  $\mathbf{z}_1, \dots, \mathbf{z}_T$  on the edges of the matchings, i.e., player  $t$  receives input  $(M_t, \mathbf{z}_t)$ . Each partial matching contains  $\alpha n$  edges, while each corresponding label  $\mathbf{z}_t$  is an element of  $\{0, 1\}^{\alpha n}$ . In the communication game, the players sequentially broadcast messages as follows. Player  $t \in [T - 1]$  computes a small message  $c_t$  which is a function of  $M_t, \mathbf{z}_t$  and all “previous messages”  $c_1, \dots, c_{t-1}$ ,<sup>2</sup> after which the  $T$ -th player outputs a single 0/1 bit that is said to be the output of the communication protocol. The complexity of the protocol is the maximum over  $t \in [T]$  of the message length  $c_t$ , and the goal of the players is to distinguish input instances drawn according to a **YES** distribution from those drawn according to a **NO** distribution, defined as follows.

In instances chosen from the **NO** distribution, the matchings  $M_1, \dots, M_T$  are chosen uniformly and independently from the set of matchings containing  $\alpha n$  edges on the vertex set  $[n]$ . Furthermore, the vectors  $\mathbf{z}_1, \dots, \mathbf{z}_T$  are chosen uniformly and independently from  $\{0, 1\}^{\alpha n}$ . In the **YES** distribution, the matchings are chosen as in the **NO** distribution, but in order to generate  $\mathbf{z}_1, \dots, \mathbf{z}_T$ , we choose a common hidden vector  $\mathbf{x}^* \in \{0, 1\}^n$  uniformly at random and set each  $\mathbf{z}_t$  as  $\mathbf{z}_t(e) = x_a^* \oplus_2 x_b^*$  for every edge  $e = (a, b)$ . Thus, the label  $\mathbf{z}_t$  can be viewed as specifying which edges of the  $i$ -th matching cross the cut determined by  $\mathbf{x}^*$ . If  $T \gg \frac{1}{\alpha}$  then it can be seen that the **YES** and **NO** distributions are very far. The key theorem shows that for every  $\alpha > 0$  and  $T$ , any

<sup>2</sup>For technical reasons the lower bounds are proved in the stronger model where player  $t$  gets  $M_1, \dots, M_{t-1}$  as well, but this difference is not crucial for the current discussion.

protocol distinguishing **YES** instances from **NO** instances with constant advantage requires  $\Omega(n)$  space. With this lower bound a space lower bound on Max Cut is straightforward.

Turning to the communication lower bound, the focus of the analysis are the sets  $B_1, \dots, B_T \subseteq \{0, 1\}^n$  corresponding to the purported hidden vector  $\mathbf{x}^*$  that are consistent with the messages  $c_1, \dots, c_T$ . Specifically for  $t \in [T]$ ,  $B_t$  is the set of all vectors  $\mathbf{x}^*$  that are consistent with the first  $t$  matchings  $M_{1:t}$  and the first  $t$  messages  $c_{1:t}$ . Kapralov and Krachun [KK19] argue that the sets  $B_t$  are not shrinking too fast (in either the **YES** case or the **NO** case) using a property that they term “ $C$ -boundedness,” defined by the Fourier spectrum of the indicator function of  $B_t$  (the function from  $\{0, 1\}^n$  to  $\{0, 1\}$  that is 1 on  $B_t$ ). We do not give the exact definition of boundedness here but roughly describe it as follows: Given an arbitrary set  $B$  of size  $S$  and a Fourier weight  $w$ , the total Fourier mass (strictly the  $\ell_1$ -mass) of the  $w$ -th level Fourier coefficients of  $B$  is well-known (by classical Fourier analysis) to be bounded by some amount  $U(w) = U_{S,n}(w)$ . For  $C$ -bounded sets, the corresponding Fourier mass is required to be at most  $C^w U(w/2)$ . The factor of two gained here in the argument of  $U$  is the crux to improvement in the space lower bound from  $\sqrt{n}$  to  $n$ . (If the right hand side had been of the form  $C^w U(\alpha w)$  then the space lower bound would be  $\Omega(n^{1/(2\alpha)})$ .) This factor of two, in turn, is attributable to the fact that the  $\mathbf{z}_t$  only contain information about pairs of bits of  $\mathbf{x}^*$ . Their analysis shows that, for every  $t$ ,  $B_t$  is  $C_t$ -bounded for some constant  $C_t$ . (The proof is inductive on  $t$  but the inductive hypothesis is complex and we won’t reproduce it here.) They further show that if  $B_T$  is  $C$ -bounded for some constant  $C$ , then the distinguishing probability is at most  $o(1)$ .

**Our Analysis.** The core of our paper essentially focuses on the setting posed by one problem for every given  $q$  and  $k$ , which we call Max  $k$ -LIN-mod  $q$ . This is the MaxCSP problem where every constraint is a conjunction of  $k - 1$  linear equations on  $k$  variables. Our main lower bound aims to prove a tight  $q^{-(k-1)} + \varepsilon$ -inapproximability of this problem for every  $q$ ,  $k$  and  $\varepsilon > 0$ . (See Theorem 3.5 and the following remark.) We formally prove this in approximability in Example 4 in Section 4.1 where we consider an even broader set of problems Max-Lin $_{k,r,q}$  whose constraints are conjunctions of  $r$  linear equations over  $k$  variables and give a tight  $q^{-r} + \varepsilon$  inapproximability for this problem for every  $1 \leq r \leq k - 1$ .

To study this problem we introduce a  $T$ -player communication problem that we call the “Implicit Randomized Mask Detection Problem” (IRMD) described as follows: There are  $T$  players each of whom receives an  $\alpha n$   $k$ -hypermatching  $M_t$  (i.e., a set of  $\alpha n$   $k$ -uniform hyperedges on  $[n]$  that are pairwise disjoint). Additionally, the players receive a label in  $\mathbb{Z}_q^k$  for every hyperedge they see. Thus the  $i$ -th player’s input is  $(M_t, \mathbf{z}_t)$  where  $\mathbf{z}_t \in (\mathbb{Z}_q^k)^{\alpha n}$ . In the **NO** distribution the  $\mathbf{z}_t$ ’s are drawn uniformly. In the **YES** distribution a vector  $\mathbf{x}^* \in [q]^n$  is drawn uniformly and the label associated with an edge  $\mathbf{j} = (j_1, \dots, j_k)$  is  $(x_{j_1}^* + a_{\mathbf{j}}, \dots, x_{j_k}^* + a_{\mathbf{j}})$  where  $a_{\mathbf{j}} \in [q]$  is chosen uniformly and independently for each edge in each matching. The goal of the players is to distinguish between the **YES** and **NO** distributions with minimal communication (with “one-way” communication from the  $t$ -th player to all higher numbered players, as before).

To lower bound the communication complexity of IRMD we consider a folded version of the problem we call IFRMD where the labels associated with an edge are from  $\mathbb{Z}_q^{k-1}$  and obtained by mapping an IRMD label  $\mathbf{z} = (z^{(1)}, \dots, z^{(k)}) \in \mathbb{Z}_q^k$  to the label  $\bar{\mathbf{z}} = (z^{(2)} - z^{(1)}, \dots, z^{(k)} - z^{(1)})$ . With this folding we recover the same communication problem as [KK19] for the case of  $k = q = 2$  and the main focus of our work is proving lower bounds for higher  $k$  and  $q$ .

Our analysis of the communication complexity of IFRMD follows the same sequence of steps (with imitation even within the steps) as [KK19]. In particular we also use the same sets  $B_1, \dots, B_T$  and use the same notion of boundedness.

Turning to the induction and the analysis of boundedness of  $B_t$  for general  $t$ , we are able to extract a clean lemma (Lemma 5.20) that makes the induction completely routine. To explain this contribution note that  $B_t$  is the intersection of  $B_{t-1}$  with a set say  $A_t$  where  $A_t$  is of the same type as  $B_t$  (both are obtained by looking at the vector  $\mathbf{x}^*$  projected to a matching followed by some folding). Thus both  $B_{t-1}$  and  $A_t$  are bounded sets. To complete the induction it would suffice to prove that the intersection of bounded sets is bounded, but alas this is not true! To get that  $B_t$  is bounded, we need to use the fact that the matching  $M_t$  is random and chosen independently of  $B_{t-1}$  but it turns out that that is all that is needed. This is exactly what we show in Lemma 5.20 — and of course this only happens with high probability over the choice of  $M_t$ .

**Incremental contribution over [KK19].** Given that our result closely follows [KK19] we now focus on some key differences, and why these contributions are conceptually significant.

1. The analysis of [KK19] is intricate and it is not a priori clear what problems it may extend to. Our choice of Max  $k$ -LIN-mod  $q$  is not the obvious choice, and was not our first choice. More natural choices would be to go for more general linear systems, or even functions supporting “one-wise independence”, but we are unable to push the analysis to more general cases. Our choice reflects an adequate one to get coarse bounds on the approximability of every problem while getting tight ones for many natural ones.
2. The choice of the communication problems to work with is also not obvious: Indeed working with both IRMD and IFRMD seems necessary for our approach — the former is more useful for our final inapproximability results whereas the latter is the one we are able to analyze.
3. The exact notion of boundedness that is necessary and sufficient for our results is also not completely obvious. It is only in hindsight, after carrying out the entire analysis, does it become clear that the notion that works is exactly the same as the one in [KK19]. Part of the challenge is that in the inductive proof of boundedness even the base case (which is quite simple in [KK19]) is not obvious in our case, and nor is the inductive step.
  - With respect to the base case we note that if we had adopted a weaker notion of boundedness allowing  $w$ -th level Fourier mass to grow roughly as  $U((k-1)w/k)$  boundedness would have been easier to prove but the result would not be optimal. Getting a bound of  $U(w/2)$  is not technically hard, but involves a non-trivial randomization in the choice of folding purely for analysis purposes. (So there is an implicit passing back and forth between the IRMD and IFRMD problems in this technical step.)
  - We also feel that it is important that we are able to extract an induction lemma (Lemma 5.20) that clearly separates the (Fourier and combinatorial) analytic ingredients from the probabilistic setup. We believe the lemma is clarifying even when applied to the proof of [KK19].
4. Finally we note that the underlying combinatorics are made significantly more intricate due to the need to work with  $k > 2$ . A conceptual difference from [KK19] here is that whereas they explore the distribution of the number of edges in a random matching that intersect with a fixed set of vertices, we have to explore the distribution of edges that have an odd intersection (or non-zero mod  $q$  intersection) with a random hypermatching. Indeed this part is clarifying the role of some of the quantities explored in the previous work. Additionally, we note that the number of parameters we have to track is much larger (and indeed it is fortunate that the number of parameters remains a constant independent of  $k$ ), and managing these in our inequalities is a non-trivial technical challenge (even given the heavy lifting in [KK19]).

## 1.5 Organization of the rest of the paper

We start with some background material in [Section 2](#). We introduce our communication problems (IRMD and IFRMD) in [Section 3](#) and state our lower bounds for these. We use these lower bounds on communication problems to prove our streaming lower bounds in [Section 4](#), and turn to proving the communication lower bounds in [Section 5](#). To do so, [Section 5](#) introduces the notion of bounded sets, states three lemmas on the properties of bounded sets, and proves the lower bound assuming these lemmas on the boundedness of sets encountered by the protocol. Finally [Section 6](#) proves these lemmas on boundedness, concluding the proofs.

## 2 Preliminaries

We use the following notations throughout the paper. Let  $\mathbb{N} = \{1, \dots\}$  denote the set of natural numbers and let  $[n] = \{1, 2, \dots, n\}$ . For a discrete set  $X$  and a function  $f : X \rightarrow \mathbb{R}$ , we denote  $\|f\|_p = (\sum_{x \in X} |f(x)|^p)^{1/p}$  for every  $p > 0$  and  $\|f\|_0 = \sum_{x \in X} \mathbf{1}_{f(x) \neq 0}$ . For a sequence of objects  $O_1, O_2, \dots, O_T$ , we define  $O_{1:t} = \{O_1, O_2, \dots, O_t\}$  for every  $t \in [T]$ .

### 2.1 Total variation distance

In our analysis we will use the total variation distance between probability distributions, and several bounds on it presented in this section.

**Definition 2.1** (Total variation distance of discrete random variables). *Let  $\Omega$  be a finite probability space and  $X, Y$  be random variables with support  $\Omega$ . The total variation distance between  $X$  and  $Y$  is defined as follows.*

$$\|X - Y\|_{tvd} := \frac{1}{2} \sum_{\omega \in \Omega} |\Pr[X = \omega] - \Pr[Y = \omega]| .$$

We will use the triangle and data processing inequalities for the total variation distance.

**Proposition 2.2** (E.g.,[\[KKS15, Claim 6.5\]](#)). *For random variables  $X, Y$  and  $W$ :*

- (Triangle inequality)  $\|X - Y\|_{tvd} \geq \|X - W\|_{tvd} - \|Y - W\|_{tvd}$ .
- (Data processing inequality) *If  $W$  is independent of both  $X$  and  $Y$ , and  $f$  is a function, then  $\|f(X, W) - f(Y, W)\|_{tvd} \leq \|X - Y\|_{tvd}$ .*

**Lemma 2.3.** *Let  $X, Y, W$  be random variables and let  $f$  be a function. If there exists  $\delta > 0$  such that for every fixed  $x$  in the support of  $X$ , we have*

$$\|f(x, Y) - f(x, W)\|_{tvd} \leq \delta ,$$

*then the following holds:*

$$\|(X, f(X, Y)) - (X, f(X, W))\|_{tvd} \leq \delta .$$

*Proof.* Consider any statistical test<sup>3</sup>  $T$  distinguishing the joint distributions  $(X, f(X, Y))$  and  $(X, f(X, W))$ . It suffices to prove that

$$\mathbb{E}_{X,Y}[T(X, f(X, Y))] - \mathbb{E}_{X,W}[T((X, f(X, W)))] \leq \delta .$$

<sup>3</sup>That is,  $T(X, Z)$  is a Boolean function that aims to maximize  $\mathbb{E}_{(X,Z) \sim (X, f(X, Y))}[T(X, Z)] - \mathbb{E}_{(X,Z) \sim (X, f(X, W))}[T(X, Z)]$ . Note that  $\|(X, f(X, Y)) - (X, f(X, W))\|_{tvd} = \max_T \{\mathbb{E}_{(X,Z) \sim (X, f(X, Y))}[T(X, Z)] - \mathbb{E}_{(X,Z) \sim (X, f(X, W))}[T(X, Z)]\}$ .

We have

$$\begin{aligned}
& \mathbb{E}_{X,Y}[T(X, f(X, Y))] - \mathbb{E}_{X,W}[T((X, f(X, W)))] \\
&= \mathbb{E}_{x \sim X} [\mathbb{E}_{y \sim Y|X=x}[T(x, f(x, y))] ] - \mathbb{E}_{x \sim X} [\mathbb{E}_{w \sim W|X=x}[T(x, f(x, w))] ] \\
&= \mathbb{E}_{x \sim X} [\mathbb{E}_{y \sim Y|X=x}[T(x, f(x, y))] ] - \mathbb{E}_{w \sim W|X=x}[T(x, f(x, w))] \\
&\leq \mathbb{E}_{x \sim X}[\delta] = \delta,
\end{aligned}$$

where the last step follows from the hypothesis that for every fixed  $x$ , we have

$$\|f(x, Y) - f(x, W)\|_{tvd} \leq \delta.$$

□

We will also need the following lemma from [KK19].

**Lemma 2.4** ([KK19, Lemma B.2]). *Let  $X^1, X^2$  be random variables taking values on finite sample space  $\Omega_1$ . Let  $Z^1, Z^2$  be random variables taking values on finite sample space  $\Omega_2$ , and suppose that  $Z^2$  is independent of  $X^1, X^2$ . Let  $f : \Omega_1 \times \Omega_2 \rightarrow \Omega_3$  be a function. Then*

$$\|(X^1, f(X^1, Z^1)) - (X^2, f(X^2, Z^2))\|_{tvd} \leq \|(X^1, f(X^1, Z^1)) - (X^1, f(X^1, Z^2))\|_{tvd} + \|X^1 - X^2\|_{tvd}.$$

## 2.2 Concentration inequality

We will use the following concentration inequality from [KK19] which is essentially an Azuma-Hoeffding style inequality for submartingales.

**Lemma 2.5** ([KK19, Lemma 2.5]). *Let  $X = \sum_{i \in [N]} X_i$  where  $X_i$  are Bernoulli random variables such that for every  $k \in [N]$ ,  $\mathbb{E}[X_k | X_1, \dots, X_{k-1}] \leq p$  for some  $p \in (0, 1)$ . Let  $\mu = Np$ . For every  $\Delta > 0$ , we have:*

$$\Pr[X \geq \mu + \Delta] \leq \exp\left(-\frac{\Delta^2}{2\mu + 2\Delta}\right).$$

## 2.3 Fourier analysis

In this paper, we will use Fourier analysis over  $\mathbb{Z}_q$  (see, for instance, [O'D14, GT19]). For a function  $f : \mathbb{Z}_q^n \rightarrow \mathbb{C}$ , its Fourier coefficients are defined by  $\widehat{f}(\mathbf{u}) = \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} f(\mathbf{a}) \cdot \overline{\omega^{\mathbf{u}^\top \mathbf{a}}}$ , where  $\mathbf{u} \in \mathbb{Z}_q^n$  and  $\omega = e^{2\pi i/q}$  is the primitive  $q$ -th root of unity. In particular, for every  $\mathbf{a}$ ,  $f(\mathbf{a}) = \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}) \cdot \omega^{\mathbf{u}^\top \mathbf{a}}$ . Later we will use the three following important tools. Note that here we define the  $p$ -norm of  $f$  as  $\|f\|_p^p = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |f(\mathbf{x})|^p$  rather than the standard definition which uses expectation. This is for future notational convenience.

**Lemma 2.6** (Parseval's identity). *For every function  $f : \mathbb{Z}_q^n \rightarrow \mathbb{C}$ ,*

$$\|f\|_2^2 = \sum_{\mathbf{a} \in \mathbb{Z}_q^n} f(\mathbf{a})^2 = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u})^2.$$

Note that for every distribution  $f$  on  $\mathbb{Z}_q^n$ ,  $\widehat{f}(0^n) = q^{-n}$ . For the uniform distribution  $U$  on  $\mathbb{Z}_q^n$ ,  $\widehat{U}(\mathbf{u}) = 0$  for every  $\mathbf{u} \neq 0^n$ . Thus, by Lemma 2.6, for any distribution  $f$  on  $\mathbb{Z}_q^n$ :

$$\|f - U\|_2^2 = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \left(\widehat{f}(\mathbf{u}) - \widehat{U}(\mathbf{u})\right)^2 = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n \setminus \{0^n\}} \widehat{f}(\mathbf{u})^2. \quad (2.7)$$

We now introduce some standard facts about how convolutions interact with the Fourier transform operation. For functions  $f, g: \mathbb{Z}_q^n \rightarrow \mathbb{C}$ , their convolution  $f \star g: \mathbb{Z}_q^n \rightarrow \mathbb{C}$  is defined as  $(f \star g)(\mathbf{a}) = \sum_{\mathbf{v} \in \mathbb{Z}_q^n} f(\mathbf{v})g(\mathbf{a} - \mathbf{v})$ . The first lemma is the so-called ‘‘convolution theorem,’’ which essentially states that, up to normalization factors, the Fourier transform of the convolution of two functions is equal to the pointwise product of the individual Fourier transforms.

**Lemma 2.8** (Convolution Theorem). *For  $f, g: \mathbb{Z}_q^n \rightarrow \mathbb{C}$ , we have*

$$\widehat{f \star g}(\mathbf{u}) = q^n \cdot \widehat{f}(\mathbf{u}) \cdot \widehat{g}(\mathbf{u}).$$

for all  $\mathbf{u} \in \mathbb{Z}_q^n$ .

*Proof.* For every  $\mathbf{u}$ ,

$$\begin{aligned} \widehat{f \star g}(\mathbf{u}) &= \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} (f \star g)(\mathbf{a}) \cdot \overline{\omega^{\mathbf{u}^\top \mathbf{a}}} \\ &= \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \left( \sum_{\mathbf{v} \in \mathbb{Z}_q^n} f(\mathbf{v})g(\mathbf{a} - \mathbf{v}) \right) \overline{\omega^{\mathbf{u}^\top \mathbf{a}}} \\ &= \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \sum_{\mathbf{v} \in \mathbb{Z}_q^n} f(\mathbf{v}) \overline{\omega^{\mathbf{u}^\top \mathbf{v}}} \cdot g(\mathbf{a} - \mathbf{v}) \overline{\omega^{\mathbf{u}^\top (\mathbf{a} - \mathbf{v})}} \\ &= \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{Z}_q^n} f(\mathbf{v}) \overline{\omega^{\mathbf{u}^\top \mathbf{v}}} \cdot \sum_{\mathbf{a} \in \mathbb{Z}_q^n} g(\mathbf{a} - \mathbf{v}) \overline{\omega^{\mathbf{u}^\top (\mathbf{a} - \mathbf{v})}} \\ &= q^n \cdot \frac{1}{q^n} \sum_{\mathbf{v} \in \mathbb{Z}_q^n} f(\mathbf{v}) \overline{\omega^{\mathbf{u}^\top \mathbf{v}}} \cdot \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} g(\mathbf{a}) \overline{\omega^{\mathbf{u}^\top \mathbf{a}}} \\ &= q^n \cdot \widehat{f}(\mathbf{u}) \cdot \widehat{g}(\mathbf{u}), \end{aligned}$$

as desired. □

We will also need the following lemma, which states that the Fourier transform of the *product* of two functions is given by the convolution of the individual Fourier transforms.

**Lemma 2.9** (Fourier transform of product of functions). *For every  $f, g: \mathbb{Z}_q^n \rightarrow \mathbb{C}$ , and  $\mathbf{u} \in \mathbb{Z}_q^n$ , we have*

$$\widehat{f \cdot g}(\mathbf{u}) = \sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}') \cdot \widehat{g}(\mathbf{u} - \mathbf{u}').$$

Furthermore, for every  $h \in [n]$ ,

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} \widehat{f \cdot g}(\mathbf{u}) = \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \widehat{f}(\mathbf{u}') \cdot \widehat{g}(\mathbf{u}).$$

*Proof.* For every  $\mathbf{u} \in \mathbb{Z}_q^n$ , we have

$$\widehat{f \cdot g}(\mathbf{u}) = \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} f(\mathbf{a}) \cdot g(\mathbf{a}) \cdot \overline{\omega^{\mathbf{u}^\top \mathbf{a}}}$$

$$\begin{aligned}
&= \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \left( \sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}') \cdot \omega^{\mathbf{u}'^\top \mathbf{a}} \right) \cdot g(\mathbf{a}) \cdot \overline{\omega^{\mathbf{u}'^\top \mathbf{a}}} \\
&= \sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}') \cdot \left( \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} g(\mathbf{a}) \cdot \overline{\omega^{(\mathbf{u}-\mathbf{u}')^\top \mathbf{a}}} \right) \\
&= \sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}') \cdot \widehat{g}(\mathbf{u} - \mathbf{u}').
\end{aligned}$$

Next, for every  $h \in [n]$ ,

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} \widehat{f \cdot g}(\mathbf{u}) = \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} \sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}') \cdot \widehat{g}(\mathbf{u} - \mathbf{u}'). \quad (2.10)$$

Letting  $\mathbf{w} = \mathbf{u} - \mathbf{u}'$  and switching the order of the summations, the right-hand side of (2.10) becomes

$$\sum_{\mathbf{u}' \in \mathbb{Z}_q^n} \sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^n \\ \|\mathbf{w} + \mathbf{u}'\|_0 = h}} \widehat{f}(\mathbf{u}') \cdot \widehat{g}(\mathbf{w}),$$

which, after renaming variables, proves the furthermore part of the lemma.  $\square$

Next we state a hypercontractivity statement from [O'D14]. Let  $(\Omega, \pi)$  be a finite probability space with  $|\Omega| \geq 2$  and assume  $\pi$  has full support. We denote by  $L^2(\Omega, \pi)$  the inner product space of square-integrable functions  $\Omega \rightarrow \mathbb{R}$  with inner product  $\langle f, g \rangle = \mathbb{E}_{x \sim \pi}[f(x)g(x)]$ .

**Lemma 2.11.** [O'D14, Chapter 10, General Hypercontractivity Theorem, page 283]

Let  $(\Omega_1, \pi_1), \dots, (\Omega_n, \pi_n)$  be finite probability spaces, in each of which every outcome has probability at least  $\lambda$ . Let  $f \in L^2(\Omega_1 \times \dots \times \Omega_n, \pi_1 \otimes \dots \otimes \pi_n)$ . Then for any  $p' > 2$ , and  $0 \leq \rho \leq \frac{1}{\sqrt{p'-1}} \lambda^{1/2-1/p'}$ ,

$$\|T_\rho f\|_2 \leq \|f\|_p,$$

where  $p$  is the Hölder's conjugate of  $p'$ , and  $T_\rho$  is the noise operator defined by

$$T_\rho f(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u}) \rho^{|\mathbf{u}|_0} \omega^{\mathbf{u}^\top \mathbf{x}}.$$

We now state the following consequence in our language:

**Lemma 2.12.** Let  $f : \mathbb{Z}_q^n \rightarrow \mathbb{R} \in L^2(\mathbb{Z}_q^n, \text{Unif}(\mathbb{Z}_q^n))$ . Then for any  $1 < p < 2$ , and  $0 \leq \rho \leq \sqrt{p-1} \cdot (1/q)^{1/p-1/2}$ ,

$$\|T_\rho f\|_2 \leq \|f\|_p.$$

*Proof.* The lemma follows from Lemma 2.11 by letting  $\Omega_i = \mathbb{Z}_q$  and  $\pi_i$  be the uniform distribution on  $\Omega_i$  yielding  $\lambda = 1/q$  and substituting  $p' = p/(p-1)$ .  $\square$

Next, we prove the following consequence of the hypercontractivity theorem.

**Lemma 2.13.** *For every  $q \in \mathbb{N}$ , there exists  $\zeta_q$  such that for every  $f : \mathbb{Z}_q^n \rightarrow [-1, 1]$  and  $B = \{\mathbf{a} \in \mathbb{Z}_q^n \mid f(\mathbf{a}) \neq 0\}$ , the following holds: If  $|B| \geq q^{n-b}$  for some  $b \in \mathbb{N}$ , then for every  $\mathbf{v} \in \mathbb{Z}_q^n$  and every  $h \in \{1, \dots, 4b\}$ , we have*

$$\frac{q^{2n}}{|B|^2} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} |\widehat{f}(\mathbf{u})|^2 \leq \left( \frac{\zeta_q \cdot b}{h} \right)^h.$$

*Proof.* We will prove the lemma for  $\zeta_q = 6q^{4/3}$ . Let  $\mathbf{v} = 0^n$  and  $f : \mathbb{Z}_q^n \rightarrow [-1, 1]$ . We choose  $p = 1 + \frac{h}{6b}$  and  $\rho = \sqrt{p-1} \cdot (1/q)^{1/p-1/2}$ . Assume  $|B| \geq q^{n-b}$ .

The choices of  $p$  and  $\rho$  satisfy the preconditions of Lemma 2.12, and so applying Lemma 2.12 we have

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} \rho^{2\|\mathbf{u}\|_0} |\widehat{f}(\mathbf{u})|^2 = \|T_\rho f\|_2^2 \leq \|f\|_p^2 = \left( \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |f(\mathbf{x})|^p \right)^{2/p} \leq \left( \frac{|B|}{q^n} \right)^{2/p},$$

where the last inequality uses the fact that  $f(x) \in [-1, 1]$  for all  $x$ .

Now, suppose  $h \in \{1, \dots, 4b\}$ . Noting that  $\rho^{2h} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} |\widehat{f}(\mathbf{u})|^2 \leq \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \rho^{2\|\mathbf{u}\|_0} |\widehat{f}(\mathbf{u})|^2$ , we have

$$\begin{aligned} \frac{q^{2n}}{|B|^2} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} |\widehat{f}(\mathbf{u})|^2 &\leq \frac{1}{\rho^{2h}} \left( \frac{q^n}{|B|} \right)^{2-2/p} \\ &\leq \frac{1}{\rho^{2h}} q^{(2-2/p)b} \\ &= \frac{q \left( -1 + \frac{2b}{h} + \frac{2}{p} - \frac{2b}{hp} \right) h}{(p-1)^h} \\ &= \left( \frac{6b}{h} \cdot q^{-1 + \frac{2b}{h} + \frac{2}{p} - \frac{2b}{hp}} \right)^h, \end{aligned} \tag{2.14}$$

where the first equality above is by our choice of  $\rho$  and the second by our choice of  $p$ .

Observe that the exponent of  $q$  in the final expression above can be bounded as follows:

$$\begin{aligned} -1 + \frac{2b}{h} + \frac{2}{p} - \frac{2b}{ph} &= -1 + \frac{2b}{h} + \frac{2(1 - \frac{b}{h})}{1 + \frac{h}{6b}} \\ &= \left( 1 + \frac{h}{6b} \right)^{-1} \left( \frac{2}{6} - \frac{h}{6b} + 1 \right) \\ &\leq 4/3. \end{aligned} \tag{2.15}$$

The expression from (2.14) can now be bounded from above by  $\left( \frac{\zeta_q b}{h} \right)^h$ , where  $\zeta_q = 6q^{4/3}$ , implying that

$$\frac{q^{2n}}{|B|^2} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} |\widehat{f}(\mathbf{u})|^2 \leq \left( \frac{\zeta_q b}{h} \right)^h.$$

In order to extend the above to sums over translational shifts, i.e.,  $\mathbf{u}$  such that  $\|\mathbf{u} + \mathbf{v}\|_0 = h$  for an arbitrary  $\mathbf{v} \in \mathbb{Z}_q^n$ , consider the function  $g(\mathbf{x}) = f(\mathbf{x}) \cdot \omega^{\mathbf{x}^\top \mathbf{v}}$ . We have for every  $\mathbf{x} \in \mathbb{Z}_q^n$ ,

$$\widehat{g}(\mathbf{u}) = q^{-n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} g(\mathbf{a}) \overline{\omega^{\mathbf{a}^\top \mathbf{u}}} = q^{-n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} f(\mathbf{a}) \overline{\omega^{\mathbf{a}^\top (\mathbf{u} - \mathbf{v})}} = \widehat{f}(\mathbf{u} - \mathbf{v}).$$

By applying the above analysis on  $g$ , we have

$$\frac{q^{2n}}{|B|^2} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} |\widehat{f}(\mathbf{u})|^2 = \frac{q^{2n}}{|B|^2} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} |\widehat{g}(\mathbf{u})|^2 \leq \left( \frac{\zeta_q b}{h} \right)^h,$$

as desired. □

### 3 Communication problems

Throughout this paper, we will be dealing with  $k$ -hypermatchings on vertices from the set  $[n]$ , i.e., a set of edges  $e_1, \dots, e_m$  where  $e_i \subseteq [n]$ ,  $|e_i| = k$  and  $e_i \cap e_j = \emptyset$  for every  $i \neq j \in [m]$ . We let  $e_i = \{(e_i)_1, \dots, (e_i)_k\}$ . The direct encoding of a matching  $M = \{e_1, \dots, e_m\}$  will be given by a *hypermatching matrix*  $A \in \{0, 1\}^{km \times n}$  where  $A_{k(i-1)+\ell, j} = 1$  if and only if  $j = (e_i)_\ell$ , for  $i \in [m], \ell \in [k]$ . (Thus,  $A$  is a matrix with row sums being 1 and column sums being at most 1. Note that  $A$  also depends on the ordering of  $e_1, e_2, \dots, e_m$  as well as the ordering of the nodes within each  $e_i$ .)

We will also find it convenient to refer to edges by their indicator vectors in  $\mathbb{Z}_q^n$ . For an edge  $e_i$ , we will use the boldface notation  $\mathbf{e}_i \in \mathbb{Z}_q^n$  to refer to this vector, i.e.,  $(\mathbf{e}_i)_j = 1$  if  $j = (e_i)_\ell$  for some  $\ell \in [k]$ , while  $(\mathbf{e}_i)_j = 0$  otherwise.

We are now ready to define the communication game, which we term the Implicit Randomized Mask Detection (IRMD) problem:

**Definition 3.1** (Implicit Randomized Mask Detection (IRMD) Problem). *Let  $q, k, n, T \in \mathbb{N}$  and  $\alpha \in (0, 1/k)$  be parameters. Let  $\mathcal{D}_Y$  and  $\mathcal{D}_N$  be distributions over  $\mathbb{Z}_q^k$ . In the  $(\mathcal{D}_Y, \mathcal{D}_N)$ -IRMD $_{\alpha, T}$  game, there are  $T$  players and a hidden  $q$ -coloring encoded by a random  $\mathbf{x}^* \in \mathbb{Z}_q^n$ . The  $t$ -th player has two inputs: (a.)  $A_t \in \{0, 1\}^{\alpha kn \times n}$ , the hypermatching matrix (see above) corresponding to a random hypermatching  $M_t$  of size  $\alpha n$  and (b.) a vector  $\mathbf{z}_t \in \mathbb{Z}_q^{\alpha kn}$  that can be generated from one of two different distributions:*

- (Yes)  $\mathbf{z}_t = A_t \mathbf{x}^* + \mathbf{b}_t$  where  $\mathbf{b}_t \in \mathbb{Z}_q^{\alpha kn}$  is of the form  $\mathbf{b}_t = (\mathbf{b}_{t,1}, \dots, \mathbf{b}_{t,\alpha n})$  and each  $\mathbf{b}_{t,i} \in \mathbb{Z}_q^k$  is sampled from  $\mathcal{D}_Y$ .
- (No)  $\mathbf{z}_t = A_t \mathbf{x}^* + \mathbf{b}_t$  where  $\mathbf{b}_t \in \mathbb{Z}_q^{\alpha kn}$  is of the form  $\mathbf{b}_t = (\mathbf{b}_{t,1}, \dots, \mathbf{b}_{t,\alpha n})$  and each  $\mathbf{b}_{t,i} \in \mathbb{Z}_q^k$  is sampled from  $\mathcal{D}_N$ .

*This is a one-way game where the  $t$ -th player broadcasts a message to all other players after receiving messages from players  $1, \dots, t-1$ . The goal is for the  $T$ -th player to be able to decide whether the  $\{\mathbf{z}_t\}$  have been chosen from the “Yes” distribution or “No” distribution. The advantage of a protocol (in which the  $T$ -th player outputs either “Yes” or “No”) is defined as  $|\Pr_{\mathcal{D}_Y}[\text{the } T\text{-th player outputs Yes}] - \Pr_{\mathcal{D}_N}[\text{the } T\text{-th player outputs Yes}]|$ .*

**Remark.** *We remark that the inputs to the  $T$  players in the IRMD problem can be viewed as a stream  $\boldsymbol{\sigma} = \boldsymbol{\sigma}^{(1)} \circ \dots \circ \boldsymbol{\sigma}^{(T)}$ , where the  $t$ -th player’s input  $(A_t, \mathbf{z}_t)$  is converted to a stream*

$\sigma^{(t)} = (\sigma^{(t)}(i) | i \in [\alpha n])$  where the elements of the stream are of the form  $\sigma^{(t)}(i) = (\mathbf{j}^{(t)}(i), \mathbf{z}^{(t)}(i))$  with  $\mathbf{j}^{(t)}(i) \in [n]^k$  is a sequence of  $k$  distinct elements of  $[n]$  and  $\mathbf{z}^{(t)}(i) \in \mathbb{Z}_q^k$ . This “streaming” representation will be used when we relate the complexity of IRMD to the approximability of various Max-CSP( $\mathcal{F}$ ) problems in [Theorem 4.3](#).

We suppress the subscripts  $\alpha$  and  $T$  when they are clear from context. Furthermore, we simply use IRMD to refer to  $(\mathcal{D}_Y, \mathcal{D}_N)$ -IRMD with  $\mathcal{D}_Y$  being the uniform distribution over  $\{0^k, 1^k, \dots, (q-1)^k\}$  and  $\mathcal{D}_N$  being the uniform distribution over  $\mathbb{Z}_q^k$ . The following theorem shows that in this special case, the IRMD problem requires linear communication. We remark that the theorem could hold for other pairs of distributions and leave the question of when such a lower bound holds as an interesting open problem.

**Theorem 3.2** (Linear lower bound for IRMD). *For every  $q, k \in \mathbb{N}$  and  $\delta \in (0, 1/2)$ , there exists  $\alpha_0 \in (0, 1/k)$  such that for every  $\alpha \in (0, \alpha_0]$  and  $T \in \mathbb{N}$ , there exists  $n_0 \in \mathbb{N}$  and  $\tau \in (0, 1)$  such that the following holds. If  $\mathcal{D}_Y$  is the uniform distribution over  $\{0^k, 1^k, \dots, (q-1)^k\}$ ,  $\mathcal{D}_N$  is the uniform distribution over  $\mathbb{Z}_q^k$ , and  $n \geq n_0$  then every protocol for  $(\mathcal{D}_Y, \mathcal{D}_N)$ -IRMD $_{\alpha, T}$  with advantage  $\delta$  requires  $\tau n$  bits of communication.*

[Theorem 3.2](#) is proved at the end of this section. Its proof uses [Theorem 3.5](#) and [Lemma 3.6](#) which we state below.

We prove the hardness of IRMD by showing the hardness of a *folded* version of IRMD defined below. In the folded version of the communication problem, we augment each hyperedge with an associated *center*  $c \in e$ . Given a  $k$ -hypermatching  $M = (e_1, \dots, e_m)$  and a sequence of centers  $\mathbf{c} = (c_1, \dots, c_m)$  with  $c_i \in e_i = \{(e_i)_1, \dots, (e_i)_k\} \subseteq [n]$ , the  $\mathbf{c}$ -centered folded encoding of  $M$  is the matrix  $A_{\mathbf{c}} \in \mathbb{Z}_q^{(k-1)m \times n}$  whose columns are indexed by the vertex set  $[n]$  and rows are indexed by pairs  $(i, \ell)$  with  $i \in [m]$  and  $\ell \in [k] \setminus \{j\}$  where  $j \in [k]$  is the index of the center, i.e.,  $(e_i)_j = c_i$  with entries of  $A_{\mathbf{c}}$  given by

$$(A_{\mathbf{c}})((i, \ell), u) = \begin{cases} 1 & \text{if } u = (e_i)_\ell \\ -1 & \text{if } u = c_i \\ 0 & \text{otherwise.} \end{cases} \quad (3.3)$$

See [Fig. 2](#) for an example. We define the folded version of the IRMD problem below (note that all the arithmetic is over  $\mathbb{Z}_q$ ):

**Definition 3.4** (Implicit Folded Randomized Mask Detection (IFRMD) Problem). *Let  $q, k, n, T \in \mathbb{N}$  and  $\alpha \in (0, 1/k)$  be parameters. In the IFRMD game, there are  $T$  players and a hidden  $q$ -coloring encoded by a random  $\mathbf{x}^* \in \mathbb{Z}_q^n$ . The  $t$ -th player has a pair of inputs  $(A_{t, \mathbf{c}_t}, \mathbf{w}_t)$  given as follows.  $A_{t, \mathbf{c}_t} \in \mathbb{Z}_q^{\alpha(k-1)n \times n}$  gives a  $\mathbf{c}_t$ -centered folded encoding of a hypermatching  $M_t$  of size  $\alpha n$  where  $M_t$  is chosen uniformly at random and  $\mathbf{c}_t$  is chosen uniformly from all possible centers for  $M_t$ . And  $\mathbf{w}_t \in \mathbb{Z}_q^{\alpha(k-1)n}$  is a vector that can be generated from two different distributions:*

- (**YES**)  $\mathbf{w}_t = A_{t, \mathbf{c}_t} \mathbf{x}^*$ .
- (**NO**)  $\mathbf{w}_t$  is uniform over  $\mathbb{Z}_q^{\alpha(k-1)n}$ .

*This is a one-way game where the  $t$ -th player broadcasts a message to all other players after receiving messages from players  $1, \dots, t-1$ . The goal is to decide (by the  $T$ -th player) whether the  $\{\mathbf{w}_t\}$  are coming from the **YES** distribution or the **NO** distribution. The advantage of a protocol is defined as*

$$\left| \Pr_{(A_{t, \mathbf{c}_t}, \mathbf{w}_t)_{t \in T} \sim \mathbf{YES}} [\text{the } T\text{-th player outputs Yes}] - \Pr_{(A_{t, \mathbf{c}_t}, \mathbf{w}_t)_{t \in T} \sim \mathbf{NO}} [\text{the } T\text{-th player outputs Yes}] \right|.$$

The main technical theorem of this paper is the following  $\Omega(n)$  communication lower bound for IFRMD.

**Theorem 3.5** (Linear lower bound for IFRMD). *For every  $q, k \in \mathbb{N}$  and  $\delta \in (0, 1/2)$ , there exists  $\alpha_0 > 0$  such that for every  $\alpha \in (0, \alpha_0]$  and  $T \in \mathbb{N}$ , there exists  $n_0 \in \mathbb{N}$  and  $\tau \in (0, 1)$  such that the following holds. When  $n \geq n_0$ , any protocol for IFRMD with advantage  $\delta$  requires  $\tau n$  bits of communication.*

An instance of the IFRMD problem can be viewed as giving  $\alpha n T$  constraints on  $n$  variables  $X_1, \dots, X_n$  where each constraint is of the form  $(c; i_1, \dots, i_{k-1}; v_1, \dots, v_{k-1})$  with  $c, i_1, \dots, i_{k-1} \in [n]$  and  $v_1, \dots, v_{k-1} \in \mathbb{Z}_q$  with the constraint requiring  $\bigwedge_{j=1}^{k-1} (X_{i_j} - X_c = v_j)$ . Thus each instance of IFRMD specifies an instance of the aforementioned Max  $k$ -LIN-mod  $q$  problem where  $\mathcal{D}_Y$  is supported on instances which are always satisfiable (by setting  $X = \mathbf{x}^*$ ). It turns out  $\mathcal{D}_N$  is supported on roughly random instances and thus it is unlikely to have a solution satisfying more than  $q^{-(k-1)}$  fraction of the constraints. (This is implicit in the proof of [Theorem 4.3](#).) The indistinguishability result in [Theorem 3.5](#) thus effectively implies a  $q^{-(k-1)} + \varepsilon$ -inapproximability for this problem. This is formally proved in [Example 4](#) in [Section 4.1](#).

The proof of [Theorem 3.5](#) is given in [Section 5.1](#). We now establish a reduction from IFRMD to IRMD that preserves the communication complexity. By this reduction, [Theorem 3.2](#) will be an immediate corollary of [Theorem 3.5](#).

**Lemma 3.6.** *Let  $n, k, \alpha$  be the parameters. Suppose there exists a protocol for IRMD using at most  $s$  bits of communication with advantage  $\delta$ , then there exists a protocol for IFRMD using at most  $s$  bits communication with advantage  $\delta$ .*

*Proof.* Suppose we have an instance of IFRMD with input  $(A_{t, \mathbf{c}_t}, \mathbf{w}_t)$  to the  $t$ -th player. We need to transform this to an input  $(\Pi_t, \mathbf{z}_t)$  to the IRMD problem (while respecting the right distributions). (Furthermore the transformation  $(A_{t, \mathbf{c}_t}, \mathbf{w}_t) \mapsto (\Pi_t, \mathbf{z}_t)$  should be locally computable by the  $t$ th player.)

Let  $m = \alpha n$ . Let  $e_1^{(t)}, e_2^{(t)}, \dots, e_m^{(t)}$  be the hyperedges corresponding to  $A_{t, \mathbf{c}_t}$ . For  $i \in [m]$  let us write  $e_i^{(t)} = \{(e_i^{(t)})_1, \dots, (e_i^{(t)})_k\} \subseteq [n]$ .<sup>4</sup> Further let  $j(i) \in [k]$  be the unique index so that  $(e_i^{(t)})_{j(i)} = c_{t, i}$ .

For each  $t$ , the  $t$ -th player performs the following computations on his/her input:

1. We index the columns of  $\Pi_t$  by the vertex set  $[n]$  and the rows by  $[m] \times [k]$ . We set  $\Pi_t((i, \ell), u) = 1$  if  $(e_i^{(t)})_\ell = u$  and 0 otherwise.
2. For each  $i \in [m]$ , sample  $a_{t, i} \in \mathbb{Z}_q$  uniformly at random. Again we assume the coordinates of  $\mathbf{z}_t \in \mathbb{Z}_q^{km}$  are indexed by pairs  $(i, \ell) \in [m] \times [k]$ . We set  $(\mathbf{z}_t)(i, \ell) = a_{t, i}$  if  $\ell = j(i)$  and  $(\mathbf{z}_t)(i, \ell) = (\mathbf{w}_t)(i, \ell) + a_{t, i}$  otherwise.

We claim that the inputs  $(A_t, \mathbf{z}_t)$  correspond to an instance of IRMD. It suffices to show that if  $(\{(A_{t, \mathbf{c}_t}, \mathbf{w}_t)\}_{t \in [T]}, \mathbf{x}^*)$  follows the **YES** (resp. **NO**) distribution of IFRMD, then  $(\{(A_t, \mathbf{z}_t)\}_{t \in [T]}, \mathbf{x}^*)$  follows the **YES** (resp. **NO**) distribution of IRMD. The **NO** case is easy to see:  $\Pi_t$  encodes a random  $k$ -hypermatching of size  $m$  and  $\mathbf{z}_t$  is uniform over  $\mathbb{Z}_q^{km}$  since  $\mathbf{w}_t \in \mathbb{Z}_q^{(k-1)m}$  and  $a_{i, t} \in \mathbb{Z}_q$  are uniform and independent of each other and of  $A_{t, \mathbf{c}_t}$ .

<sup>4</sup>Note that the choice of ordering of vertices within an edge is arbitrary. Altering this will only (simultaneously) permute the rows of  $\Pi_t$  and  $\mathbf{z}_t$ .

We now turn to the **YES** case. Fix  $i \in [m]$ . For  $\ell = j(i)$ , we have

$$(\mathbf{z}_t)(i, \ell) = a_{t,i} = \mathbf{x}_{(\mathbf{c}_t)_i}^* + (-\mathbf{x}_{(\mathbf{c}_t)_i}^* + a_{t,i}) = \mathbf{x}_{(e_i^{(t)})_\ell}^* + (-\mathbf{x}_{(\mathbf{c}_t)_i}^* + a_{t,i}).$$

For  $\ell \in [k] \setminus \{j(i)\}$ , we have

$$(\mathbf{z}_t)(i, \ell) = (\mathbf{w}_t)(i, \ell) + a_{t,i} = \mathbf{x}_{(e_i^{(t)})_\ell}^* - \mathbf{x}_{(\mathbf{c}_t)_i}^* + a_{t,i} = \mathbf{x}_{(e_i^{(t)})_\ell}^* + (-\mathbf{x}_{(\mathbf{c}_t)_i}^* + a_{t,i}),$$

where the second equality uses  $\mathbf{w} = A_{t, \mathbf{c}_t} \cdot \mathbf{x}^*$  in the **YES** case.

Thus, it follows that  $\mathbf{z}_t = \Pi_t \mathbf{x}^* + \mathbf{b}_t$ , where  $\mathbf{b}_t = (\mathbf{b}_{t,1}, \dots, \mathbf{b}_{t,m})$  is given by  $\mathbf{b}_{t,i} = (-\mathbf{x}_{\mathbf{c}_t,i}^* + a_{t,i}) \cdot \mathbf{1}_k$  where  $\mathbf{1}_k$  is the all 1 vector of length  $k$ . Thus for every  $t, i$ ,  $\mathbf{b}_{t,i} \in \mathbb{Z}_q^k$  is a uniformly chosen constant vector independent of  $\mathbf{x}^*$  (and of other  $\mathbf{b}_{t,i'}$  for  $i' \neq i$ ) as required in the **YES** case and thus showing that  $(\Pi_t, \mathbf{z}_t)$  are distributed according to  $\mathcal{D}_Y$ .  $\square$

*Proof of Theorem 3.2 (assuming Theorem 3.5).* For the sake of contradiction, suppose there exists a protocol for IRMD with advantage  $\delta$  using fewer than  $\tau n$  bits of communication. Then by Lemma 3.6 there exists a protocol for IFRMD with advantage  $\delta$  using fewer than  $\tau n$  bits of communication, which contradicts Theorem 3.5. This completes the proof of Theorem 3.2.  $\square$

In the following section we show how Theorem 3.2 yields the claimed hardness of streaming problems. In the rest of this paper, we focus on the proof of Theorem 3.5, i.e., the linear communication lower bound for IFRMD.

## 4 Streaming problems and hardness

In this section we state our main technical theorem establishing linear space lower bounds for the approximability of many CSPs. We also prove these lower bounds assuming Theorem 3.5 and in particular its corollary Theorem 3.2.

Below we define the two crucial constants associated with a family  $\mathcal{F}$  which lay out the “trivial” approximability, and the inapproximability that we prove. In particular we define the notion of a width  $\omega(\mathcal{F}) \in [1/q, 1]$  for every family  $\mathcal{F}$ . The notion of a wide family from Theorem 1.1 corresponds to a family with maximum width, i.e.,  $\omega(\mathcal{F}) = 1$ .

**Definition 4.1** (Minimum value, Width of  $\mathcal{F}$ ). *For a family  $\mathcal{F}$ , we define its minimum value  $\rho_{\min}(\mathcal{F})$  to be the infimum over all instances  $\Psi$  of Max-CSP( $\mathcal{F}$ ) of  $\text{val}_\Psi$ . For  $\mathbf{b} \in \mathbb{Z}_q^k$  and  $f : \mathbb{Z}_q^k \rightarrow \{0, 1\}$  we define  $\mathbf{b}$ -width of  $f$ , denoted  $\omega_{\mathbf{b}}(f)$  to be the quantity  $\frac{|\{a \in \mathbb{Z}_q \mid f(\mathbf{b} + a^k) = 1\}|}{q}$ . The width of  $f$ , denoted  $\omega(f)$ , is given by  $\omega(f) = \max_{\mathbf{b} \in \mathbb{Z}_q^k} \{\omega_{\mathbf{b}}(f)\}$ . Finally for a family  $\mathcal{F}$ , we define its width to be  $\omega(\mathcal{F}) = \min_{f \in \mathcal{F}} \{\omega(f)\}$ . We say that a family  $\mathcal{F}$  is wide if  $\omega(\mathcal{F}) = 1$ .*

As described above  $\rho_{\min}(\mathcal{F})$  may not even be computable given  $\mathcal{F}$ , but as pointed out in [CGSV21a] it is a computable function. Key to this assertion is the following equivalent definition of  $\rho_{\min}(\mathcal{F})$  which follows from Definition 2.4 and Proposition 2.5 of [CGSV21a].

**Proposition 4.2** ([CGSV21a, Proposition 2.5]). *For every  $k, q, \mathcal{F} \subseteq \{f : \mathbb{Z}_q^k \rightarrow \{0, 1\}\}$  we have*

$$\rho_{\min}(\mathcal{F}) = \rho(\mathcal{F}) := \min_{\mathcal{D}_{\mathcal{F}} \in \Delta(\mathcal{F})} \left\{ \max_{\mathcal{D} \in \Delta([q])} \left\{ \mathbb{E}_{f \sim \mathcal{D}_{\mathcal{F}}, \mathbf{a} \sim \mathcal{D}^k} [f(\mathbf{a})] \right\} \right\}.$$

We are now ready to prove the main theorem of the paper on the approximability of CSPs by applying Theorem 3.2.

**Theorem 4.3** (Linear Space Inapproximability of CSPs). *For every  $k, q, \mathcal{F} \subseteq \{f : \mathbb{Z}_q^k \rightarrow \{0, 1\}\}$  and every  $\varepsilon > 0$  we have the following: Every randomized single-pass streaming  $(1 + \varepsilon) \cdot \frac{\rho(\mathcal{F})}{\omega(\mathcal{F})}$ -approximation algorithm for  $\text{Max-CSP}(\mathcal{F})$  requires  $\Omega(n)$  space.*

*Proof.* We assume  $0 < \varepsilon \leq 1/10$ , since the theorem only gets weaker for larger  $\varepsilon$ . Given  $k, q, \mathcal{F}$  we let  $\alpha = \min\{\alpha_0, \varepsilon/(100k^2q)\}$  where  $\alpha_0$  is the constant from [Theorem 3.2](#) with  $\delta = 1/6$ . We now set  $T$  to be some large enough constant that only depends on  $q, k, \mathcal{F}, \varepsilon, \alpha$  (but not  $n$ ).

Let **ALG** be a space  $s$  algorithm distinguishing instances from the set  $\{\Psi \mid \text{val}_\Psi \geq (1 - \varepsilon/3)\omega(\mathcal{F})\}$  from instances from the set  $\{\Psi \mid \text{val}_\Psi \leq (1 + \varepsilon/3)\rho(\mathcal{F})\}$  with success probability at least  $2/3$ . We show how to use **ALG** to devise an  $s$ -bit communication protocol for  $\text{IRMD} = \text{IRMD}_{\alpha, T}$  with advantage at least  $1/6$ .

For  $f \in \mathcal{F}$ , let  $\mathbf{b}_f \in \mathbb{Z}_q^k$  be a sequence maximizing  $\omega_{\mathbf{b}_f}(f)$  and let  $S_f = \{\mathbf{b}_f + a^k \mid a \in \mathbb{Z}_q\}$ . Further let  $\mathcal{D}_{\mathcal{F}} \in \Delta(\mathcal{F})$  be a distribution achieving the minimum in the equivalent definition of  $\rho(\mathcal{F})$  from [Proposition 4.2](#). Let  $\sigma = (\sigma_1, \dots, \sigma_m)$  be an instance of  $\text{IRMD}$  with  $T$  players, so that  $m = T\alpha n$  and  $\sigma_i = (\mathbf{j}(i), \mathbf{z}(i))$  where  $\mathbf{j}(i) \in [n]^k$  is a sequence of  $k$  distinct elements of  $[n]$  and  $\mathbf{z}(i) \in \mathbb{Z}_q^k$ . For each  $\sigma_i$  we either generate 0 or 1 constraint of  $\text{Max-CSP}(\mathcal{F})$  as follows: We sample  $f(i) \sim \mathcal{D}_{\mathcal{F}}$  and output the constraint  $(f(i), \mathbf{j}(i))$  if  $\mathbf{z}(i) \in S_{f(i)}$  and output no constraint otherwise. Applying this step independently to each  $\sigma_i$  generates an instance  $\Psi$  of  $\text{Max-CSP}(\mathcal{F})$  with  $\tilde{m} \leq m$  constraints on  $n$  variables. We make the following claims about  $\Psi$ .

- (1)  $\Pr_{\mathbf{YES}}[\tilde{m} > (1 + \varepsilon/10) \cdot q^{-(k-1)} \cdot m] = o(1)$  and  $\Pr_{\mathbf{NO}}[\tilde{m} < (1 - \varepsilon/10) \cdot q^{-(k-1)} \cdot m] = o(1)$ , i.e., the number of constraints  $\tilde{m}$  does not deviate (in the wrong direction) from its expectation  $q^{-(k-1)} \cdot m$  with too high a probability.<sup>5</sup>
- (2) If  $\sigma$  is generated from the **YES** distribution with hidden vector  $\mathbf{x}^*$  then with high probability the number of constraints of  $\Psi$  satisfied by  $\mathbf{x}^*$  is at least  $\omega(\mathcal{F})(1 - \varepsilon/10) \cdot q^{-(k-1)} \cdot m$ . In particular,
 
$$\Pr_{\mathbf{YES}}[\text{val}_\Psi \leq (1 - \varepsilon/3) \cdot \omega(\mathcal{F})] = o(1).$$
- (3) If  $\sigma$  is generated from the **NO** distribution with hidden vector  $\mathbf{x}^*$  then with high probability for every  $\nu$  the number of constraints of  $\Psi$  satisfied by  $\nu$  is at most  $\rho(\mathcal{F})(1 + \varepsilon/10) \cdot q^{-(k-1)} \cdot m$ . In particular,  $\Pr_{\mathbf{NO}}[\text{val}_\Psi \geq (1 + \varepsilon/3) \cdot \rho(\mathcal{F})] = o(1)$ .

With the above claims in hand, it is straightforward to convert **ALG** into an  $O(s)$ -bit communication protocol for  $\text{IRMD}$  with advantage at least  $1/6$  — the  $t$ -th player gets the state of **ALG** after processing constraints corresponding to the first  $t - 1$  blocks from the  $(t - 1)$ -th player; generates the constraints corresponding to the  $t$ -th block of the stream  $\sigma$ , and simulates **ALG** on this part of the stream corresponding to  $\Psi$ , and passes the resulting state on to the  $(t + 1)$ -th player. The  $T$ -th player outputs 1 if **ALG** outputs 1 and 0 otherwise. It is straightforward to see that if **ALG** is correct on every input with probability  $2/3$  and Claims (1)-(3) above hold, then the resulting communication protocol achieves advantage at least  $1/3 - o(1) \geq 1/6$  on  $\text{IRMD}$ . Finally, we invoke [Theorem 3.2](#) and conclude that  $s = \Omega(n)$ .

We thus turn to proving claims (1)-(3). Given  $\sigma_1, \dots, \sigma_m$  and  $\nu \in \mathbb{Z}_q^n$ , we create a collection of related variables as follows: For  $i \in [m]$ , let  $V_i = 1$  if  $\sigma_i$  results in a constraint and 0 otherwise. Further, let  $Y_i(\nu) = 1$  if  $V_i = 1$  and the resulting constraint is satisfied by the assignment  $\nu$ . (Note all these are random variables depending on  $\sigma$ ). Below, we bound the expectations of the sums of

<sup>5</sup>In these claims the  $o(1)$  term goes to zero as  $n \rightarrow \infty$ . In fact, the proof will show that these terms go to zero exponentially fast in  $n$  but we won't need this additional fact.

these random variables in the **YES** and **NO** cases, and also argue that these variables are close to their expectations (or at least give bounds on deviating from the expectation in one direction). This will suffice to prove claims (1)-(3) and thus the theorem.

**Proof of Claim (1).** We start with  $\tilde{m} = \sum_{i=1}^m V_i$  in the **NO** case: In this case  $\mathbb{E}[V_i] = |S_f|/q^k = q^{-(k-1)}$  (note that  $|S_f| = q$  for every  $f$ ). Furthermore the  $V_i$ 's are independent since  $\mathbf{z}(i)$ 's are uniform and independent of each other. Thus  $\tilde{m}$  is sharply concentrated around  $q^{-(k-1)} \cdot m$  and we get that  $\Pr_{\mathbf{NO}}[\tilde{m} \notin (1 \pm \varepsilon/10) \cdot q^{-(k-1)} \cdot m] = o(1)$ .

Turning to the **YES** case, since  $\mathbf{z}(i)$ 's are no longer independent, the  $V_i$ 's are correlated. To enable the analysis, we define a vector  $\mathbf{x}^*$  to be  $\gamma$ -good for  $\gamma > 0$  if for every  $\tau \in \mathbb{Z}_q$  we have  $\Pr_{i \in [n]}[\mathbf{x}_i^* = \tau] \in (1 \pm \gamma)(1/q)$ . Note that for every constant  $\gamma > 0$ , the probability that  $\mathbf{x}^*$  is not  $\gamma$ -good is  $o(1)$ . Fix  $\mathbf{x}^*$  that is  $\gamma$ -good. We claim that in this case,  $\mathbb{E}[V_i | V_{1:i-1}] \leq q^{-(k-1)} \cdot (1 + \gamma + \alpha k q)^k$ . To see this note that the effect of conditioning on  $V_{1:i-1}$  only affects  $V_i$  due to the fact that now  $\mathbf{j}(i)$  is chosen from a smaller set of variables and not all of  $[n]$ . Let  $t \in [T]$  denote the block containing  $i$  (i.e.,  $i \in ((t-1)\alpha n, t\alpha n]$ ). Let  $S$  denote the set of variables that do not participate in the edges  $\mathbf{j}((t-1)\alpha n + 1), \dots, \mathbf{j}(i-1)$ . Note  $|S| \geq (1 - k\alpha)n$  and so for every  $\tau \in \mathbb{Z}_q$  we have  $\Pr_{\ell \in S}[\mathbf{x}_\ell^* = \tau] \leq (1 + \gamma + \alpha k q)/q$ . We conclude that the probability  $\Pr[\mathbf{x}^*|_{\mathbf{j}(i)} \in S_f | V_{1:i-1}] \leq |S_f| \cdot ((1 + \gamma + \alpha k q)/q)^k = q^{-(k-1)} \cdot (1 + \gamma + \alpha k q)^k$ . Setting  $\gamma = \varepsilon/(100k)$  and using  $\alpha \leq \varepsilon/(100k^2 q)$ , we conclude  $\mathbb{E}[V_i | V_{1:i-1}] \leq q^{-(k-1)} \cdot (1 + \varepsilon/(50k))^k \leq q^{-(k-1)} \cdot (1 + \varepsilon/20)$  (where we use  $\varepsilon \leq 1/10$  to get  $(1 + \varepsilon/(50k))^k (1 + \varepsilon/20)$ ). Applying Lemma 2.5 we conclude that here again we get that  $\Pr_{\mathbf{YES}}[\tilde{m} = \sum_i V_i > (1 + \varepsilon/10)q^{-(k-1)}m] = o(1)$ . (Note that the  $o(1)$  term goes to zero exponentially fast with  $m$ .)

**Proof of Claim (2).** Now we analyze the number of satisfiable constraints of the resulting instance  $\Psi$  in the **YES** case, where we argue that  $\mathbf{x}^*$  satisfies a large fraction of constraints with high probability. Again with probability  $1 - o(1)$  we have that  $\mathbf{x}^*$  is  $\gamma$ -good. Now an argument similar to the one in the analysis of  $X$  in the **YES** case shows that for every  $\mathbf{b} \in \mathbb{Z}_q^k$ ,  $\Pr[\mathbf{x}^*|_{\mathbf{j}(i)} = \mathbf{b} | Y_{1:i-1}] \geq (1 - \varepsilon/50) \cdot q^{-k}$ . Fix  $f(i)$  and let  $W = S_{f(i)} \cap f(i)^{-1}(1)$ . Note by definition of  $\omega(\mathcal{F})$  that  $|W| \geq \omega(\mathcal{F}) \cdot q$ . The event that the  $i$ -th constraint is satisfied by  $\mathbf{x}^*$  is equivalent to the event that  $\mathbf{x}_{\mathbf{j}(i)}^* \in T$  and the probability of this event, conditioned on  $Y_{1:i-1}$  is at least  $|W| \cdot (1 - \varepsilon/50) \cdot q^{-k} \geq (1 - \varepsilon/50) \cdot \omega(\mathcal{F}) \cdot q^{-(k-1)}$ . Using Lemma 2.5 we conclude again that  $\Pr[Y(\mathbf{x}^*) = \sum_{i=1}^m Y_i(\mathbf{x}^*) \leq (1 - \varepsilon/10) \cdot \omega(\mathcal{F}) \cdot q^{-(k-1)} \cdot m] = o(1)$ . Combining this with the lower bound on  $\tilde{m}$  from Claim (1) we conclude that  $\Pr[\text{val}_\Psi \leq (1 - \varepsilon/3) \cdot \omega(\mathcal{F})] = o(1)$ .

**Proof of Claim (3).** Finally we analyze the number of satisfiable constraints in the **NO** case. Fix  $\nu \in \mathbb{Z}_q^k$  and let  $\mathcal{D} \in \Delta(\mathbb{Z}_q)$  be the distribution obtained by sampling a uniformly random  $\ell \in [n]$  and outputting  $\nu_\ell$ . By Proposition 4.2 we have that  $\mathbb{E}_{f \sim \mathcal{D}_\mathcal{F}, \mathbf{b} \sim \mathcal{D}^k}[f(\mathbf{b})] \leq \rho(\mathcal{F})$ . We use this to prove that for every  $i \in [m]$ ,  $\mathbb{E}[Y_i(\nu) | Y_{1:i-1}(\nu)] \leq (1 + \varepsilon/50) \cdot \rho(\mathcal{F}) \cdot q^{-(k-1)}$ .

First, as in the proof for Claim (2) we have that the total variation distance between  $\mathbf{b} \sim \mathcal{D}^k$  and  $\{\nu_{\mathbf{j}(i)} | Y_{1:i-1}(\nu)\}$  is at most  $k^2\alpha$ . (In particular, this is upper bounded by the probability that  $k$  uniformly and independently chosen elements of  $[n]$  either collide or fall in a set of size at most  $k(\alpha n - 1)$ .) We conclude that the probability that the  $i$ -th ‘‘potential constraint’’ (given by  $(f(i), \mathbf{j}(i))$ ) is satisfied is at most  $\rho(\mathcal{F}) + k^2\alpha$ . Next, note that the event  $X_i = 1$  (i.e., the  $i$ -th constraint is chosen in  $\Psi$ ) is independent of  $Y_i(\nu)$  since in the **NO** case  $\mathbf{z}(i) \in \mathbb{Z}_q^k$  is uniform and independent of all other random variables. We conclude that  $\mathbb{E}[Y_i(\nu) | Y_{1:i-1}(\nu)] \leq (1 + \varepsilon/50) \cdot \rho(\mathcal{F}) \cdot q^{-(k-1)}$ . Finally, we apply Lemma 2.5 again to conclude that  $\Pr[Y(\nu) = \sum_{i=1}^m Y_i(\nu) > (1 + \varepsilon/10) \cdot \rho(\mathcal{F}) \cdot q^{-(k-1)} \cdot m] \leq c^{-m}$

where  $c > 1$  depends on  $q, k, \mathcal{F}, \alpha, \varepsilon$  but not on  $T$  or  $n$ . Thus by setting  $T$  large enough, we can bound  $c^{-m} \leq q^{-2n}$ . This allows us to use the union bound to conclude that the probability that there exists  $\nu \in \mathbb{Z}_q^n$  such that  $Y(\nu) > (1 + \varepsilon/10) \cdot \rho(\mathcal{F}) \cdot q^{-(k-1)} \cdot m$  is at most  $q^{-n} = o(1)$ . Combining with the lower bound on  $\tilde{m}$  from Claim (1) we get that with probability  $1 - o(1)$  we have  $\text{val}_\Psi \leq (1 + \varepsilon/3) \cdot \rho(\mathcal{F})$  in this case.

This concludes the proofs of the claims and thus the proof of [Theorem 4.3](#). □

[Theorems 1.1](#) and [1.2](#) follow immediately from [Theorem 4.3](#) as we show below.

*Proof of [Theorem 1.1](#).* The theorem follows from the fact that for a wide family  $\omega(\mathcal{F}) = 1$  and in this case [Theorem 4.3](#) asserts that a  $\rho(\mathcal{F}) + \varepsilon$  approximation requires linear space. □

*Proof of [Theorem 1.2](#).* The theorem follows from the fact that for every non-zero function  $f$  we have  $\omega(f) \geq 1/q$  and so for every family  $\mathcal{F}$  also we have  $\omega(\mathcal{F}) \geq 1/q$ . Thus [Theorem 4.3](#) asserts that a  $\rho(\mathcal{F}) \cdot q + \varepsilon$  approximation requires linear space, where  $\rho(\mathcal{F})$  approximation is trivial. □

## 4.1 Some examples

We now give some examples illustrating the power of [Theorem 4.3](#). Our first example is the familiar  $q$ -coloring problem.

### Example 1 (Max- $q$ Col).

Let  $k = 2$  and  $q \geq 2$ . Let  $\mathcal{F} = \{f : \mathbb{Z}_q^2 \rightarrow \{0, 1\}\}$  where  $f(u, v) = 1$  if and only if  $u \neq v$ . The “Max  $q$ -Coloring” problem is defined to be  $\text{Max-}q\text{Col} = \text{Max-CSP}(\mathcal{F})$ . It is easy to verify  $\rho(\mathcal{F}) = 1 - 1/q$  and  $\omega(\mathcal{F}) = 1$ . We thus conclude by [Theorem 1.1](#) that  $\text{Max-}q\text{Col}$  is approximation resistant.

Next we turn to the Unique Games Problem.

### Example 2 (Max- $q$ UG).

Let  $k = 2$  and  $q \geq 2$ . Let  $\mathcal{F} = \{f : \mathbb{Z}_q^2 \rightarrow \{0, 1\} \mid f^{-1}(1) \text{ is a bijection}^a\}$ . The “ $q$ -ary Unique Games” problem is defined to be  $\text{Max-}q\text{UG} = \text{Max-CSP}(\mathcal{F})$ . We show below that  $\rho(\mathcal{F}) = 1/q$ . We also show that there exists  $\mathcal{F}' \subseteq \mathcal{F}$  such that  $\rho(\mathcal{F}') = 1/q$  and  $\omega(\mathcal{F}') = 1$ . Applying [Theorem 1.1](#) to  $\mathcal{F}'$  we get that  $1/q + \varepsilon$  approximating  $\text{Max-CSP}(\mathcal{F}')$  requires linear space and the same holds for  $\text{Max-}q\text{UG} = \text{Max-CSP}(\mathcal{F})$  by monotonicity.

We define the family  $\mathcal{F}'$  to be  $\mathcal{F}' = \{f_a \mid a \in \mathbb{Z}_q\}$  where  $f_a(u, v) = 1$  if and only if  $u = v + a$ . Let  $\mathcal{D} = \text{Unif}(\mathbb{Z}_q)$ . For every  $f \in \mathcal{F}$  we have that  $\mathbb{E}_{(u,v) \sim \mathcal{D}^2}[f(u, v)] = 1/q$ . So for every  $\mathcal{D}_{\mathcal{F}} \in \Delta(\mathcal{F})$  we have  $\mathbb{E}_{f \sim \mathcal{D}_{\mathcal{F}}} \mathbb{E}_{(u,v) \sim \mathcal{D}^2}[f(u, v)] = 1/q$ . This proves  $\rho(\mathcal{F}), \rho(\mathcal{F}') \geq 1/q$ . To get the upper bound we let  $\mathcal{D}_{\mathcal{F}}$  be uniform over  $\mathcal{F}'$ . For every  $(u, v) \in \mathbb{Z}_q^2$  we have  $\mathbb{E}_{f \sim \mathcal{D}_{\mathcal{F}}}[f(u, v)] = 1/q$  and so for every distribution  $\mathcal{D} \in \Delta(\mathbb{Z}_q^k)$  (which is more than we need) we have  $\mathbb{E}_{f \sim \mathcal{D}_{\mathcal{F}}} \mathbb{E}_{(u,v) \sim \mathcal{D}}[f(u, v)] \leq 1/q$ . This proves  $\rho(\mathcal{F}'), \rho(\mathcal{F}) = 1/q$  (since  $\mathcal{D}_{\mathcal{F}}$  is supported on  $\mathcal{F}'$ ).

Now turning to  $\omega(\mathcal{F}')$ , note that for every  $f_a \in \mathcal{F}'$  we have  $\{(b + a, b) \mid b \in \mathbb{Z}_q\} \subseteq f_a^{-1}(1)$ . Thus  $\omega(f_a) \geq \omega_{(a,0)}(f_a) = 1$ . It follows that  $\omega(\mathcal{F}') = 1$ .

<sup>a</sup>We consider a set  $S \subseteq \mathbb{Z}_q^2$  to be a bijection if for every  $a \in \mathbb{Z}_q$ , there exists a unique  $a' \in \mathbb{Z}_q$  such that  $(a, a') \in S$  and there exists a unique  $a'' \in \mathbb{Z}_q$  such that  $(a'', a) \in S$ .

Our third example talks about constraints that are simple equalities.

**Example 3 (Max- $k$ -All-Equal $_q$ ).**

For  $k \geq 2$  and prime  $q$ , we define Max- $k$ -All-Equal $_q$  to be the Max-CSP( $\mathcal{F}$ ) for  $\mathcal{F} = \{f_{\text{All-EQ}}\}$  where  $f_{\text{All-EQ}}(x_1, \dots, x_k) = 1$  if and only if  $x_1 = \dots = x_k$ . It is easy to verify that for every  $k, r, q$ ,  $\rho(\mathcal{F}) \geq q^{-1}$  (In particular  $\mathcal{D}_{\mathcal{F}}$  is trivial since  $|\mathcal{F}| = 1$ .) Since every  $\mathbf{b} \in F_q^k$  has width 1 it follows that  $\omega(\mathcal{F}) = 1$  and so Max-CSP( $\mathcal{F}$ ) can not be approximated to within  $\frac{1}{q}(1 + \varepsilon)$ -factor in  $o(n)$  space (and is thus approximation resistant).

Our next example generalizes the above to all linear systems.

**Example 4 (Max-Lin $_{k,r,q}$ ).**

For  $k \geq 2$  and prime  $q$  and  $0 \leq r < k$ , we define Max-Lin $_{k,r,q} = \text{Max-CSP}(\mathcal{F})$  for  $\mathcal{F} = \mathcal{F}_{k,r,q} = \{f_{A,\mathbf{b}} : \mathbb{Z}_q^k \rightarrow \{0, 1\} \mid A \in \mathbb{Z}_q^{r \times k}, \mathbf{b} \in \mathbb{Z}_q^k\}$  where  $f_{A,\mathbf{b}}(x) = 1$  if and only if  $Ax = \mathbf{b}$ . (Thus constraints are systems of satisfiable linear equations with solutions of dimension at least  $k - r$ .) Note that the Max  $k$ -LIN-mod  $q$  problem mentioned in the abstract and Section 1.4 is the special case where  $r = k - 1$ . We show below that Max-Lin $_{k,r,q} = \text{Max-CSP}(\mathcal{F})$  is approximation-resistant for every  $1 \leq r \leq k - 1$ . Let  $\mathcal{F}'_{k,r,q} = \{f_{r,k}\}$  where  $f_{r,k}(x_1, \dots, x_k) = 1$  if and only if  $x_1 = \dots = x_{r+1}$ . It is easy to see that  $q^{-r} \leq \rho(\mathcal{F}) \leq \rho(\mathcal{F}') = q^{-r}$ . Furthermore  $\omega(\mathcal{F}') = 1$  (as argued in Example 3). Thus, applying Theorem 1.1 to  $\mathcal{F}'$  we get that Max-CSP( $\mathcal{F}'$ ) is approximation-resistant. The same holds for Max-Lin $_{k,r,q} = \text{Max-CSP}(\mathcal{F})$  by monotonicity.<sup>a</sup>

<sup>a</sup>We believe this system is not approximation resistant for  $r = k$ . This is proved for  $q = 2$  in [CGSV21b, Lemma 2.14]. The case of general  $q$  may not have been explicitly resolved in previous work.

Finally we mention one more problem. This problem arises in the work of Singer, Sudan and Velusamy [SSV21] who use it to show the approximation resistance of the “maximum acyclic subgraph” problem to  $o(\sqrt{n})$  space algorithms. We suspect the improved space lower bound should improve their work to rule out  $o(n)$  space algorithms.

**Example 5 (Max-Less-Than $_q$ ).**

For  $k = 2$  and  $q \geq 2$  we define  $\mathcal{F} = \{<_q\}$  where  $<_q : \mathbb{Z}_q^2 \rightarrow \{0, 1\}$  is given by  $<_q(u, v) = 1$  if and only if  $u < v$ . It is possible to show  $\rho(\mathcal{F}) = \frac{1}{2}(1 - 1/q)$ . Also  $\omega_{(0,1)}(<_q) = 1 - 1/q$  and this can be used to show that  $\omega(\mathcal{F}) = 1 - 1/q$ . By Theorem 4.3 it follows that  $1/2 + \varepsilon$ -approximating Max-CSP( $\mathcal{F}$ ) requires linear space.

## 5 Lower bound on the communication complexity

In this section we prove a linear lower bound on the communication complexity of IFRMD (Theorem 3.5). Our proof is via a hybrid argument which starts with all players receiving inputs from

the **NO** distribution, and switching the players' input distributions one at a time, starting with Player 1, to the **YES** distribution. We state a key “hybrid lemma” (Lemma 5.1) which asserts that any one step of switching does not alter the distribution of the message output by the switched player.

To state our lemma we recall some notations and set up a few new ones. Let  $\alpha, n, k, q, T, m = \alpha n \in \mathbb{N}$  denote the usual parameters of IFRMD. Recall that the player  $t$  gets as input a matrix  $A_{t, \mathbf{c}_t} \in \mathbb{Z}_q^{(k-1)m \times n}$  corresponding to a  $k$ -uniform hypermatching  $M_t$  consisting of  $m$  hyperedges folded over the center vector  $\mathbf{c}_t$  and a vector  $\mathbf{w}_t \in \mathbb{Z}_q^{(k-1)m}$ . For notational convenience, we will separate the input  $A_{t, \mathbf{c}_t}$  into a matrix  $A_t \in \mathbb{Z}_q^{(k-1)m \times n}$  and the center  $\mathbf{c}_t$ . The message  $S_t$  sent by the  $t$ -th player is a function of  $A_{1:t}, \mathbf{c}_{1:t}, \mathbf{w}_t$  and  $S_{1:t-1}$ .<sup>6</sup> Next, note that by Yao's principle [Yao77], we may assume that the messages sent by the players in IFRMD are all deterministic. Namely, a protocol for IFRMD can be specified by deterministic message functions  $r_1, r_2, \dots, r_T$  so that  $S_t = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}, \mathbf{w}_t)$  denotes the message sent by the  $t$ -th player. The communication complexity of a protocol is defined as the largest output length of  $r_t$ . When  $(A_{1:T}, \mathbf{c}_{1:T}, \mathbf{w}_{1:T})$  is drawn from the **YES** distribution (resp. the **NO** distribution), we denote by  $S_{1:T}^Y$  (resp.  $S_{1:T}^N$ ) the resulting messages. Without loss of generality  $S_T$  is just a bit “Yes/No” indicating the output of the protocol. Thus, to prove Theorem 3.5 we need to show that  $S_T^Y$  and  $S_T^N$  are close in total variation distance. For the induction we prove the much stronger statement that  $(A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^Y)$  and  $(A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^N)$  are close in total variation distance, i.e.,

$$\|(A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^Y) - (A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^N)\|_{tvd} \leq \delta.$$

The following lemma provides the key step in this analysis. Roughly it says that if the first  $t-1$  players' inputs are according to the **YES** distribution then the  $t$ -th player's output on the **YES** input is typically distributed very similarly to the output on the **NO** distribution (even conditioned on all previously announced hypermatchings, centers and messages). Formally, the lemma identifies a sequence of events  $\mathcal{E}_1 \supset \mathcal{E}_2 \supset \dots \supset \mathcal{E}_T$  such that (i)  $\mathcal{E}_t$  enforces a “typicality” restriction on the messages and inputs that the  $t$ -th player receives and (ii) if the messages and input received by the  $t$ -th player are typical then the player cannot distinguish whether its input is sampled from the **YES** distribution or the **NO** distribution (assuming all previous players' inputs were from the **YES** distribution).

**The Probability Space:** In what follows in the rest of this section (and indeed in the rest of this paper), the underlying probability space will be that of describing all the inputs in the communication problem. Specifically, we let  $\Omega = \Omega_{k,q,\alpha,n,T}$  be the distribution over tuples  $(\mathbf{x}^*, A_{1:T}, \mathbf{c}_{1:T}, \mathbf{w}_{1:T})$  where  $\mathbf{x}^* \sim \text{Unif}(\mathbb{Z}_q^n)$ ,  $A_t \in \{0, 1\}^{\alpha k n \times n}$  is the incidence matrix of a uniform random  $k$ -hypermatching on  $[n]$  with  $\alpha n$  edges,  $\mathbf{c}_t \in [n]^{\alpha n}$  is a uniform choice of centers consistent with  $A_t$ , and  $\mathbf{w}_t \in \mathbb{Z}_q^{\alpha(k-1)n}$  is a uniform vector, for every  $t \in [T]$ . These variables along with a deterministic protocol given by  $r_1, \dots, r_T$  specify additional random variables that are determined by  $(\mathbf{x}^*, A_{1:T}, \mathbf{c}_{1:T}, \mathbf{w}_{1:T})$  including  $B_{1:t}, B_{r,1:t}, S_t^Y$ . Thus when we write a probability expression of the form  $\Pr[X]$  without specifying the random variables we intend the space to be  $\Omega$ . Furthermore an expression of the form  $\forall Y, \Pr[X|Y]$  is shorthand for  $\forall y, \Pr[X|Y=y]$ .

**Lemma 5.1** (Hybrid lemma). *For every  $q, k \in \mathbb{N}$ , there exists  $\alpha_0 > 0$  such that for every  $T \in \mathbb{N}$ , and  $\delta \in (0, 1)$ , there exists  $\tau \in (0, 1)$  and  $n_0 < \infty$  such that the following holds for every  $n \geq n_0$ :*

<sup>6</sup>Note that even though the  $t$ -th player does not have access to  $A_{1:t-1}, \mathbf{c}_{1:t-1}$ , and  $S_{1:t-2}$ , allowing them to see these only makes our lower bound stronger.

Let  $\Pi = (r_1, \dots, r_T)$  be a deterministic protocol for IFRMD where each message function  $r_t$  outputs a message of at most  $\tau n$  bits. Let  $(\mathbf{x}^*, A_{1:T}, \mathbf{c}_{1:T}, \mathbf{w}_{1:T}) \sim \Omega$ . Then there exists a sequence of events  $\{\mathcal{E}_t\}_{t \in [T]}$  and non-negative  $\delta_1, \dots, \delta_T$  with  $\sum_{t=1}^T \delta_t \leq \delta/2$  such that:

- (i)  $\mathcal{E}_1$  holds with probability 1. For  $t \geq 2$ ,  $\mathcal{E}_t$  only depends on  $(A_{1:t}, \mathbf{c}_{1:t})$  and  $S_{1:t-1}^Y$  (with  $S_{1:0}$  denoting an empty set of variables).
- (ii) For every  $t \geq 2$ ,  $\mathcal{E}_t \Rightarrow \mathcal{E}_{t-1}$  and  $\Pr[\overline{\mathcal{E}}_t | \mathcal{E}_{t-1}] \leq \delta_t$ .
- (iii) For every fixed  $(A_{1:t}, \mathbf{c}_{1:t})$  and  $S_{1:t-1}^Y$  satisfying  $\mathcal{E}_t$ , one has

$$\|S_t^Y - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \delta_t, \quad (5.2)$$

where  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)an})$ .

Theorem 3.5 follows almost immediately from Lemma 5.1 as shown in Section 5.1. In the rest of this paper we prove Lemma 5.1. In this section we introduce some new notions and state three key lemmas that together suffice to prove Lemma 5.1. This (conditional) proof is given in Section 5.4. In the following sections we prove the key lemmas. First we give an overview of the proof of Lemma 5.1 that explains the nature of these key lemmas.

The general idea behind the proof of Lemma 5.1 is to argue that information about  $\mathbf{x}^*$  “leaked” by the messages of the first  $t-1$  players (i.e.,  $S_{1:t-1}$ ) is not sufficient for the  $t$ -th player to distinguish between the case where  $\mathbf{w}_t = A_{t,c_t} \mathbf{x}^*$  (the **YES** case) and the case where  $\mathbf{w}_t$  is uniform. The earlier proofs of this type (in particular as in [KKS15]) simply counted the total information gleaned about  $\mathbf{x}^*$  which is bounded by the total communication. Such proofs are inherently limited to achieving only a  $\sqrt{n}$  lower bound. To go further [KK19] introduced the approach of reasoning about the structure of the information learned about  $\mathbf{x}^*$ . Note in particular that no player sees  $\mathbf{x}^*$  directly, and the  $t$ -th player only sees  $A_{t,c_t} \cdot \mathbf{x}^*$ . (In particular no coordinate of  $\mathbf{x}^*$  is revealed directly, though the sum of many pairs of coordinates are directly revealed.) Thus the information about  $\mathbf{x}^*$  comes from a “reduced space” and we would like to capture and exploit the structural restriction imposed by this restriction. Information-theoretic tools seem to fail to capture this restriction and the key to the work of [KK19] is to give a Fourier analytic condition, that they call “boundedness”, that captures this restriction.

The boundedness condition applies to what we call the “posterior distribution” of  $\mathbf{x}^*$ , i.e., the distribution of  $\mathbf{x}^*$  conditioned on the first  $t$  messages. This distribution turns out to be the uniform distribution over a set  $B_t \subseteq \mathbb{Z}_q^n$  (see Lemma 5.8). The boundedness condition places restrictions on the Fourier spectrum of the indicator function of this set. (See Definition 5.14.) To use this condition we need three ingredients elaborated below, which we abstract as lemma statements in this section and prove in later sections. Given these three lemmas the proof of Lemma 5.1 follows and is given in Section 5.4.

The first ingredient we need is that boundedness of  $B_{t-1}$  does imply that the  $t$ -th player is unable to distinguish between its input being from the **YES** distribution or the **NO** distribution. This is stated as Lemma 5.19. Next we need to show that given information about  $A_{t,c_t} \mathbf{x}^*$ , the posterior distribution of  $\mathbf{x}^*$  is indeed bounded, and we assert this in Lemma 5.18. Finally we argue that if  $B_{t-1}$  is bounded, then for most pairs of matchings  $A_t$  and centers  $\mathbf{c}_t$  the resulting set  $B_t$  is bounded. This is asserted in Lemma 5.20. See also Fig. 1 for a pictorial overview of the proof structure of Lemma 5.1.

In the rest of this section, after showing that Lemma 5.1 implies Theorem 3.5 in Section 5.1, we introduce the posterior sets and discuss their basic properties in Section 5.2, we introduce boundedness and state the three lemmas above in Section 5.3, and finally conclude with the proof of Lemma 5.1 in Section 5.4.

## 5.1 Proof of Theorem 3.5

We now show how the lemma suffices to prove [Theorem 3.5](#). The proof is analogous to the proof of Lemma 6.3 in [\[KK19\]](#). We remark that the lemma is not immediate and effectively depends on the fact that players can jointly sample from the **NO** distribution on their own. (Note the players can't jointly sample from the **YES** distribution since these samples are correlated by the hidden vector  $\mathbf{x}^*$ . So the proof is inherently asymmetric via the treatment of the **YES** and **NO** distributions.)

*Proof of Theorem 3.5.* For the sake of contradiction, assume that there exists a protocol  $\Pi = (r_1, \dots, r_T)$  that solves IFRMD with advantage more than  $\delta$  and less than  $\tau n$  bits of communication for some  $n \geq n_0$ . In what follows, we will show that  $\|(A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^Y) - (A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^N)\|_{tvd} \leq \delta$ , which implies that the advantage of the protocol cannot be greater than  $\delta$ , hence producing a contradiction.

Let  $\mathcal{E}_1 \supset \mathcal{E}_2 \supset \dots \supset \mathcal{E}_T$  be the sequence of events guaranteed by [Lemma 5.1](#) such that  $\Pr[\overline{\mathcal{E}}_t | \mathcal{E}_{t-1}] \leq \delta_t$  for  $t \geq 2$ . Note that by [Lemma 5.1](#), we also have

$$\|S_t^Y - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd, \mathcal{E}_t} \leq \delta_t$$

for all  $t \in [T]$ , where  $\|\cdot\|_{tvd, \mathcal{E}_t}$  denotes the total variation distance, conditioned on  $\mathcal{E}_t$ . We inductively show that for every  $t \in [T]$ ,

$$\|(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^Y) - (A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^N)\|_{tvd} \leq \sum_{1 \leq j \leq t} (\delta_j + \Pr[\overline{\mathcal{E}}_j | \mathcal{E}_{j-1}]) \quad (\text{Induction hypothesis})$$

where  $\mathcal{E}_0$  is the trivial event that is always true.

First, we prove the base case  $t = 1$ . Recalling that  $S_0^Y = S_0^N$ , we have

$$\begin{aligned} \|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, S_1^N)\|_{tvd, \mathcal{E}_1} &= \|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, r_1(M_1, \mathbf{c}_1, S_0^N, U_1))\|_{tvd, \mathcal{E}_1} \\ &= \|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, r_1(M_1, \mathbf{c}_1, S_0^Y, U_1))\|_{tvd, \mathcal{E}_1}. \end{aligned}$$

Observe that for every fixed  $A_1, \mathbf{c}_1$  and  $S_0^Y$  satisfying  $\mathcal{E}_1$ , we have  $\|S_1^Y - r_1(M_1, \mathbf{c}_1, S_0^Y, U_1)\|_{tvd} \leq \delta_1$ , where the randomness is over  $S_1^Y$  and  $U_1$ . It follows from [Lemma 2.3](#) that

$$\|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, r_1(M_1, \mathbf{c}_1, S_0^Y, U_1))\|_{tvd, \mathcal{E}_1} \leq \delta_1.$$

Therefore,

$$\begin{aligned} \|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, r_1(M_1, \mathbf{c}_1, S_0^Y, U_1))\|_{tvd} &\leq \|(A_1, \mathbf{c}_1, S_1^Y) - (A_1, \mathbf{c}_1, r_1(M_1, \mathbf{c}_1, S_0^Y, U_1))\|_{tvd, \mathcal{E}_1} + \Pr[\overline{\mathcal{E}}_1] \\ &\leq \delta_1 + \Pr[\overline{\mathcal{E}}_1], \end{aligned}$$

which completes the base case.

Next, we prove the inductive step. For every  $t = 2, \dots, T$ , we have

$$\begin{aligned} &\|(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^Y) - (A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^N)\|_{tvd} \\ &= \|(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_t \mathbf{x}^*)) - (A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^N, r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^N, U))\|_{tvd}. \end{aligned}$$

Let us define  $Q_{t-1}^Y = (A_{1:t-1}, \mathbf{c}_{1:t-1}, S_{1:t-1}^Y)$  and  $Q_{t-1}^N = (A_{1:t-1}, \mathbf{c}_{1:t-1}, S_{1:t-1}^N)$ . Then, we can rewrite the above expression for total variation distance in terms of the new notation as follows:

$$\|(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_t \mathbf{x}^*)) - (A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^N, r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^N, U))\|_{tvd}$$

$$= \|(Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)) - (Q_{t-1}^N, A_t, \mathbf{c}_t, r_t(Q_{t-1}^N, A_t, \mathbf{c}_t, U))\|_{tvd}. \quad (5.3)$$

We now apply [Lemma 2.4](#) to [Equation 5.3](#). Applying this lemma with  $X^1 = Q_{t-1}^Y$ ,  $X^2 = Q_{t-1}^N$ ,  $Z^1 = (A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)$ ,  $Z^2 = (A_t, \mathbf{c}_t, U)$ , and  $f$  as the function that maps the tuple  $(X, (B, C))$  to  $(B, r_t(X, B, C))$ , we get

$$\begin{aligned} & \|(Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)) - (Q_{t-1}^N, A_t, \mathbf{c}_t, r_t(Q_{t-1}^N, A_t, \mathbf{c}_t, U))\|_{tvd} \\ & \leq \|Q_{t-1}^Y - Q_{t-1}^N\|_{tvd} + \|(Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)) - (Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, U))\|_{tvd}. \end{aligned} \quad (5.4)$$

Now, by applying the induction hypothesis, we have that

$$\|Q_{t-1}^Y - Q_{t-1}^N\|_{tvd} \leq \sum_{j=1}^{t-1} (\delta_j + \Pr[\overline{\mathcal{E}}_j | \mathcal{E}_{j-1}]). \quad (5.5)$$

Next, we bound the second term on the right hand side of [\(5.4\)](#), i.e.,

$$\|(Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)) - (Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, U))\|_{tvd},$$

by applying condition (iii) from [Lemma 5.1](#). According to this condition, for every *fixed*  $(A_{1:t}, \mathbf{c}_{1:t})$  and  $S_{1:t-1}^Y$  satisfying  $\mathcal{E}_t$ , we have

$$\|r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t,\mathbf{c}_t} \mathbf{x}^*) - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \delta_t,$$

where  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})$ . Thus, by [Lemma 2.3](#), it follows that

$$\|(Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, A_{t,\mathbf{c}_t} \mathbf{x}^*)) - (Q_{t-1}^Y, A_t, \mathbf{c}_t, r_t(Q_{t-1}^Y, A_t, \mathbf{c}_t, U))\|_{tvd, \mathcal{E}_t} \leq \delta_t. \quad (5.6)$$

Combining [Eqs. \(5.3\)](#) to [\(5.6\)](#), we have

$$\|(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^Y) - (A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^N)\|_{tvd} \leq \sum_{j=1}^t (\delta_j + \Pr[\overline{\mathcal{E}}_j | \mathcal{E}_{j-1}]),$$

which completes the induction.

Thus,

$$\|(A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^Y) - (A_{1:T}, \mathbf{c}_{1:T}, S_{1:T}^N)\|_{tvd} \leq \sum_{j=1}^T (\delta_j + \Pr[\overline{\mathcal{E}}_j | \mathcal{E}_{j-1}]) \leq 2 \cdot \sum_{j=1}^T \delta_j \leq \delta.$$

This implies that  $\Pi$  cannot have advantage more than  $\delta$ , which contradicts the assumptions of the theorem statement. Therefore, we conclude that any protocol for IFRMD with advantage  $\delta$  requires  $\tau n$  bits of communication, as desired.  $\square$

## 5.2 Posterior sets and functions

The main challenge in proving [Lemma 5.1](#) lies in the condition (iii), i.e., requiring the closeness of the Yes message (i.e.,  $S_t^Y = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t,\mathbf{c}_t} \mathbf{x}^*)$ ) and the hybrid No message (i.e.,  $r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)$ ). Intuitively, if  $\mathbf{x}^* \sim \text{Unif}(\mathbb{Z}_q^n)$  and is independent of the other arguments, then  $A_{t,\mathbf{c}_t} \mathbf{x}^*$  is uniformly distributed over  $\mathbb{Z}_q^{(k-1)\alpha n}$  and hence  $S_t^Y$  follows the same distribution as

$r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)$ . However,  $\mathbf{x}^*$  is correlated<sup>7</sup> with the previous messages  $S_{1:t-1}^Y$  so the above ideal situation would not happen in general. Nevertheless, we are able to analyze the conditional distribution of  $A_{t,\mathbf{c}_t}\mathbf{x}^*$  on the previous messages by explicitly characterizing the *posterior distribution* of  $\mathbf{x}^*$  after receiving the messages from the first  $t-1$  players. That is, the conditional distribution of  $A_{t,\mathbf{c}_t}\mathbf{x}^*$  can be described by first sampling  $\mathbf{x}^*$  from the posterior distribution and then applying  $A_{t,\mathbf{c}_t}$ .

For every fixed  $A_{1:t}, \mathbf{c}_{1:t}$  and  $S_{1:t}$ , we would like to identify a distribution  $\mathcal{D}_t$  over  $\mathbb{Z}_q^n$  such that  $\mathcal{D}_t$  is the conditional distribution of  $\mathbf{x}^*$  given messages  $S_{1:t}$ . Note that by the choice of the No case, the conditional distribution of  $\mathbf{x}^*$  given messages  $S_{1:t}$  is simply the uniform distribution over  $\mathbb{Z}_q^n$ . Thus, we only need to worry about the Yes case.

**Definition 5.7** (Posterior sets and functions). *Under the setting described above, for each  $t$  and fixed  $A_{1:t}, \mathbf{c}_{1:t}$ , and  $S_{1:t}$ , define*

- (Reduced posterior set)  $B_{r,t} \subseteq \mathbb{Z}_q^{(k-1)m}$  be the set of possible values of  $z_t = A_{t,\mathbf{c}_t}\mathbf{x}$  that leads to message  $S_t$ ; Note that  $B_{r,t}$  should be thought of as a function on  $A_t, \mathbf{c}_t$ , and  $S_t$  in the sense that  $B_{r,t} = g_t^{-1}(S_t)$  where  $g_t(\cdot) = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}, \cdot)$ . Let  $\mathbf{1}_{B_{r,t}}$  be the indicator function of  $B_{r,t}$ .

- (Posterior set and function) Let

$$B_t := \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{t,\mathbf{c}_t}\mathbf{x} \in B_{r,t}\}.$$

Also, let  $\mathbf{1}_{B_t} : \mathbb{Z}_q^n \rightarrow \{0, 1\}$  be the indicator function of  $B_t$ .

- (Aggregated posterior set and function) Let

$$B_{1:t} := \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{t',\mathbf{c}_{t'}}\mathbf{x} \in B_{r,t'}, \forall t' = 1, \dots, t\} = \bigcap_{t'=1}^t B_{t'}.$$

Also, let  $\mathbf{1}_{B_{1:t}} : \mathbb{Z}_q^n \rightarrow \{0, 1\}$  be the indicator function of  $B_{1:t}$ . Namely,  $\mathbf{1}_{B_{1:t}} = \prod_{t'=1}^t \mathbf{1}_{B_{t'}}$ .

Now, we show that  $\mathbf{1}_{B_{1:t}}$  captures the posterior distribution (i.e., the conditional distribution) of  $\mathbf{x}$  given messages  $S_1, S_2, \dots, S_t$ :

**Lemma 5.8** (Posterior function  $\mathbf{1}_{B_{1:t}}$  captures the posterior distribution.). *For every  $t \in [T]$ ,  $\mathbf{a} \in \mathbb{F}_q^n$ ,  $A_{1:t}$ ,  $\mathbf{c}_{1:t}$  and  $S_{1:t}$ ,*

$$\Pr[\mathbf{x}^* = \mathbf{a} \mid A_{1:t}, \mathbf{c}_{1:t}, S_{1:t}^Y] = \mathbf{1}_{B_{1:t}}(\mathbf{a}) / |B_{1:t}|.$$

*In particular, for fixed  $A_{1:t}, \mathbf{c}_{1:t}$ , and  $S_{1:t-1}^Y$ , we have  $S_t^Y = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t,\mathbf{c}_t}\mathbf{x}^*)$ , where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t-1})$ .*

*Proof.* Recall that  $S_t^Y = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t,\mathbf{c}_t}\mathbf{x}^*)$  by definition,  $B_t = \{\mathbf{b} \in \mathbb{F}_q^n \mid r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t,\mathbf{c}_t}\mathbf{b}) = S_t^Y\}$ , and  $B_{1:t} = B_1 \cap B_2 \cap \dots \cap B_t$ . It follows that if  $\mathbf{a} \notin B_{1:t}$  then there must exist a smallest index such that  $S_i^Y \neq r_i(A_{1:i}, \mathbf{c}_{1:i}, S_{1:i-1}^Y, A_{i,\mathbf{c}_i}\mathbf{a})$  and so the probability that  $\mathbf{x}^* = \mathbf{a}$  conditioned on  $r_i(A_{1:i}, \mathbf{c}_{1:i}, S_{1:i-1}^Y, A_{i,\mathbf{c}_i}\mathbf{x}^*) = S_i^Y$  is zero. For  $\mathbf{a} \in B_{1:t}$ , we simply note that  $\mathbf{x}^*$  is a priori uniformly distributed over  $\mathbb{Z}_q^n$  and conditioning on any event (in our case that  $\mathbf{x}^* \in B_{1:t}$ ) its distribution is uniform on the subset of  $\mathbb{Z}_q^n$  for which the event holds.  $\square$

<sup>7</sup>In particular,  $\mathbf{x}^*$  has to be consistent with the previous messages  $S_{1:t-1}^Y$ .

Now that we have a characterization of the posterior distribution of  $\mathbf{x}^*$ , the following corollary shows that Equation 5.2 (i.e., the condition (iii) of Lemma 5.1) can be simplified to bounding the total variation distance between the posterior distribution and the uniform distribution.

**Corollary 5.9** (Reducing Eq. (5.2)). *Let  $r_t, S_{1:t-1}^Y, A_{1:t}, \mathbf{c}_{1:t}, B_{1:t}, U$  be defined as before, we have*

$$\|r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t, \mathbf{c}_t} \mathbf{x}^*) - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \|(A_{t, \mathbf{c}_t} \mathbf{x}^*) - U\|_{tvd}$$

where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t})$ .

*Proof.* By Lemma 5.8, we have

$$S_t^Y = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t, \mathbf{c}_t} \mathbf{x}^*)$$

where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t})$ . Note that when we fix  $A_{1:t}, \mathbf{c}_{1:t}$ , and  $S_{1:t-1}^Y$  (hence  $B_{1:t}$  is also fixed), by data processing inequality (see item 2 of Proposition 2.2) we have

$$\|r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t, \mathbf{c}_t} \mathbf{x}^*) - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \|(A_{t, \mathbf{c}_t} \mathbf{x}^*) - U\|_{tvd}. \quad \square$$

Namely, Equation 5.2 (i.e., the condition (iii) of Lemma 5.1) can be replaced with  $\|(A_{t, \mathbf{c}_t} \mathbf{x}^*) - U\|_{tvd} \leq \delta/T$ , i.e., after applying a random folded hypermatching matrix  $A_{t, \mathbf{c}_t}$  to the posterior distribution  $\text{Unif}(B_{1:t})$ , the distribution of the resulting string is close to the uniform distribution  $\text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})$ .

Finally, the following lemma shows that when the amount of communication is small, the posterior set is large with high probability.

**Lemma 5.10** (Posterior set is large). *Let  $\Pi = (r_1, \dots, r_T)$  be a deterministic protocol for IFRMD where each message function  $r_t$  outputs a message of length at most  $s$  bits for some  $1 \leq s \leq n$ . Let  $B_t$  be the posterior set defined in Definition 5.7 for every  $t \in [T]$ . For every  $\delta \in (0, 1)$  and  $t \in [T]$ , we have  $|B_t| \geq \delta \cdot q^{n-s}$  with probability at least  $1 - \delta$  over the randomness of  $\mathbf{x} \in \mathbb{Z}_q^n$ .*

*Proof.* Fix a hypermatching  $M$  and centers  $\mathbf{c}$ , the  $t$ -th message function induces a partition  $P_1 \cup P_2 \cup \dots \cup P_{2^s}$  of  $\mathbb{Z}_q^n$ . For each  $\mathbf{x} \in \mathbb{Z}_q^n$ , we define  $P(\mathbf{x})$  to be the part that contains  $\mathbf{x}$ , i.e., if  $\mathbf{x} \in P_i$ , then  $P(\mathbf{x}) = P_i$ . Note that

$$\mathbb{E}_{\mathbf{x} \in \mathbb{Z}_q^n} \left[ \frac{1}{|P(\mathbf{x})|} \right] = \sum_{i=1}^{2^s} \frac{\Pr_{\mathbf{x} \in \mathbb{Z}_q^n}[\mathbf{x} \in P_i]}{|P_i|} = \sum_{i=1}^{2^s} \frac{|P_i| \cdot q^{-n}}{|P_i|} = \frac{2^s}{q^n} \leq q^{s-n}.$$

By Markov's inequality, we have  $|P(\mathbf{x})| < \delta \cdot q^{n-s}$  with probability at most  $\delta$  as desired.  $\square$

### 5.3 Fourier analytic conditions

In this subsection, we define and analyze Fourier-analytic properties of the posterior set  $B$  and show that these properties are sufficient for the condition (iii) (i.e., Corollary 5.9) of Lemma 5.1.

#### 5.3.1 Three key definitions

Recall that given a matching  $M = (e_1, \dots, e_m)$  and centers  $\mathbf{c} = (c_1, \dots, c_m)$ ,  $A_{\mathbf{c}}$  is the  $\mathbf{c}$ -centered folded encoding of  $M$ . We are going to define three properties for sets  $B$  in  $\mathbb{Z}_q^n$ . First, we say a set  $B \subseteq \mathbb{Z}_q^n$  is  $(M, \mathbf{c})$ -restricted if  $B$  is a union of cosets (affine shifts) of the null space of  $A_{\mathbf{c}}$ .

**Definition 5.11** (Restricted set). Let  $M$  be a  $k$ -hypermatching of size  $m$  and  $\mathbf{c}$  be centers. We say a set  $B \subseteq \mathbb{Z}_q^n$  is  $(M, \mathbf{c})$ -restricted if there exists a (“reduced”) set  $B_r \subseteq \mathbb{Z}_q^{(k-1)m}$  such that  $B = \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{\mathbf{c}}\mathbf{x} \in B_r\}$ .

Note that the posterior set (Definition 5.7) of round  $t$  is  $(M_t, \mathbf{c}_t)$ -restricted.

Next, we introduce the notion of a subset of  $\mathbb{Z}_q^n$  being (strongly/weakly) bounded. These notions are similar to those in [KK19, Definition 4.3]. They say that a set  $B$  is bounded if the Fourier spectrum of the indicator function  $\mathbf{1}_B$  can be appropriately bounded in terms of the  $\ell_1$  norm on various Hamming levels.

First, we introduce some notation. Note that for every set  $B \subseteq \mathbb{Z}_q^n$ , the  $\mathbf{0}$ -th Fourier coefficient of the indicator function  $\mathbf{1}_B$  is  $|B|/q^n$ . In what follows we study the Fourier coefficients of  $\mathbf{1}_B$  after scaling by  $q^n/|B|$  so that the  $\mathbf{0}$ -th Fourier coefficient after scaling has value 1. In what follows we define weak and strong bounding functions for the  $\ell_1$  norm of the Fourier coefficients based on Hamming weight. Not all functions will satisfy the desired bounds, but indicators of posterior sets turn out to satisfy these bounds and this is the crux of our (and [KK19]’s) analysis.

$$W_{C,s}(h) := \begin{cases} 1, & h = 0, \\ \left(\frac{C\sqrt{sn}}{h}\right)^{h/2}, & 1 \leq h \leq s, \\ \infty, & h > s. \end{cases} \quad (5.12)$$

$$U_{C,s}(h) := \begin{cases} W_{C,s}(h), & 0 \leq h \leq s, \\ \min \left\{ W_{C,h}(h), \left(\frac{2q^2e^2n}{h}\right)^{h/2} \right\}, & h > s. \end{cases} \quad (5.13)$$

(Above,  $U$  stands for Upper bound, while  $W$  stands for a Weak upper bound.)

**Definition 5.14** ((Strongly/weakly) Bounded set). Let  $n, q \in \mathbb{N}$ ,  $0 \leq s \leq n$ ,  $C > 0$ , and  $B \subset \mathbb{Z}_q^n$ . We say  $B$  (as well as its indicator function  $\mathbf{1}_B$ ) is  $(C, s)$ - (strongly)-bounded if, for every  $h \in [n]$ ,

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}_B}(\mathbf{u}) \right| \leq U_{C,s}(h). \quad (5.15)$$

We say that  $B$  is  $(C, s)$ -weakly-bounded if the bound on the RHS above is replaced by  $W_{C,s}(h)$ . (Unless otherwise specified we use “bounded” to mean “strongly bounded”.)

**Remark.** As we keep track of posterior sets that are inductively refined, we will need the entire Fourier spectrum of the corresponding indicator functions to be bounded from above by the function  $U_{C,s}$  (for appropriate  $C, s > 0$ ). The notion of boundedness is such that it allows us to show that  $A_{\mathbf{c}}\mathbf{x}$  is close to the uniform distribution on  $\mathbb{Z}_q^{(k-1)\alpha n}$  when  $\mathbf{x}$  is drawn from a bounded posterior set  $B \subset \mathbb{Z}_q^n$  (see Lemma 5.19). Our upper bounds typically establish only the weak bound  $W_{C,s}(h)$  (particularly, Lemma 6.18 and Lemma 6.26), we usually prove this holds for every  $s$  in some large interval and this allows us along with standard Fourier analysis (see Lemma 6.5) to establish the stronger bound for a slightly worse choice of constant  $C$ .

We describe some non-trivial properties of boundedness in Section 6 but we start with some elementary assertions.

**Proposition 5.16.** 1. If  $B \subseteq \mathbb{Z}_q^n$  is  $(C, s)$ - (strongly/weakly)-bounded then it is also  $(C', s)$ - (strongly/weakly)-bounded for every  $C' \geq C$ .

2. The set  $B_0 = \mathbb{Z}_q^n$  is  $(C, s)$ -strongly-bounded for every  $C \geq 0$  and every  $0 \leq s \leq n$ .

*Proof.* Part (1) follows from the fact that  $W_{C,s}(h) \leq W_{C',s}(h)$  and  $U_{C,s}(h) \leq U_{C',s}(h)$  for every  $s, h$  and  $C' \geq C$ . Part (2) follows from the fact that  $\widehat{\mathbf{1}}_B(\vec{0}) = 1$  and  $\widehat{\mathbf{1}}_B(\mathbf{u}) = 0$  for all non-zero  $\mathbf{u} \in \mathbb{Z}_q^n$  and so  $B_0$  is  $(0, s)$ -strongly-bounded for every  $0 \leq s \leq n$ . Combining with Part (1) now yields the claim for every  $C \geq 0$ .  $\square$

Finally, in what follows we will show that the intersection of a bounded set with a “restricted set” is also bounded and this will be the core of our induction. To do this we need to understand the Fourier behavior of restricted sets. It turns out that restricted sets satisfy a property stronger than being bounded, which we term “reduced”-ness below.

**Definition 5.17** ((Weakly/Strongly) Reduced set). *Let  $n, q \in \mathbb{N}$ ,  $0 \leq s \leq n$ ,  $C > 0$ , and  $B \subset \mathbb{Z}_q^n$ . Let  $M$  be a  $k$ -hypermatching. We say  $B$  (as well as its indicator function  $\mathbf{1}_B$ ) is  $(M, C, s)$ -(strongly)-reduced if the following hold.*

- For every  $\mathbf{u} \in \mathbb{Z}_q^n$ , if there exists  $i \in [n]$  such that  $u_i = 1$  but  $i$  is not contained<sup>8</sup> in  $M$  (i.e., none of the hyperedges of  $M$  contains  $i$ ), then  $\widehat{\mathbf{1}}_B(\mathbf{u}) = 0$ .
- For every  $\mathbf{u} \in \mathbb{Z}_q^n$ , if there exists a hyperedge  $e_i$  of  $M$  such that  $\langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$ , then  $\widehat{\mathbf{1}}_B(\mathbf{u}) = 0$ .
- For every  $h \in \{1, \dots, n\}$  and  $\mathbf{v} \in \mathbb{Z}_q^n$ ,

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \leq U_{C,s}(h).$$

If the bound in the RHS is replaced by the weaker  $W_{C,s}(h)$  bound, then we say that  $B$  is a weakly-reduced set. (Again we usually suppress the word “strongly” and simply refer to strongly-reduced sets as reduced set.)

As a remark, the first two conditions in the definition of reducedness are motivated by the Fourier analytic properties of posterior sets (e.g., [Lemma 6.1](#), and [Claim 6.17](#)). The third condition is a strengthening of boundedness. In particular the third condition applied with  $\mathbf{v} = \mathbf{0}$  implies that every  $(M, C, s)$ -(strongly/weakly)-reduced set  $B$  is also  $(C, s)$ -(strongly/weakly)-bounded. That is why we say reducedness is the intersection of restrictedness and boundedness.

In summary, restrictedness ([Definition 5.11](#)) is a certain posterior property and boundedness is a certain Fourier analytic condition while reducedness is the intersection of the two. By [Definition 5.7](#), we immediately have that each posterior set  $B_t$  is  $(M_t, \mathbf{c}_t)$ -restricted and in the lemmas stated below we will establish that  $B_t$  is  $(M_t, C_0, s)$ -reduced and the aggregated posterior set  $B_{1:t}$  is  $(C_t, s)$ -bounded with high probability (for some choices of parameters  $s, C_0, C_1, \dots, C_T$ ). See also [Fig. 1](#) for a pictorial view of these definitions.

### 5.3.2 Three key lemmas

There are three key lemmas about these Fourier analytic conditions. The first lemma establishes the “large” enough restricted sets are reduced. We typically apply this lemma to the sets  $B_t$ .

---

<sup>8</sup>We use “contained in” and “touched by” interchangeably as in some later contexts it makes more sense to use “touched by” when working with a set of vertices or hyperedges.

**Lemma 5.18** (Posterior set). *For every  $q, k \geq 2$ , there exist constants  $\varepsilon_0 > 0$  and  $C_0 < \infty$  such that for every sufficiently large  $n$ , every  $k$ -hypermatching  $M$  on vertex set  $[n]$ , every pair of integers  $b, s$  satisfying  $0 < b \leq s \leq \varepsilon_0 \cdot n$  the following holds. If  $B \subseteq \mathbb{Z}_q^n$  satisfies (i) there exists a sequence of centers  $\mathbf{c}$  such that  $B$  is  $(M, \mathbf{c})$ -restricted, and (ii)  $|B| \geq q^{n-b}$ , then  $B$  is  $(M, C_0, s)$ -reduced.*

The proof of Lemma 5.18 is given in Section 6.3.

Recall from Corollary 5.9 that the condition (iii) in Lemma 5.1 is implied by showing  $A_{\mathbf{c}}\mathbf{x}$  is close to the uniform distribution over  $\mathbb{Z}_q^{(k-1)m}$  with high probability over the choice of  $A_{\mathbf{c}}$  where  $\mathbf{x}$  is sampled uniformly from the posterior set  $B_{1:t}$ . The second key lemma shows that  $A_{\mathbf{c}}\mathbf{x}^*$  is indeed close to uniform when the posterior set is bounded.

**Lemma 5.19** (Boundedness implies (closeness to) uniformity). *For every  $q, k \geq 2$  there exists  $\alpha_0 = \alpha_0(k, q)$  such that for every  $\delta \in (0, 1/2)$  and  $C < \infty$ , there exists  $\tau = \tau(q, k, \delta, C) > 0$  and  $s_0 = s_0(\delta) < \infty$  such that the following holds for every sufficiently large  $n$ :*

*Let  $B \subseteq \mathbb{Z}_q^n$  be a  $(C, s)$ -bounded set with  $|B| \geq q^{n-b}$ , for  $s_0 \leq b \leq s \leq \tau n$ . Let  $M$  be a random  $k$ -hypermatching of size  $m \leq \alpha_0 n$  and  $\mathbf{c}$  be a uniformly random sequence of centers for  $M$  and let  $A_{\mathbf{c}}$  denote the  $\mathbf{c}$  centered folded encoding of  $M$ . Then, with probability at least  $1 - \delta$  over the choice of  $M$  and  $\mathbf{c}$ , for every  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ , we have that*

$$1 - \delta < q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}}\mathbf{x} = \mathbf{z}_0] < 1 + \delta.$$

As a consequence, we also have (with probability at least  $1 - \delta$  over the choice of  $(M, \mathbf{c})$ ):

1.  $\|(A_{\mathbf{c}}\mathbf{x}) - U\|_{\text{tvd}} \leq \delta$  where  $\mathbf{x} \sim \text{Unif}(B)$  and  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)m})$ .
2. For every non-negative function  $f : \mathbb{Z}_q^{(k-1)m} \rightarrow \mathbb{R}^{\geq 0}$ ,

$$(1 - \delta) \leq \frac{\mathbb{E}_{\mathbf{x} \sim \text{Unif}(B)} [f(A_{\mathbf{c}}\mathbf{x})]}{\mathbb{E}_{\mathbf{z} \sim \text{Unif}(\mathbb{Z}_q^{(k-1)m})} [f(\mathbf{z})]} \leq (1 + \delta).$$

The proof of Lemma 5.19 is postponed to Section 6.4.

Our final lemma of this section asserts that if  $\mathbf{1}_{B_{1:t}}$  is  $(C, s)$ -bounded, then  $f_{1:t+1}$  is  $(O(C), s)$ -bounded with high probability.

**Lemma 5.20** (Induction step). *For every  $q, k \in \mathbb{N}$  there exist  $\alpha_0 > 0$  and  $C_0 < \infty$  such that for every  $C \geq C_0$ , and  $\delta \in (0, 1/2)$ , there exist  $\tau_0 = \tau_0(q, k, \delta, C) \in (0, 1)$  and  $C' = C'(q, k, \delta, C) > 0$  such that the following holds. For every  $n, b, b', s, m \in \mathbb{N}$ , satisfying  $m \leq \alpha_0 n$ ,  $0 < b, b', s < \tau_0 n$  and every  $(C, s)$ -bounded set  $B \subseteq \mathbb{Z}_q^n$  satisfying  $|B| \geq q^{n-b}$ , we have that with probability at least  $1 - 4\delta$  over a uniformly random  $k$ -hypermatching  $M$  of size  $m$  and every  $(M, C_0, s)$ -reduced set  $B' \subseteq \mathbb{Z}_q^n$  satisfying  $|B'| \geq q^{n-b'}$  and  $|B \cap B'| \geq (1 - \delta) \cdot |B| \cdot |B'| / q^n \geq q^{n-s}$ , we have  $B \cap B'$  is  $(C', s)$ -bounded.*

Lemma 5.20 is proved in Section 6.5. In our inductive application of the lemma above, we set  $B \leftarrow B_{1:t-1}$  and  $B' \leftarrow B_t$  for every  $t \in \{2, 3, \dots, T\}$  to get that all the  $B_t$ 's are bounded and this is the core of the proof of Lemma 5.1.

## 5.4 Proof of Lemma 5.1

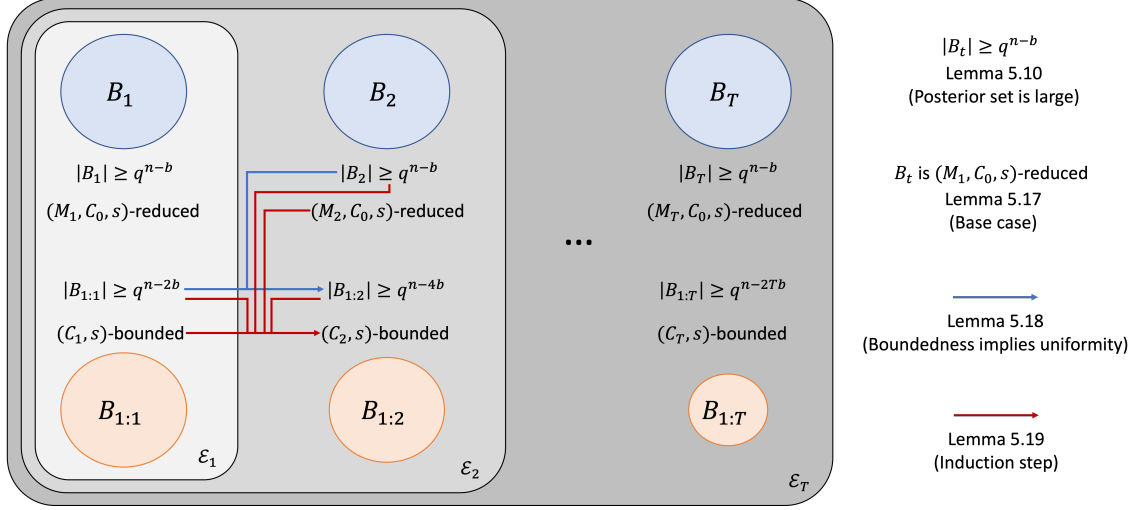


Figure 1: A pictorial overview of the proof of Lemma 5.1. Each posterior set  $B_t$  (the blue sets) is both  $(M_t, \mathbf{c}_t)$ -restricted (followed from Definition 5.7) and  $(M_t, C_0, s)$ -reduced (followed from Lemma 5.18). Each aggregated posterior set  $B_{1:t}$  (the orange sets) is  $(C_t, s)$ -bounded (followed from Lemma 5.20).

**Lemma 5.1** (Hybrid lemma). *For every  $q, k \in \mathbb{N}$ , there exists  $\alpha_0 > 0$  such that for every  $T \in \mathbb{N}$ , and  $\delta \in (0, 1)$ , there exists  $\tau \in (0, 1)$  and  $n_0 < \infty$  such that the following holds for every  $n \geq n_0$ :*

*Let  $\Pi = (r_1, \dots, r_T)$  be a deterministic protocol for IFRMD where each message function  $r_t$  outputs a message of at most  $\tau n$  bits. Let  $(\mathbf{x}^*, A_{1:T}, \mathbf{c}_{1:T}, \mathbf{w}_{1:T}) \sim \Omega$ . Then there exists a sequence of events  $\{\mathcal{E}_t\}_{t \in [T]}$  and non-negative  $\delta_1, \dots, \delta_T$  with  $\sum_{t=1}^T \delta_t \leq \delta/2$  such that:*

- (i)  $\mathcal{E}_1$  holds with probability 1. For  $t \geq 2$ ,  $\mathcal{E}_t$  only depends on  $(A_{1:t}, \mathbf{c}_{1:t})$  and  $S_{1:t-1}^Y$  (with  $S_{1:0}$  denoting an empty set of variables).
- (ii) For every  $t \geq 2$ ,  $\mathcal{E}_t \Rightarrow \mathcal{E}_{t-1}$  and  $\Pr[\overline{\mathcal{E}}_t | \mathcal{E}_{t-1}] \leq \delta_t$ .
- (iii) For every fixed  $(A_{1:t}, \mathbf{c}_{1:t})$  and  $S_{1:t-1}^Y$  satisfying  $\mathcal{E}_t$ , one has

$$\|S_t^Y - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \delta_t, \quad (5.1)$$

where  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})$ .

*Proof of Lemma 5.1.*

**Overview of proof:** (See Fig. 1 for a pictorial overview of the proof.) The rough overview of the proof is to show that for an appropriate choice of the constants  $C_1, \dots, C_T$ , for every  $t \in [T]$ , the posterior set  $B_{1:t}$  is  $(C_t, s)$ -bounded. Once we have this, we can apply “boundedness implies uniformity” lemma (Lemma 5.19) to conclude that the messages sent by the  $t$ th player on the YES and NO distributions are indistinguishable. To show the boundedness condition for  $B_{1:t}$  we use induction to deduce that  $B_{1:t-1}$  is bounded, and then reason about  $B_t$  to conclude that it

is large,  $(M, C_0, s)$ -reduced (for appropriate  $C_0$ ), and crucially that it is roughly independent of  $B_{1:t-1}$ . Proving the above involves, among other reasoning, another application of the boundedness implies uniformity lemma (on  $B_{1:t-1}$ ). With these ingredients in place the induction step lemma (Lemma 5.20) yields the boundedness of  $B_{1:t}$ . We give the details below.

**Setting of parameters:** We note that in addition to the parameters  $\alpha_0, \tau, n_0, \{\delta_t\}_{t \in [T]}$  required by the lemma statement, we also need to specify the constants  $\{C_t\}_{t \in [T]}$  alluded to in the overview. Additionally we also specify three integer parameters:  $s^*$  which specifies the length of the message,  $b$  which quantifies largeness of various posterior sets, and  $s$  which quantifies the boundedness of posterior functions.

Given  $q$  and  $k$ , let  $\alpha_{0,1}$  be the  $\alpha_0(k, q)$  from Lemma 5.19 and  $\alpha_{0,2}$  be the  $\alpha_0(k, q)$  from Lemma 5.20. We set  $\alpha_0 = \min\{\alpha_{0,1}, \alpha_{0,2}\}$ . Let  $\varepsilon_0 = \varepsilon_0(k, q)$  and  $C_0 = C_0(k, q)$  be the constants from Lemma 5.18. Now given  $T$  and  $\delta$ , we need to specify  $\tau > 0$  and  $n_0 < \infty$ . We first set a large number of intermediate parameters that will be used in the rest of the proof. Recall that Lemma 5.20 takes as input parameters  $q, k, \delta$  and  $C \geq C_0$  and gives constants  $C' = C'(q, k, \delta, C)$  and  $\tau_0(q, k, \delta, C)$  for which the lemma holds. We let  $\delta' = \delta/(12 \cdot 2^T)$  and  $\delta_1 = 6\delta'$  and  $\delta_{t+1} = 2\delta_t$  for  $1 \leq t \leq T-1$ . (Note these settings satisfy  $\sum_{t=1}^T \delta_t \leq \delta/2$ , as required in the conclusion of the lemma, and  $\delta_{t+1} \geq \sum_{i=1}^t \delta_i + 6\delta'$  as required in the proof below.) For  $t \in [T]$  we set  $C_t = C'(q, k, \delta', C_{t-1})$  where  $C'(\dots)$  is the aforementioned function from Lemma 5.20. Next for every  $t \in [T]$  we set  $\gamma_t = \tau_0(q, k, \delta', C_t)$ . Further, let  $\tau(q, k, \delta, C)$  and  $s_0(\delta)$  be the functions from Lemma 5.19. For  $t \in [T]$ , let  $\rho_t = \tau(q, k, \delta', C_t)$  and  $s_0 = s_0(\delta')$ . Let  $\zeta = \min\{\varepsilon_0, \min_{t \in [T]}\{\gamma_t\}, \min_{t \in [T]}\{\rho_t\}\}$ . Let  $\nu = \zeta/(2T)$  and let  $\tau = \nu/2$ .

Finally we let  $n_0 = \max\{\frac{2}{\nu} \log_q(1/\delta'), s_0/\nu\}$ .<sup>9</sup> Finally, given  $n \geq n_0$  we set  $s = \zeta n$ ,  $b = \nu n$  and  $s^* = \tau n$ .

Note that these settings ensure  $b \geq 1$ ,  $s^* \leq b/2 \leq b - \log_q(1/\delta')$ ,  $2tb \leq s \leq \varepsilon_0 n$  for every  $t \in [T]$ ,  $s \leq \gamma_t n = \tau_0(q, k, \delta', C_t)n$  for every  $t \in [T]$  and  $s_0 \leq b \leq 2tb \leq s \leq \rho_t n = \tau(q, k, \delta', C_t)n$  for every  $t \in [T]$ . These inequalities will be used in the proof below.

**The events  $\{\mathcal{E}_t\}_{t \in [T]}$ :** Recall the notion of posterior sets  $B_t$  and aggregate posterior sets  $B_{1:t}$  for  $t \in [T]$  from Definition 5.7. Let  $B_0 = \mathbb{Z}_q^n$ . We define  $\mathcal{E}_1$  to be the event that  $B_0$  is  $(C_0, s)$ -bounded and large i.e.,  $|B_0| \geq q^n$ . For  $2 \leq t \leq T$ , let  $\mathcal{E}_t^1$  denote the event that  $B_{t-1}$  is  $(M_{t-1}, C_0, s)$ -reduced and the aggregated posterior set  $B_{1:t-1}$  is  $(C_{t-1}, s)$ -bounded and large i.e.,  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$ . We also define  $\mathcal{E}_t^2$  to be the event that  $\|A_{t, \mathbf{c}_t} \mathbf{x}^* - U\|_{tvd} \leq \delta_t$ , where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t-1})$  and  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)an})$ . Finally, let  $\mathcal{E}_t = \mathcal{E}_{t-1} \cap \mathcal{E}_t^1 \cap \mathcal{E}_t^2$ . We now turn to proving conditions (i)-(iii) hold for this choice of events.

**Causality and Indistinguishability:** It is immediate from the definition that  $\mathcal{E}_t \implies \mathcal{E}_{t-1}$  and  $\mathcal{E}_t$  only depends on  $A_{1:t}, \mathbf{c}_{1:t}$ , and  $S_{1:t-1}^Y$ . This establishes condition (i). Next we note that conditioned on  $\mathcal{E}_t$  we have condition (iii). In particular, by the definition of  $\mathcal{E}_t$ , we have  $\|(A_{t, \mathbf{c}_t} \mathbf{x}^*) - U\|_{tvd} \leq \delta_t$  where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t-1})$  and  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)an})$ . As  $S_t^Y = r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, A_{t, \mathbf{c}_t} \mathbf{x}^*)$  where  $\mathbf{x}^* \sim \text{Unif}(B_{1:t-1})$  (by Lemma 5.8), by the data processing inequality we have

$$\|S_t^Y - r_t(A_{1:t}, \mathbf{c}_{1:t}, S_{1:t-1}^Y, U)\|_{tvd} \leq \|A_{t, \mathbf{c}_t} \mathbf{x}^* - U\| \leq \delta_t$$

as desired for condition (iii). It remains to prove (ii) which we do from now on.

<sup>9</sup>The reader may notice that several of the terms in the parameter settings obviously dominate the others and we could skip the mins and maxes thereby simplifying the expressions. But we keep them separate for easier verifiability in the proof. We follow this practice through most of this paper.

**Probability of bad events:** By definition of  $B_0 = \mathbb{Z}_q^n$ , we have it is large (i.e.,  $|B_0| \geq q^n$ ). Further by Part (2) of [Proposition 5.16](#) we have that  $B_0$  is  $(C_0, s)$ -bounded. Thus it follows that  $\mathcal{E}_1$  holds with probability 1. We now analyze  $\mathcal{E}_{t+1}^1$  for  $t \geq 1$  (and then turn to  $\mathcal{E}_{t+1}^2$ ). We show that, conditioned on  $\mathcal{E}_t$ ,  $\mathcal{E}_{t+1}^1$  holds with probability at least  $1 - 5\delta' - \sum_{i=1}^t \delta_i$ . The main part of it is proving that  $B_{1:t}$  is large, which we do in the claim below. (Proving boundedness is then a straightforward application of [Lemma 5.20](#), as we show later.)

**Claim 5.21.** *Let  $2 \leq t \leq T$ . Let  $M_t$  and  $\mathbf{c}_t$  be chosen uniformly conditioned on  $\mathcal{E}_t$ . Then with probability at least  $(1 - \delta' - \sum_{i=1}^t \delta_i)$  the posterior set  $B_{1:t}$  satisfies*

$$|B_{1:t}| \geq (1 - \delta') \cdot |B_{1:t-1}| \cdot |B_t|/q^n.$$

*Proof.* Fix some  $B_{1:t-1}$  that is  $(C_{t-1}, s)$ -bounded and satisfies  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$  and consider a uniform choice of  $A_t$  and  $\mathbf{c}_t$ . We now apply [Lemma 5.19](#). Note this lemma takes four ‘‘parameters’’  $B, b, \delta$  and  $C$ . We apply the lemma with  $(B, b, \delta, C)_{\text{Lemma 5.19}} = (B_{1:t-1}, 2(t-1)b, \delta', C_{t-1})$ . Note that the parameter settings ensure  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$ ,  $s_0 \leq 2(t-1)b \leq s \leq \tau(q, k, \delta', C_{t-1})n$  and so the preconditions of [Lemma 5.19](#) are satisfied. By Part(2) of the lemma we get:

$$(1 - \delta') \leq \frac{\mathbb{E}_{x \sim \text{Unif}(B_{1:t-1})} [f(A_t, \mathbf{c}_t x)]}{\mathbb{E}_{z \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})} [f(z)]} \leq (1 + \delta') \quad (5.22)$$

for every non-negative function  $f$  over  $\mathbb{Z}_q^{(k-1)\alpha n}$ , with probability at least  $1 - \delta'$  (over a *uniform* choice of  $M_t$  and  $\mathbf{c}_t$ ). Setting  $f$  to be the indicator function of  $B_{r,t}$  (recall that  $B_{r,t}$  is the ‘‘reduced posterior set’’ from [Definition 5.7](#)) and applying [Eq. \(5.22\)](#), we have

$$\mathbb{E}_{x \sim \text{Unif}(B_{1:t-1})} [\mathbf{1}_{B_{r,t}}(A_t, \mathbf{c}_t x)] = \frac{|B_{1:t}|}{|B_{1:t-1}|},$$

and

$$\mathbb{E}_{z \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})} [\mathbf{1}_{B_{r,t}}(z)] = \frac{|B_{r,t}|}{q^{(k-1)\alpha n}} = \frac{|B_t|}{q^n}.$$

We have

$$\begin{aligned} \frac{|B_{1:t}|}{q^n} &= \frac{|B_{1:t-1}|}{q^n} \cdot \mathbb{E}_{x \sim \text{Unif}(B_{1:t-1})} [\mathbf{1}_{B_{r,t}}(A_t, \mathbf{c}_t x)] \\ &\geq (1 - \delta') \frac{|B_{1:t-1}|}{q^n} \cdot \mathbb{E}_{z \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})} [\mathbf{1}_{B_{r,t}}(z)] \\ &= (1 - \delta') \frac{|B_{1:t-1}|}{q^n} \cdot \frac{|B_t|}{q^n}. \end{aligned}$$

We conclude that for every  $B_{1:t-1}$ , with probability at least  $1 - \delta'$  over a uniform choice of  $A_t$  and  $\mathbf{c}_t$ , we have that if  $B_{1:t-1}$  is  $(C_{t-1}, s)$ -bounded and satisfies  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$ , then

$$\frac{|B_{1:t}|}{q^n} \geq (1 - \delta') \frac{|B_{1:t-1}|}{q^n} \cdot \frac{|B_t|}{q^n}.$$

Now we condition on the event  $\mathcal{E}_t$ . Doing so, alters the distribution of  $(A_t, \mathbf{c}_t)$  (since  $\mathcal{E}_t$  depends on  $A_t, \mathcal{E}_t$ ) but the total variation distance is bounded by  $\Pr[\bar{\mathcal{E}}_t] \leq \sum_{i=1}^t \delta_i$ . We thus have that for every  $B_{1:t-1}$ , with probability at least  $1 - \delta' - \sum_{i=1}^t \delta_i$  over choice of  $A_t$  and  $\mathbf{c}_t$  conditioned on  $\mathcal{E}_t$ , we have that if  $B_{1:t-1}$  is  $(C_{t-1}, s)$ -bounded and satisfies  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$

$$\frac{|B_{1:t}|}{q^n} \geq (1 - \delta') \frac{|B_{1:t-1}|}{q^n} \cdot \frac{|B_t|}{q^n}.$$

But finally note that  $\mathcal{E}_t$  implies  $B_{1:t-1}$  is  $(C_{t-1}, s)$ -bounded and satisfies  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$ , and so we simply get that with probability at least  $1 - \delta' - \sum_{i=1}^t \delta_i$  we have, over the choice of  $B_{1:t-1}, A_t$  and  $\mathbf{c}_t$  conditioned on  $\mathcal{E}_t$ ,

$$\frac{|B_{1:t}|}{q^n} \geq (1 - \delta') \frac{|B_{1:t-1}|}{q^n} \cdot \frac{|B_t|}{q^n}. \quad \square$$

To use the claim above we now analyze  $|B_t|$ . By the ‘‘posterior set is large’’ lemma (i.e., [Lemma 5.10](#)) we have  $|B_t| \geq q^{n-b}$  (again using  $s \leq b - \log_q(1/\delta')$ ). When  $B_t$  is large, then by [Lemma 5.18](#) we have  $B_t$  is  $(M_t, C_0, s)$ -reduced using  $b \leq s \leq \varepsilon_0 n$ . Furthermore if  $|B_t| \geq q^{n-b}$ , then combined with the inductive bound that  $|B_{1:t-1}| \geq q^{n-2(t-1)b}$  (implied by  $\mathcal{E}_t$ , [Claim 5.21](#) implies

$$|B_{1:t}| = |B_{1:t-1} \cap B_t| \geq (1 - \delta') \cdot |B_{1:t-1}| \cdot |B_t|/q^n \geq (1 - \delta') q^{n-(2t-2)b} q^{-b} \geq q^{n-2tb},$$

where the final inequality uses the very crude (but true) inequality  $1 - \delta' \geq \frac{1}{2} \geq q^{-b}$ .

Conditioned on  $B_t$  being large and reduced, we can finally invoke the ‘‘induction step’’ lemma (i.e., [Lemma 5.20](#)) with  $B = B_{1:t-1}$  and  $B' = B_t$  with  $C = C_{t-1}$  to get that  $B_{1:t} = B_{1:t-1} \cap B_t$  is  $(C_t, s)$ -bounded with probability at least  $1 - 4\delta'$  where we use  $C_t = C'(q, k, \delta', C_{t-1})$ . We note this application requires  $\max\{b, 2(t-1)b, s\} \leq \gamma_{t-1}n := \tau_0(q, k, \delta', C_{t-1})n$  which is ensured by our setting of parameters.

Taking the union bound over the three error events, namely (a)  $B_t$  not being large, (b)  $B_{1:t}$  not being large conditioned on  $B_t$  being large and (c)  $B_{1:t}$  not being bounded condition on being large, we get that  $\mathcal{E}_{t+1}^1$  holds with probability at least  $1 - 5\delta' - \sum_{i=1}^t \delta_i$  conditioned on  $\mathcal{E}_t$ .

Finally we turn to bounding  $\mathcal{E}_{t+1}^2$  conditioned on  $\mathcal{E}_{t+1}^1$ . Since  $|B_{1:t}| \geq q^{n-2tb}$  and  $B_{1:t}$  is  $(C_t, s)$ -bounded, we apply [Lemma 5.19](#) to analyze  $\|(A_{t+1, \mathbf{c}_{t+1}} \mathbf{x}^*) - U\|_{tvd}$ , for  $\mathbf{x}^* \sim \text{Unif}(B_{1:t})$ . The application requires  $s_0 \leq 2(t+1)b \leq s \leq \rho_{t+1}n := \tau(q, k, \delta', C_{t+1})n$  which we do have with our setting of parameters. We conclude that  $\|(A_{t+1, \mathbf{c}_{t+1}} \mathbf{x}^*) - U\|_{tvd} \leq \delta'$  with probability at least  $1 - \delta'$  for every fixing of  $A_{1:t, \mathbf{c}_{1:t}}$  and  $S_{1:t-1}^Y$  (over the choice of  $M_{t+1}$  and  $\mathbf{c}_{t+1}$ ). We thus have that  $\mathcal{E}_{t+1}^2$  holds with probability at least  $1 - \delta'$  conditioned on  $\mathcal{E}_{t+1}^1$ .

Putting the two together we get for every  $t \in [T]$  (including  $t = 1$ ), we have  $\mathcal{E}_t$  holds with probability at least  $1 - 6\delta' - \sum_{i=1}^t \delta_i \geq 1 - \delta_{t+1}$  as required for condition (ii).

This completes the proof of [Lemma 5.1](#). □

## 6 Analysis of bounded functions

In this section, we prove three important lemmas from [Section 5](#): the ‘‘posterior set’’ lemma (i.e., [Lemma 5.18](#)), the ‘‘boundedness implies uniformity’’ lemma (i.e., [Lemma 5.19](#)), and the ‘‘induction step’’ lemma (i.e., [Lemma 5.20](#)). We first establish useful structure on the Fourier coefficients of restricted sets (posterior set is a special case of restricted set) in [Section 6.1](#). Next, we prove useful properties for the Fourier analytic conditions in [Section 6.2](#). Finally, we prove the three lemmas in [Section 6.3](#), [Section 6.4](#), and [Section 6.5](#) respectively.

### 6.1 Fourier coefficients of the posterior function

Given a  $k$ -hypermatching  $M = (e_1, \dots, e_m)$  and centers  $\mathbf{c} = (c_1, \dots, c_m)$  we say that a set  $B \subseteq \mathbb{Z}_q^n$  is  $(M, \mathbf{c})$ -restricted if there exists a (‘‘reduced’’) set  $B_r \subseteq \mathbb{Z}_q^{(k-1)m}$  such that  $B = \{\mathbf{x} \in \mathbb{Z}_q^n | A_{\mathbf{c}} \mathbf{x} \in B_r\}$ , where  $A_{\mathbf{c}}$  is the  $\mathbf{c}$ -centered folded encoding of  $M$ . In this section we aim to prove that large restricted sets are bounded. Recall that given a  $k$ -hypermatching  $M = (e_1, \dots, e_m)$  on vertex set  $[n]$  with  $m = \alpha n$  edges and sequence of centers  $\mathbf{c} = (c_1, \dots, c_m)$  with  $c_i \in e_i \subseteq [n]$ , the  $\mathbf{c}$ -centered

folded representation of  $M$  was denoted  $A_{\mathbf{c}} \in \mathbb{Z}_q^{(k-1)m \times n}$ . Recall that a set  $B \subseteq \mathbb{Z}_q^n$  is said to be  $(M, \mathbf{c})$ -restricted if there exists a (“reduced”) set  $B_r \subseteq \mathbb{Z}_q^{(k-1)m}$  such that  $B = \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{\mathbf{c}}\mathbf{x} \in B_r\}$ . For our next lemma we will also need a variant of this matrix named the  $\mathbf{c}$ -centered projection induced by  $M$ , which we denote  $\tilde{A}_{\mathbf{c}} \in \mathbb{Z}_q^{(k-1)m \times n}$ , which is simply the matrix  $A_{\mathbf{c}}$  with the columns corresponding to  $c_1, \dots, c_m$  zeroed out. (In  $A_{\mathbf{c}}$  each of these columns has  $(k-1)$   $-1$ 's. See Figure 2.) With this definition in place we can now relate the Fourier coefficients of the indicator of a restricted set to its image.

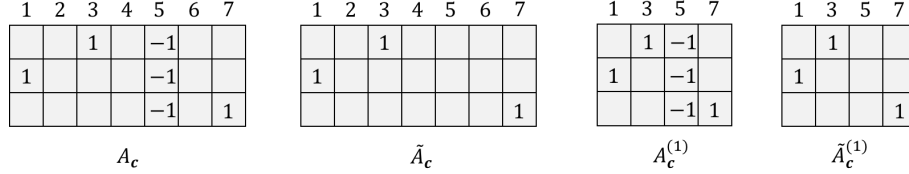


Figure 2: An example of  $A_{\mathbf{c}}, \tilde{A}_{\mathbf{c}}, A_{\mathbf{c}}^{(1)}, \tilde{A}_{\mathbf{c}}^{(1)}$  with  $m = 1, n = 7, k = 4, e_1 = \{1, 3, 5, 7\}$  and  $c_1 = \{5\}$ .

Recall that we use  $\mathbf{e}_i \in \mathbb{Z}_q^n$  to denote the indicator vector of hyperedge  $e_i$  (see Section 3).

**Lemma 6.1** (Fourier coefficients of the posterior function). *Let  $M$  be a  $k$ -hypermatching of size  $m$  and  $\mathbf{c}$  be a sequence of centers. Let  $A_{\mathbf{c}}$  be the folded representation of  $M$  and  $\tilde{A}_{\mathbf{c}}$  be the projection induced by  $M$ . Furthermore, let  $B \subseteq \mathbb{Z}_q^n$  be an  $(M, \mathbf{c})$ -restricted set with  $B_r \subseteq \mathbb{Z}_q^{(k-1)m}$  satisfying  $B = \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{\mathbf{c}}\mathbf{x} \in B_r\}$ . Let  $\mathbf{1}_B$  denote the indicator function of  $B$ . Then for every  $\mathbf{u} \in \mathbb{Z}_q^n$  we have:*

$$\widehat{\mathbf{1}}_B(\mathbf{u}) = \begin{cases} 0, & \text{if } \mathbf{u} \text{ contains a node not in } M. \\ 0, & \text{if } \exists i \in [m] \text{ such that } \langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}. \\ \widehat{\mathbf{1}}_{B_r}(\tilde{A}_{\mathbf{c}}\mathbf{u}), & \text{otherwise.} \end{cases}$$

*Proof.* From the definition of the Fourier coefficient we have  $\widehat{\mathbf{1}}_B(\mathbf{u}) = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \mathbf{1}_B(\mathbf{x}) \omega^{\mathbf{u}^\top \mathbf{x}}$  where  $\omega = e^{2\pi i/q}$  being the primitive  $q$ -th root of unity. Using the fact that  $B$  is restricted, we get

$$\widehat{\mathbf{1}}_B(\mathbf{u}) = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \mathbf{1}_B(\mathbf{x}) \cdot \omega^{\mathbf{u}^\top \mathbf{x}} = \frac{1}{q^n} \sum_{\mathbf{z} \in \mathbb{Z}_q^{(k-1)m}} \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^n \\ A_{\mathbf{c}}\mathbf{x} = \mathbf{z}}} \mathbf{1}_{B_r}(\mathbf{z}) \cdot \omega^{\mathbf{u}^\top \mathbf{x}} = \frac{1}{q^n} \sum_{\mathbf{z} \in B_r} \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^n \\ A_{\mathbf{c}}\mathbf{x} = \mathbf{z}}} \omega^{\mathbf{u}^\top \mathbf{x}}.$$

We now fix  $\mathbf{z} \in B_r$  and explore the final term  $\sum_{\mathbf{x} \in \mathbb{Z}_q^n, A_{\mathbf{c}}\mathbf{x} = \mathbf{z}} \omega^{\mathbf{u}^\top \mathbf{x}}$ . Let  $\mathbf{z} = (\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)})$  where  $\mathbf{z}^{(i)} \in \mathbb{Z}_q^{k-1}$ . Also let  $A_{\mathbf{c}}^{(1)}, \dots, A_{\mathbf{c}}^{(m)} \in \mathbb{Z}_q^{(k-1) \times n}$  denote the blocks of  $A_{\mathbf{c}}$  corresponding to the  $m$  edges. Now, think of  $\mathbb{Z}_q^n$  as a free module over  $\mathbb{Z}_q$  and consider the direct sum decomposition  $\mathbb{Z}_q^n = W^{(0)} \oplus \dots \oplus W^{(m)}$  where for  $i \in [m]$ ,  $W^{(i)}$  is the sub-module of  $\mathbb{Z}_q^n$  generated by  $e_i$ ,  $W^{(0)}$  is the sub-module generated by  $[n] - (\cup_i e_i)$ , and “ $\oplus$ ” denotes the direct sum of modules. Let us write  $\mathbf{x} = \mathbf{x}^{(0)} + \dots + \mathbf{x}^{(m)}$  where for  $i \in \{0, \dots, m\}$ ,  $\mathbf{x}^{(i)} \in W^{(i)}$ . Similarly write  $\mathbf{u} = \mathbf{u}^{(0)} + \dots + \mathbf{u}^{(m)}$ . Since  $(\mathbf{u}^{(i)})^\top \mathbf{x}^{(j)} = 0$  if  $i \neq j$  we have  $\mathbf{u}^\top \mathbf{x} = \sum_{i=0}^m (\mathbf{u}^{(i)})^\top \mathbf{x}^{(i)}$ . Note also that  $\mathbf{z} = A_{\mathbf{c}}\mathbf{x}$  if and only if  $\mathbf{z}^{(i)} = A_{\mathbf{c}}^{(i)}\mathbf{x}^{(i)}$  for every  $i \in [m]$ . Using this notation, we have

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^n \\ A_{\mathbf{c}}\mathbf{x} = \mathbf{z}}} \omega^{\mathbf{u}^\top \mathbf{x}} = \left( \sum_{\mathbf{x}^{(0)} \in W^{(0)}} \omega^{(\mathbf{u}^{(0)})^\top \mathbf{x}^{(0)}} \right) \cdot \prod_{i=1}^m \left( \sum_{\substack{\mathbf{x}^{(i)} \in W^{(i)} \\ A_{\mathbf{c}}^{(i)}\mathbf{x}^{(i)} = \mathbf{z}^{(i)}}} \omega^{(\mathbf{u}^{(i)})^\top \mathbf{x}^{(i)}} \right).$$

Now note that if  $\mathbf{u}^{(0)} = 0$  then the first term is  $|W^{(0)}| = q^{n-km}$ , else it is zero. Similarly for  $i \in [m]$ , there are exactly  $q$  vectors  $\mathbf{x}^{(i)} \in W^{(i)}$  such that  $A_{\mathbf{e}}^{(i)} \mathbf{x}^{(i)} = \mathbf{z}^{(i)}$  (which are additive shifts of each other on coordinates in  $e_i$ ). Concretely, these two solutions are of the form  $(\tilde{A}_{\mathbf{e}}^{(i)})^\top \mathbf{z}^{(i)} + a^k$  for some  $a \in \mathbb{Z}_q$ . So we have

$$\sum_{\mathbf{x}^{(i)} \in W^{(i)} : A_{\mathbf{e}}^{(i)} \mathbf{x}^{(i)} = \mathbf{z}^{(i)}} \omega^{(\mathbf{u}^{(i)})^\top \mathbf{x}^{(i)}} = \sum_{a \in \mathbb{Z}_q} \omega^{(\mathbf{u}^{(i)})^\top (\tilde{A}_{\mathbf{e}}^{(i)})^\top \mathbf{z}^{(i)} + (\mathbf{u}^{(i)})^\top a^k} = \omega^{(\mathbf{u}^{(i)})^\top (\tilde{A}_{\mathbf{e}}^{(i)})^\top \mathbf{z}^{(i)}} \sum_{a \in \mathbb{Z}_q} \omega^{a \cdot \|\mathbf{u}^{(i)}\|_1}.$$

Moreover,

$$\sum_{a \in \mathbb{Z}_q} \omega^{a \cdot \|\mathbf{u}^{(i)}\|_1} = \begin{cases} 0 & \text{if } \|\mathbf{u}^{(i)}\|_1 \not\equiv 0 \pmod{q} \\ q & \text{otherwise.} \end{cases}$$

Putting all the above together we get

$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n : A_{\mathbf{e}} \mathbf{x} = \mathbf{z}} \omega^{\mathbf{u}^\top \mathbf{x}} = \begin{cases} 0 & \text{if } \mathbf{u} \text{ contains a node not in } M. \\ 0 & \text{if } \exists i \in [m] \text{ such that } \langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}. \\ q^{n-(k-1)m} \cdot \omega^{(\tilde{A}_{\mathbf{e}} \mathbf{u})^\top \mathbf{z}} & \text{otherwise.} \end{cases}$$

Summing up over all  $\mathbf{z} \in \mathbb{Z}_q^{(k-1)m}$  and normalizing yields the lemma.  $\square$

## 6.2 Basic properties of large weakly-bounded sets

In this section, we relate weakly bounded sets to strongly bounded ones, and also show that the notion of restricted-ness of sets is independent of the choice of centers. These help us prove boundedness in the base case.

We start by stating an immediate consequence of Parseval's lemma applied to our indicator functions.

**Lemma 6.2.** *For every  $B \subseteq \mathbb{Z}_q^n$  we have  $\sum_{\mathbf{v} \in \mathbb{Z}_q^n} \widehat{\mathbf{1}}_B(\mathbf{v})^2 \leq |B|/q^n$ .*

(Lemma 6.2 follows from Lemma 2.6 by noticing that  $\sum_{\mathbf{a} \in \mathbb{Z}_q^n} \mathbf{1}_B(\mathbf{a}) = |B|$ .) Recall that the  $(C, s)$ -bounded criterion bounds the sum of Fourier coefficients with a fixed weight at most  $s$ . As we also need to bound the sum of Fourier coefficients of high weight, this can be guaranteed from Parseval's inequality as shown in the following lemma.

**Lemma 6.3.** *Suppose  $B \subseteq \mathbb{Z}_q^n$  satisfies  $|B| \geq q^{n-b}$  for some  $b \in \mathbb{N}$ . Then, for every  $\mathbf{v} \in \mathbb{Z}_q^n$  and  $b < h \leq n$ , we have*

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \leq \left( \frac{2q^2 e^2 n}{h} \right)^{h/2}.$$

*Proof.* From Lemma 6.2, we have that  $\sum_{\|\mathbf{u} + \mathbf{v}\|_0 = h} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right|^2 \leq |B|/q^n$ . Using

$$\left| \{ \mathbf{u} \in \mathbb{Z}_q^n \mid \|\mathbf{u} + \mathbf{v}\|_0 = h \} \right| \leq (q-1)^h \cdot \binom{n}{h} \leq \left( \frac{qen}{h} \right)^h$$

and the Cauchy-Schwarz inequality we get that

$$\begin{aligned}
\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| &\leq \frac{q^n}{|B|} \sqrt{(|B|/q^n) \cdot (qen/h)^h} \\
&= \sqrt{(q^n/|B|) \cdot (qen/h)^h} \\
&\leq \sqrt{q^b (qen/h)^h} && (\because |B| \geq q^{n-b}) \\
&\leq \sqrt{q^h (qen/h)^h} && (\because h > b) \\
&\leq (2q^2 e^2 n/h)^{h/2}.
\end{aligned}$$

□

Next, we note a basic monotonicity property of the notion of boundedness which will be useful in the future. Recall the function  $W_{C,s}(\cdot)$  used in the notion of *weakly-bounded* sets from [Definition 5.14](#).

**Lemma 6.4** (Monotonicity of boundedness). *The following monotonicities hold for  $W$  and  $U$ .*

1. If  $h \leq s \leq s'$  then  $W_{C,s}(h) \leq W_{C,s'}(h)$ .
2. If  $s \leq s'$  then for every  $h$ ,  $U_{C,s}(h) \leq U_{C,s'}(h)$ . Consequently, if a set  $B$  is  $(C, s)$ -strongly-bounded then it is also  $(C, s')$ -strongly-bounded.
3. If  $C > e$ , then  $W_{C,s}(h)$  and  $U_{C,s}(h)$  are monotonically increasing in  $h \in [1, s]$ .

*Proof.* The first two monotonicities are definitional, whereas the third one requires some calculations. Details are provided below.

1. The inequality holds trivially for  $h = 0$ . For  $1 \leq h \leq s \leq s'$ , we have that  $W_{C,s}(h) = (C\sqrt{sn}/h)^{h/2} \leq (C\sqrt{s'n}/h)^{h/2} = W_{C,s'}(h)$ .
2. Here we consider three possible ranges for  $h$ . For  $h \leq s \leq s'$ ,  $U_{C,s}(h) = W_{C,s}(h)$  and  $U_{C,s'}(h) = W_{C,s'}(h)$  and the inequality follows from Item (1). For  $h > s'$ , we have  $U_{C,s}(h) = \min\{W_{C,h}(h), (2q^2 e^2 n/h)^{h/2}\} = U_{C,s'}(h)$  yielding the desired inequality as an equality. For  $s < h \leq s'$ , we have  $U_{C,s}(h) = \min\{W_{C,h}(h), (2q^2 e^2 n/h)^{h/2}\} \leq W_{C,h}(h) \leq W_{C,s'}(h) = U_{C,s'}(h)$ , where the second inequality again follows from the Item (1). Thus in all cases we have  $U_{C,s}(h) \leq U_{C,s'}(h)$  and so if a set  $B$  is  $(C, s)$ -strongly-bounded then it is also  $(C, s')$ -strongly-bounded.
3. Recall that the function  $f(x) = x^{1/x}$  is decreasing in the interval  $(e, \infty)$  (since  $f'(x) = x^{1/x} \cdot \frac{1-\ln x}{x^2}$  is negative for  $x > e$ ). Note that for  $h \in [1, s]$ ,  $W_{C,s}(h) = U_{C,s}(h) = x^{\frac{C\sqrt{sn}}{2x}}$  for  $x = \frac{C\sqrt{sn}}{h}$ . Note that  $x$  is a strictly decreasing function of  $h$ . Moreover, for  $h \leq s$ , we have  $x \geq \frac{C\sqrt{sn}}{s} \geq C > e$ . Hence, it follows from monotonically decreasing property of  $f$  that  $W_{C,s}(h)$  and  $U_{C,s}(h)$  are monotonically increasing in the described interval, as desired.

□

We now show how weak boundedness of a large set in an entire regime of  $s$  implies it is strongly bounded.

**Lemma 6.5** (From weak-boundedness to strong-boundedness). *For every  $q, C$ , and  $\varepsilon_0$  there exists  $C'$  s.t. for all  $n$  and  $s \leq \varepsilon_0 n$  the following holds: If  $B \subseteq \mathbb{Z}_q^n$  with  $|B| \geq q^{n-s}$  is  $(C, s')$ -weakly-bounded for every  $s \leq s' \leq \varepsilon_0 n$  then  $B$  is  $(C', s)$ -strongly bounded. Similarly, if  $B \subseteq \mathbb{Z}_q^n$  with  $|B| \geq q^{n-s}$  is  $(C, s')$ -weakly-reduced for every  $s \leq s' \leq \varepsilon_0 n$  then  $B$  is  $(C', s)$ -strongly reduced.*

*Proof.* We prove the lemma for  $C' := \max\{C, 2q^2 e^2 / \varepsilon_0^{1/2}\}$ . We prove the reducedness condition (and the boundedness follows similarly). Fix  $B \subseteq \mathbb{Z}_q^n$  with  $|B| \geq q^{n-s}$  and  $\mathbf{v} \in \mathbb{Z}_q^n$ . Let

$$\text{wt}(h) := \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right|,$$

and let  $\tilde{W}(h) = (2q^2 e^2 n / h)^{h/2}$ . Our goal is to prove that for  $h \leq s$ ,  $\text{wt}(h) \leq U_{C', s}(h) = W_{C', s}(h)$ , and for  $h > s$  that  $\text{wt}(h) \leq \min\{W_{C', h}(h), \tilde{W}(h)\}$ . For  $h \leq s$ , by the fact that  $B$  is  $(C, s)$ -weakly-reduced, we have  $\text{wt}(h) \leq W_{C, s}(h) \leq W_{C', s}(h)$  where the second inequality follows from the definition of  $W_{C, s}$  which is monotone in  $C$ . For every  $h > s$  we have that  $\text{wt}(h) \leq \tilde{W}(h)$  by [Lemma 6.3](#) and so it suffices to prove that  $\text{wt}(h) \leq W_{C', h}(h)$  for every  $h > s$ . For  $h \leq \varepsilon_0 n$  we use that  $B$  is  $(C, s')$ -weakly-reduced for  $s' = h$  (this is ok since  $s \leq s' = h \leq \varepsilon_0 n$ ) to conclude that  $\text{wt}(h) \leq W_{C, h}(h) \leq W_{C', h}(h)$ . For  $h > \varepsilon_0 n$  we note that

$$W_{C', h}(h) = (C' \sqrt{hn} / h)^{h/2} = (C' \sqrt{n/h})^{h/2} \geq (2q^2 e^2 \sqrt{n/\varepsilon_0 h})^{h/2} \geq (2q^2 e^2 n / h)^{h/2} = \tilde{W}(h),$$

where the first inequality uses  $C' \geq (2q^2 e^2 / \varepsilon_0^{1/2})$  and the next inequality uses  $h > \varepsilon_0 n$ .

Thus in this case we have  $\text{wt}(h) \leq \tilde{W}(h) \leq W_{C', h}(h)$  as desired, concluding the proof that  $B$  is  $(C', s)$ -strongly-reduced.  $\square$

Finally we show that the notion of a set being restricted is independent of the choice of centers. Recall the definition of set being restricted from [Definition 5.11](#).

**Lemma 6.6** (Recentering). *Let  $\mathbf{c} = (c_1, \dots, c_m)$  and  $\mathbf{c}' = (c'_1, \dots, c'_m)$  be two sequences of centers for the same matching  $M$ . Then a set  $B \subseteq \mathbb{Z}_q^n$  is  $(M, \mathbf{c})$ -restricted if and only if it is  $(M, \mathbf{c}')$ -restricted.*

*Proof.* Let  $e_i^{(t)} = ((e_i^{(t)})_1, \dots, (e_i^{(t)})_k = c_t)$  (for  $t = 1, 2, \dots, m$ ) be the ordering of hyperedges corresponding to centering  $\mathbf{c}$ , and let  $e'_i{}^{(t)} = ((e'_i{}^{(t)})_1, \dots, (e'_i{}^{(t)})_k = c'_t)$ .

Given a permutation  $\pi : [k] \rightarrow [k]$ , let  $P_\pi$  be a  $(k-1) \times (k-1)$  matrix defined as follows: For  $1 \leq i, j \leq k-1$ , let

$$(P_\pi)_{i,j} = \begin{cases} 1 & \text{if } j = \pi(i), \\ -1 & \text{if } j = \pi(k), \\ 0 & \text{otherwise.} \end{cases}$$

For  $t = 1, 2, \dots, m$ , let  $\pi_t : [k] \rightarrow [k]$  be the permutation defined by  $(e'_i{}^{(t)})_j = (e_i^{(t)})_{\pi(j)}$ , and let  $\pi'_t : [k] \rightarrow [k]$  be the permutation defined by  $(e_i^{(t)})_j = (e'_i{}^{(t)})_{\pi(j)}$ . Then, it is not hard to see that  $A_{\mathbf{c}'} = Q \cdot A_{\mathbf{c}}$  and  $A_{\mathbf{c}} = Q' \cdot A_{\mathbf{c}'}$  where

$$Q = \begin{pmatrix} P_{\pi_1} & & & \\ & P_{\pi_2} & & \\ & & \ddots & \\ & & & P_{\pi_m} \end{pmatrix}, \quad Q' = \begin{pmatrix} P_{\pi'_1} & & & \\ & P_{\pi'_2} & & \\ & & \ddots & \\ & & & P_{\pi'_m} \end{pmatrix},$$

and  $QQ' = Q'Q = I$ , the  $(k-1)m \times (k-1)m$  identity matrix.

Now, suppose  $B \subseteq \mathbb{F}_2^n$  is  $(M, \mathbf{c})$ -restricted. Let  $B_r \subseteq \mathbb{Z}_q^{(k-1)m}$  be the corresponding reduced set satisfying  $B = \{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{\mathbf{c}}\mathbf{x} \in B_r\}$ . Then, let  $B'_r = \{Q\mathbf{y} \mid \mathbf{y} \in B_r\}$ .

Note that if  $\mathbf{x} \in B$ , then  $A_{\mathbf{c}'}\mathbf{x} = Q(A_{\mathbf{c}}\mathbf{x}) \in B'_r$ . Similarly, if  $A_{\mathbf{c}'}\mathbf{x} \in B'_r$ , then there is some  $\mathbf{y} \in B_r$  such that  $A_{\mathbf{c}'}\mathbf{x} = Q\mathbf{y}$ , and so,  $A_{\mathbf{c}}\mathbf{x} = Q'A_{\mathbf{c}'}\mathbf{x} = Q'Q\mathbf{y} = \mathbf{y} \in B_r$ , implying that  $\mathbf{x} \in B$ . It follows that  $B$  is  $(M, \mathbf{c}')$ -restricted with reduced set  $B'_r$ .

In an analogous fashion, it follows that if  $B$  is  $(M, \mathbf{c}')$ -restricted, then  $B$  is also  $(M, \mathbf{c})$ -restricted. This completes the proof.  $\square$

### 6.3 Proof of the ‘‘posterior set’’ lemma

In this subsection, we prove the ‘‘posterior set’’ lemma (Lemma 5.18), which shows that every posterior set  $B_t$  is  $(M_t, C, s)$ -reduced for some constant  $C$ . We include the statement again below for convenience.

**Lemma 5.18** (Posterior set). *For every  $q, k \geq 2$ , there exist constants  $\varepsilon_0 > 0$  and  $C_0 < \infty$  such that for every sufficiently large  $n$ , every  $k$ -hypermatching  $M$  on vertex set  $[n]$ , every pair of integers  $b, s$  satisfying  $0 < b \leq s \leq \varepsilon_0 \cdot n$  the following holds. If  $B \subseteq \mathbb{Z}_q^n$  satisfies (i) there exists a sequence of centers  $\mathbf{c}$  such that  $B$  is  $(M, \mathbf{c})$ -restricted, and (ii)  $|B| \geq q^{n-b}$ , then  $B$  is  $(M, C_0, s)$ -reduced.*

To see how the above lemma connects to posterior sets, think of  $B$  as  $B_t$ ,  $M$  as  $M_t$ , and  $\mathbf{c}$  as  $\mathbf{c}_t$ . Note that condition (i) of Lemma 5.18 holds by the definition of  $B_t$ . As for condition (ii), it holds when the message  $S_t$  is *typical* and we know by averaging argument that this is the case with high probability (see Lemma 5.10 for more details).

We now turn to the proof of Lemma 5.18. The overall proof follows the outline of [KK19], but we require extra care in our case, and the proof crucially depends on the ability to recenter (Lemma 6.6) and a slightly more careful probabilistic analysis.

*Proof of Lemma 5.18.* Given  $q$ , let  $\zeta_q$  be the constant from Lemma 2.13. Let  $\zeta_1 = \max\{1, \zeta_q\}$ . Given  $k$ , let  $\varepsilon_0 = \min\{1, k/(8\zeta_1)\}$ . Further let  $C_1 = \sqrt{2^{7/2}\zeta_1^{1/2}ek^{3/2}q^{2k}}$  and  $C_2 = (2^8\zeta_1e^2kq^{2k})^{1/2}$  and  $C = \max\{2, C_1 + C_2\}$ . For this choice of  $C$  and  $\varepsilon_0$  let  $C'$  be the constant given by Lemma 6.5. We prove the lemma for  $C_0 = C'$ .

Let  $M$  be a hypermatching with  $m$  edges. (Note we must have  $m \leq n/k$ .) Recall the definition of  $(M, C, s)$ -reducedness (Definition 5.17). The first two conditions of  $(M, C, s)$ -reducedness are immediate corollaries of Lemma 6.1. In the rest of the proof we focus on showing for every  $b \leq s \leq \varepsilon_0 n$  and every  $h \in \{1, \dots, s\}$  and  $\mathbf{v} \in \mathbb{Z}_q^n$ ,

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \leq W_{C,s}(h). \quad (\text{Goal of Lemma 5.18})$$

Since this holds for every  $s \in [b, \varepsilon_0 n]$ , by Lemma 6.5, we get that there is a  $C'$  such that  $B$  is  $(C', s)$ -reduced for every  $s \in [b, \varepsilon_0 n]$  and this yields the lemma given the bound above.

Fix an arbitrary  $\mathbf{v} \in \mathbb{Z}_q^n$ . For each  $h \in \{1, \dots, s\}$ , let  $S_h = S_{\mathbf{v},h} = \{\mathbf{u} : \|\mathbf{u} + \mathbf{v}\|_0 = h\}$ , i.e., the set of Fourier coefficients in the LHS of the above inequality. We prune  $S_h$  to eliminate some terms that are zero. Recall by Lemma 6.1 that  $\widehat{\mathbf{1}}_B(\mathbf{w}) = 0$  if  $\text{supp}(\mathbf{w}) \not\subseteq \text{supp}(M)$ , or if there exists  $i \in [m]$  such that  $\langle \mathbf{w}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$ . Let

$$T_{\mathbf{v},h,M} = \{\mathbf{u} \in S_{\mathbf{v},h} \mid \text{supp}(\mathbf{u}) \subseteq \text{supp}(M), \langle \mathbf{u}, \mathbf{e}_i \rangle \equiv 0 \pmod{q} \forall i \in [m]\},$$

denote the resulting set of vectors which includes all non-zero Fourier coefficients. Roughly, our approach below is to (1) give an upper bound on the size of the set  $T_{\mathbf{v},h,M}$  and (2) bound the sum of the squares of the coefficients in this set. Once we have both these bounds, we can use the Cauchy-Schwartz inequality to conclude the desired bound. Before we undertake these steps, we make some simplifications and some refinements.

**Step 0: Regular condition of  $\mathbf{v}$ .** First note that we can assume  $\text{supp}(\mathbf{v}) \subseteq \text{supp}(M)$ . If this is not the case, consider the vector  $\tilde{\mathbf{v}}$  given by  $\tilde{v}_i = v_i$  if  $i \in \text{supp}(M)$  and  $\tilde{v}_i = 0$  otherwise. Also, let  $a = |\{i \mid v_i \neq 0 \text{ and } i \notin \text{supp}(M)\}|$  be the number of nodes in the support of  $\mathbf{v}$  that are not contained in the hypermatching  $M$ . Then note that  $T_{\mathbf{v},h,M} = T_{\tilde{\mathbf{v}},h-a,M}$ . If we show that  $(q^n/|B|) \cdot \sum_{\mathbf{u} \in T_{\tilde{\mathbf{v}},h-a,M}} |\widehat{\mathbf{1}}_B(\mathbf{u})| \leq U_{C,s}(h-a)$  then, by the monotonicity of  $U_{C,s}(\cdot)$  in the interval  $[1, s]$  (see Lemma 6.4), it follows that  $(q^n/|B|) \cdot \sum_{\mathbf{u} \in T_{\mathbf{v},h,M}} |\widehat{\mathbf{1}}_B(\mathbf{u})| \leq U_{C,s}(h)$ . Thus, from now on, we assume  $\text{supp}(\mathbf{v}) \subseteq \text{supp}(M)$ .

**Step 1: A partition of  $T_{\mathbf{v},h,M}$ .** We now further refine  $T_{\mathbf{v},h,M}$ , i.e., the set of non-zero Fourier coefficients. For an integer  $\ell$ , let  $T_{\mathbf{v},h,\ell,M} = \{\mathbf{u} \in T_{\mathbf{v},h,M} \mid \#\{i \in [m] \mid e_i \cap \text{supp}(\mathbf{u} + \mathbf{v}) \neq \emptyset\} = \ell\}$  be the set  $\mathbf{u} \in T_{\mathbf{v},h,\ell,M}$ 's such that the support of  $\mathbf{u} + \mathbf{v}$  touches exactly  $\ell$  edges. Since  $\mathbf{v}, h$  and  $M$  will be fixed in the rest of this proof, we simplify the notation and refer to this set as  $T_\ell$ . Note that  $h/k \leq \ell \leq \min\{m, h\}$ . Thus, the quantity we are interested in this lemma can be upper bounded as follows.

$$\begin{aligned}
\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{v}\|_0 = h}} \frac{q^n}{|B|} |\widehat{\mathbf{1}}_B(\mathbf{u})| &= \frac{q^n}{|B|} \sum_{\mathbf{u} \in S_h} |\widehat{\mathbf{1}}_B(\mathbf{u})| \\
&= \frac{q^n}{|B|} \sum_{\mathbf{u} \in T_{\mathbf{v},h,M}} |\widehat{\mathbf{1}}_B(\mathbf{u})| \\
&= \sum_{\ell=h/k}^{\min\{m,h\}} \frac{q^n}{|B|} \sum_{\mathbf{u} \in T_\ell} |\widehat{\mathbf{1}}_B(\mathbf{u})| \\
&\leq \sum_{\ell=h/k}^{\min\{m,h\}} \frac{q^n}{|B|} \sqrt{|T_\ell| \sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2} \tag{6.7}
\end{aligned}$$

where the second equality is due to Lemma 6.1, the third equality is due to the partition, and the last inequality is by Cauchy-Schwarz inequality. (The reason why we partition  $T_{\mathbf{v},h,M}$  into  $T_\ell$ 's is that the Fourier square-mass within  $T_\ell$  and the cardinality of  $T_\ell$  can be properly upper bounded respectively.)

**Step 2: Upper bounding the squared Fourier mass within  $T_\ell$ .** To upper bound the squared Fourier mass within  $T_\ell$ , we utilize the fact that the posterior set  $B$  is independent to the choice of center  $\mathbf{c}$  (i.e., Lemma 6.6) and hypercontractivity (i.e., Lemma 2.13). We stress that in the bound we establish below it is crucial that the exponent of  $b$  is  $h - \ell$  (as opposed to the more trivial  $h$ , or  $h(k-1)/k$ ). In turn this bound is obtained by using a random center  $\mathbf{c}$  and this randomization is permitted at the analysis stage by Lemma 6.6.

**Claim 6.8.** Let  $\zeta_1 = \max\{1, \zeta_q\}$  where  $\zeta_q$  is the constant from Lemma 2.13. If  $|B| \geq q^{n-b}$  for some  $b \in \mathbb{N}$  then for every  $1 \leq \ell < h \leq b$ , we have

$$\sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2 \leq k^\ell \left( \frac{|B|}{q^n} \right)^2 \left( \frac{\zeta_1 \cdot b}{h - \ell} \right)^{h-\ell}.$$

The proof of this claim uses Lemma 6.1 to relate the Fourier coefficients of the function  $\mathbf{1}_B$  to those of  $\mathbf{1}_{B_r}$ . But note that the “reduced set”  $B_r$  depends on the choice of the center. Furthermore the weight of the Fourier coefficient in the reduced space depends on how the centers overlap with  $\text{supp}(\mathbf{u} + \mathbf{v})$ . Specifically we have that for centers  $\mathbf{c}$ ,  $\|\tilde{A}_{\mathbf{c}}(\mathbf{u} + \mathbf{v})\|_0 = \|\mathbf{u} + \mathbf{v}\|_0 - t$ , where  $t = |\{i \in [m] \mid c_i \in \mathbf{u} + \mathbf{v}\}|$  is the number of centers contained in  $\mathbf{u} + \mathbf{v}$ . Note that  $t \leq \ell$  since the number centers in  $\text{supp}(\mathbf{u} + \mathbf{v})$  can not exceed the number of edges touching this set. The crux of this proof is that we if choose the centers randomly then there is a positive probability that all centers (of the edges that touch  $\text{supp}(\mathbf{u} + \mathbf{v})$ ) are in  $\text{supp}(\mathbf{u} + \mathbf{v})$ . We argue the formal details below.

*Proof of Claim 6.8.* For a random center  $\mathbf{c}$ , let  $A_{\mathbf{c}}$  denote the  $\mathbf{c}$ -centered folded encoding of  $M$ , and let  $B_{r,\mathbf{c}} = \{A_{\mathbf{c}}\mathbf{x} \mid \mathbf{x} \in B\} \subseteq \mathbb{Z}_q^{(k-1)m}$ . For  $\mathbf{u} \in T_\ell$ , let  $I_{\mathbf{u}}(\mathbf{c}) = 1$  if  $c_i \in \text{supp}(\mathbf{u} + \mathbf{v})$  for every  $i \in [m]$  with  $e_i \cap \text{supp}(\mathbf{u} + \mathbf{v}) \neq \emptyset$  and 0 otherwise. Note that  $\Pr_{\mathbf{c}}[I_{\mathbf{u}}(\mathbf{c}) = 1] \geq k^{-\ell}$ . Now consider the following expression:

$$\begin{aligned} \mathbb{E}_{\mathbf{c}} \left[ \sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^{(k-1)m} \\ \|\mathbf{w} + \tilde{A}_{\mathbf{c}}\mathbf{v}\|_0 = h-\ell}} \widehat{\mathbf{1}}_{B_{r,\mathbf{c}}}(\mathbf{w})^2 \right] &\geq \mathbb{E}_{\mathbf{c}} \left[ \sum_{\mathbf{u} \in T_\ell} I_{\mathbf{u}}(\mathbf{c}) \cdot \widehat{\mathbf{1}}_B(\mathbf{u})^2 \right] && (\because \text{Lemma 6.1}) \\ &= \sum_{\mathbf{u} \in T_\ell} \left( \widehat{\mathbf{1}}_B(\mathbf{u})^2 \mathbb{E}_{\mathbf{c}} [I_{\mathbf{u}}(\mathbf{c})] \right) && (\because B \text{ and } T_\ell \text{ are independent to } \mathbf{c}) \\ &\geq k^{-\ell} \sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2. && (\because \Pr_{\mathbf{c}}[I_{\mathbf{u}}(\mathbf{c}) = 1] \geq k^{-\ell}) \end{aligned}$$

Rearranging the above we get

$$\sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2 \leq k^\ell \cdot \mathbb{E}_{\mathbf{c}} \left[ \sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^{(k-1)m} \\ \|\mathbf{w} + \tilde{A}_{\mathbf{c}}\mathbf{v}\|_0 = h-\ell}} \widehat{\mathbf{1}}_{B_{r,\mathbf{c}}}(\mathbf{w})^2 \right]. \quad (6.9)$$

On the other hand, since  $B$  is  $(M, \mathbf{c})$ -restricted, we have  $|B| = |\{\mathbf{x} \in \mathbb{Z}_q^n \mid A_{\mathbf{c}}\mathbf{x} \in B_{r,\mathbf{c}}\}| = |B_{r,\mathbf{c}}| \cdot q^{n-\text{rank}(A_{\mathbf{c}})}$ . As  $\text{rank}(A_{\mathbf{c}}) = (k-1)m$  and  $|B| \geq q^{n-b}$ , we have that  $|B_{r,\mathbf{c}}| = |B|/q^{n-(k-1)m} \geq q^{(k-1)m-b}$ . Hence, by Lemma 2.13 (invoked with  $n \leftarrow (k-1)m$  and  $B \leftarrow B_{r,\mathbf{c}}$ ), for every  $\mathbf{c}$  we have

$$\sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^{(k-1)m} \\ \|\mathbf{w} + \tilde{A}_{\mathbf{c}}\mathbf{v}\|_0 = h-\ell}} \widehat{\mathbf{1}}_{B_{r,\mathbf{c}}}(\mathbf{w})^2 \leq \left( \frac{|B_{r,\mathbf{c}}|}{q^{(k-1)m}} \right)^2 \left( \frac{\zeta_1 b}{h - \ell} \right)^{h-\ell},$$

where  $\zeta_1 = \max\{1, \zeta_q\}$  and  $\zeta_q$  is the constant from Lemma 2.13. Also, by  $|B| = |B_{r,\mathbf{c}}| \cdot q^{n-(k-1)m}$ , the above inequality becomes

$$\sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^{(k-1)m} \\ \|\mathbf{w} + \tilde{A}_e \cdot \mathbf{v}\|_0 = h-\ell}} \widehat{\mathbf{1}}_{B_{r,\mathbf{c}}}(\mathbf{w})^2 \leq \left(\frac{|B|}{q^n}\right)^2 \left(\frac{\zeta_1 \cdot b}{h-\ell}\right)^{h-\ell}.$$

Taking expectations over  $\mathbf{c}$  we thus get:

$$\mathbb{E}_{\mathbf{c}} \left[ \sum_{\substack{\mathbf{w} \in \mathbb{Z}_q^{(k-1)m} \\ \|\mathbf{w} + \tilde{A}_e \cdot \mathbf{v}\|_0 = h-\ell}} \widehat{\mathbf{1}}_{B_{r,\mathbf{c}}}(\mathbf{w})^2 \right] \leq \left(\frac{|B|}{q^n}\right)^2 \left(\frac{\zeta_1 \cdot b}{h-\ell}\right)^{h-\ell}. \quad (6.10)$$

Putting the inequalities Eq. (6.9) and Eq. (6.10) together we get

$$\sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2 \leq k^\ell \left(\frac{|B|}{q^n}\right)^2 \left(\frac{\zeta_1 \cdot b}{h-\ell}\right)^{h-\ell},$$

thus proving the claim.  $\square$

**Step 3: Upper bounding the cardinality of  $T_\ell$ .** Next, we turn to bounding the size of the set  $T_\ell$ . To do so we explore the structure of the vectors in  $T_\ell$ . We start with some notation. Let  $E = \{i \in [m] \mid \langle \mathbf{v}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}\}$  and  $O = \{i \in [m] \mid \langle \mathbf{v}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}\}$ . Given a vector  $\mathbf{u}$ , we define  $W_e = W_e(\mathbf{u}) = (\mathbf{u} + \mathbf{v}) \odot (\sum_{i \in E} \mathbf{e}_i)$  and  $W_o = W_o(\mathbf{u}) = (\mathbf{u} + \mathbf{v}) \odot (\sum_{i \in O} \mathbf{e}_i)$ , where  $\odot$  is used to denote the Hadamard product (entrywise product) of two vectors. Let  $\eta$  denote the number of edges touched by  $W_e$  and let  $o$  denote the number of edges touched by  $W_o$ . Note the following conditions hold when  $\mathbf{u} \in T_\ell$ .

**Claim 6.11.** *If  $\mathbf{u} \in T_\ell$ , then all the following conditions hold: (1)  $|O| \leq h$ , (2)  $\eta + o = \ell$ , and (3)  $\eta \leq h/2$ .*

*Proof.* We prove each of the individual claims below:

1. Note that  $\langle \mathbf{u} + \mathbf{v}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$  for every  $i \in O$ , since  $\langle \mathbf{u}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}$  and  $\langle \mathbf{v}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$ . Therefore,  $|\text{supp}(\mathbf{u} + \mathbf{v}) \cap e_i| \geq 1$  for every  $i \in O$ , implying that  $|O| \leq \sum_{i \in O} |\text{supp}(\mathbf{u} + \mathbf{v}) \cap e_i| \leq \|\mathbf{u} + \mathbf{v}\|_0 = h$ .
2. Since  $\mathbf{u} + \mathbf{v}$  touches  $\ell$  edges,  $\eta + o = \ell$ .
3. Note that  $\langle \mathbf{u} + \mathbf{v}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}$  for every  $i \in E$ , since  $\langle \mathbf{u}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}$  and  $\langle \mathbf{v}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}$ . Therefore, if  $i \in E$  is touched by  $W_e$  (i.e.,  $W_e \odot \mathbf{e}_i \neq \mathbf{0}$ ), then it follows that  $W_e$  touches it in at least two points, i.e.,  $|\text{supp}(W_e \odot \mathbf{e}_i)| \geq 2$  (see Figure 3). Combined with the fact that  $|\text{supp}(W_e)| \leq \|\mathbf{u} + \mathbf{v}\|_0 = h$ , we obtain  $\eta \leq h/2$ , as desired.

$\square$

Based on these restrictions on  $\mathbf{u} \in T_\ell$ , we can now get the following bound on  $|T_\ell|$ .

**Claim 6.12.** *For every  $\ell \in \{h/k, \dots, \min\{h, m\}\}$  we have:*

$$|T_\ell| \leq (4q^{2k})^h (em/\eta^*)^{\eta^*}, \quad \text{where } \eta^* := \min\{\ell, h/2\}.$$

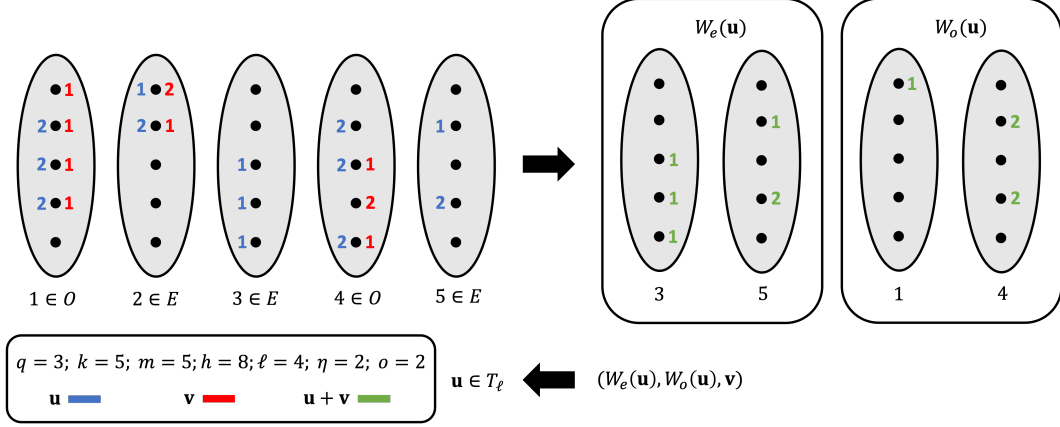


Figure 3: Upper bound the cardinality of  $T_\ell$ . In this example,  $q = 3, k = 5, m = 5$ , and  $\mathbf{v}$  is specified by integers in red. Note that  $E = \{2, 3, 5\}$  and  $O = \{1, 4\}$ . Next, we consider  $h = 8, \ell = 4$  and a  $\mathbf{u} \in T_\ell$  specified by integers in blue. Note that by definition we have  $\eta = o = 2$ . In particular, the tuple  $(W_e(\mathbf{u}), W_o(\mathbf{u}))$  is described on the right and  $\mathbf{u} + \mathbf{v}$  is specified by integers in green. It is immediate to see that  $(W_e(\mathbf{u}), W_o(\mathbf{u}), \mathbf{v})$  uniquely specifies  $\mathbf{u}$  because one can subtract  $W_e(\mathbf{u})$  and  $W_o(\mathbf{u})$  by  $\mathbf{v}$  to get the value of  $\mathbf{u}$  in those coordinates. In the rest of the coordinates,  $\mathbf{u}$  has the same values as  $\mathbf{v}$ . Moreover, observe that every hyperedge in  $W_e(\mathbf{u})$  should contain at least 2 non-zero points because both  $\mathbf{u}$  and  $\mathbf{v}$  sum up to 0 mod  $q$  within those hyperedges.

*Proof.* Recall that each  $\mathbf{u} \in T_\ell$  is uniquely specified by the pair  $(W_e, W_o)$  (see Figure 3) and it therefore suffices to count the number of distinct choices of  $(W_e, W_o)$ . First, we see that the number of possibilities for  $W_o$  is at most  $(q^k)^{|O|} \leq q^{kh}$  (since  $|O| \leq h$  by the first item of Claim 6.11). Now, having fixed  $W_o$  and  $o$ , consider the number of possibilities of  $W_e$ . We may choose  $W_e$  by picking a set  $F \subseteq E$  with  $\eta$  edges, and then picking  $|\text{supp}(W_e)| = h - |\text{supp}(W_o)|$  elements from the union of the edges in  $F$ , each of which is given a value in  $\mathbb{Z}_q \setminus \{0\}$ . Note that  $F$  can be chosen in at most  $\binom{|E|}{\eta} \leq \binom{m}{\eta}$  ways, after which  $W_e$  can be chosen in  $\leq q^{k\eta}$  ways. Finally, note that by the second and third items of Claim 6.11 we have  $\eta \leq \min\{\ell, h/2\} =: \eta^*$ . Putting these together we get:

$$|T_\ell| \leq \sum_{\eta=0}^{\eta^*} \left\{ q^{kh} \binom{m}{\eta} q^{k\eta} \right\} \leq q^{2kh} \sum_{\eta=0}^{\eta^*} \binom{m}{\eta},$$

where the second inequality uses  $\eta \leq h$ . Now we consider two cases based on whether  $\eta^* \leq m/3$  or not. If  $\eta^* > m/3$ , since  $\eta^* \leq \ell \leq m$  we have

$$\sum_{\eta=0}^{\eta^*} \binom{m}{\eta} \leq \sum_{\eta=0}^m \binom{m}{\eta} = 2^m \leq 2^{2h},$$

where the final inequality uses  $\min\{\ell, h/2\} > m/3$  to infer  $m < 3h/2 < 2h$ . Thus in this case we get

$$|T_\ell| \leq q^{2kh} 4^h = (4q^{2k})^h \leq (4q^{2k})^h (em/\eta^*)^{\eta^*},$$

where the final inequality above uses  $em \geq m \geq \eta^*$ . In the case,  $\eta^* \leq m/3$  we note that  $\binom{m}{\eta} \geq 2\binom{m}{\eta-1}$  for every  $\eta \in \{0, \dots, \eta^*\}$  and thus  $\sum_{\eta=0}^{\eta^*} \binom{m}{\eta}$  is a telescoping sum bounded by  $2\binom{m}{\eta^*}$  which in turn is bounded by  $2(em/\eta^*)^{\eta^*} \leq 2^{2h}(em/\eta^*)^{\eta^*}$ . Again the desired bound on  $|T_\ell|$  follows.  $\square$

**Step 4: Completing the proof of Lemma 5.18.** The boundedness of  $B$  now follows from some straightforward (though tedious) calculations. Continuing with the RHS of Eq. (6.7), we have:

$$\begin{aligned}
\sum_{\ell=h/k}^{\min\{h,m\}} \frac{q^n}{|B|} \sqrt{|T_\ell| \sum_{\mathbf{u} \in T_\ell} \widehat{\mathbf{1}}_B(\mathbf{u})^2} &\leq \sum_{\ell=h/k}^{\min\{h,m\}} \frac{q^n}{|B|} \sqrt{(4q^{2k})^h \cdot (em/\eta^*)^{\eta^*} \cdot k^\ell \cdot \left(\frac{|B|}{q^n}\right)^2 \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}} \\
&\quad \text{(By Claim 6.8 and Claim 6.12, and using } b \leq s\text{)} \\
&= \sum_{\ell=h/k}^{\min\{h,m\}} \sqrt{(4q^{2k})^h \cdot (em/\eta^*)^{\eta^*} \cdot k^\ell \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}} \\
&= S_1 + S_2
\end{aligned}$$

where

$$S_1 := \sum_{\ell=h/k}^{h/2} \sqrt{(4q^{2k})^h \cdot (em/\eta^*)^{\eta^*} \cdot k^\ell \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}},$$

and

$$S_2 := \sum_{\ell=h/2+1}^{\min\{h,m\}} \sqrt{(4q^{2k})^h \cdot (em/\eta^*)^{\eta^*} \cdot k^\ell \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}}.$$

Using  $\eta^* = \ell$  for the regime in  $S_1$  and  $\eta^* = h/2$  in the  $S_2$  regime we can simplify the above two sums as follows:

$$\begin{aligned}
S_1 &= \sum_{\ell=h/k}^{h/2} \sqrt{(4q^{2k})^h \cdot (em/\ell)^\ell \cdot k^\ell \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}} \\
&\leq \sum_{\ell=h/k}^{h/2} \sqrt{(4ekq^{2k})^h \cdot (m/\ell)^\ell \cdot \left(\frac{\zeta_1 s}{h-\ell}\right)^{h-\ell}} \\
&\leq \sum_{\ell=h/k}^{h/2} \sqrt{(4ekq^{2k})^h \cdot (m/\ell)^\ell \cdot \left(\frac{2\zeta_1 s}{h}\right)^{h-\ell}} \quad \text{(Using } \ell \leq h/2\text{)} \\
&= (8\zeta_1 ekq^{2k})^{h/2} \left(\frac{s}{h}\right)^{h/2} \sum_{\ell=h/k}^{h/2} \sqrt{\left(\frac{mh}{2\zeta_1 s\ell}\right)^\ell} \\
&\leq (8\zeta_1 ekq^{2k})^{h/2} \left(\frac{s}{h}\right)^{h/2} \sum_{\ell=h/k}^{h/2} \sqrt{\left(\frac{km}{2\zeta_1 s}\right)^\ell} \quad \text{(Using } \ell \geq h/k\text{)} \\
&\leq (8\zeta_1 ekq^{2k})^{h/2} \left(\frac{s}{h}\right)^{h/2} \sum_{\ell=h/k}^{h/2} \sqrt{\left(\frac{kn}{2\zeta_1 s}\right)^\ell} \quad \text{(Using } m \leq n\text{)} \\
&\leq (8\zeta_1 ekq^{2k})^{h/2} \left(\frac{s}{h}\right)^{h/2} \cdot 2 \cdot \left(\frac{kn}{2\zeta_1 s}\right)^{h/4} \quad \text{(Using } s \leq \varepsilon_0 n. \text{ See footnote}^{10}\text{.)} \\
&= 2(2^{5/2} \zeta_1^{1/2} ek^{3/2} q^{2k})^{h/2} \left(\frac{\sqrt{sn}}{h}\right)^{h/2}
\end{aligned}$$

$$\leq C_1^h \left( \frac{\sqrt{sn}}{h} \right)^{h/2},$$

for  $C_1 \geq \sqrt{27/2} \zeta_1^{1/2} e k^{3/2} q^{2k}$ . We now turn to simplifying  $S_2$ . We have

$$\begin{aligned} S_2 &= \sum_{\ell=h/2+1}^{\min\{h,m\}} \sqrt{(4q^{2k})^h \cdot (em/\eta^*)^{\eta^*} \cdot k^\ell \cdot \left( \frac{\zeta_1 s}{h-\ell} \right)^{h-\ell}} \\ &= \sum_{\ell=h/2+1}^{\min\{h,m\}} \sqrt{(4q^{2k})^h \cdot (2em/h)^{h/2} \cdot k^\ell \cdot \left( \frac{\zeta_1 s}{h-\ell} \right)^{h-\ell}} \quad (\text{Using } \eta^* = h/2 \text{ in this regime}) \\ &\leq \sum_{\ell=h/2+1}^h \sqrt{(4q^{2k})^h \cdot (2em/h)^{h/2} \cdot k^\ell \cdot \left( \frac{\zeta_1 s}{h-\ell} \right)^{h-\ell}} \\ &\leq (8ekq^{2k})^{h/2} (m/h)^{h/4} \sum_{\ell=h/2+1}^h \sqrt{\left( \frac{\zeta_1 s}{h-\ell} \right)^{h-\ell}} \\ &= (8ekq^{2k})^{h/2} (m/h)^{h/4} \sum_{\ell'=0}^{h/2-1} \sqrt{\left( \frac{\zeta_1 s}{\ell'} \right)^{\ell'}} \\ &\leq (8ekq^{2k})^{h/2} (m/h)^{h/4} \sum_{\ell'=0}^{h/2-1} \sqrt{\left( \frac{\zeta_1 s}{h/2} \right)^{\ell'}} e^{h/2} \quad (\text{Using } (x/y)^y \leq (x/z)^y \cdot e^z, \quad \forall x > 0, y \geq 1, z \geq 1)^{11} \\ &\leq (8e^2 k q^{2k})^{h/2} (m/h)^{h/4} \sum_{\ell'=0}^{h/2-1} \sqrt{\left( \frac{\zeta_1 s}{h/2} \right)^{\ell'}} \\ &\leq (8e^2 k q^{2k})^{h/2} (n/h)^{h/4} \zeta_1^{h/2} 4((2s)/h)^{h/4} \quad (\text{Using } m \leq n, \zeta_1 \geq 1 \text{ and } h \leq s) \\ &\leq C_2^h \left( \frac{\sqrt{sn}}{h} \right)^{h/2}, \end{aligned}$$

for  $C_2 \geq (2^8 \zeta_1 e^2 k q^{2k})^{1/2}$ . Combining the bounds on  $S_1$  and  $S_2$  we get

$$\sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}+\mathbf{v}\|_0=h}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| = \frac{q^n}{|B|} \sum_{\mathbf{u} \in S_h} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \leq S_1 + S_2 \leq (C_1^h + C_2^h) (\sqrt{sn}/h)^{h/2} \leq C^h (\sqrt{sn}/h)^{h/2}$$

for  $C \geq \max\{2, C_1 + C_2\}$ .

Thus, we conclude that  $B$  is  $(M, C, s)$ -weakly-reduced for every  $s \in [b, \varepsilon_0 n]$ , and so by Lemma 6.5,  $B$  is  $(M, C_0, s)$ -strongly-reduced for every  $s \in [b, \varepsilon_0 n]$ . This concludes the proof of Lemma 5.18.  $\square$

## 6.4 Proof: boundedness implies near uniformity

In this section we prove Lemma 5.19 which is used to prove condition (iii) of Lemma 5.1. We restate the lemma below for convenience.

<sup>10</sup>Since  $s \leq \varepsilon_0 n \leq kn/8\zeta_1$ , we have  $\sqrt{\frac{kn}{2\zeta_1 s}} \geq 2$  and so the sum  $\sum_{\ell=h/k}^{h/2} \sqrt{\left( \frac{kn}{2\zeta_1 s} \right)^\ell}$  telescopes to at most  $2 \left( \frac{kn}{2\zeta_1 s} \right)^{h/4}$ .

<sup>11</sup>This inequality is derived by seeing  $(x/y)^y = (x/z)^y (z/y)^y$  and  $(z/y)^y \leq e^z$  for every  $y, z \geq 1$ .

**Lemma 5.19** (Boundedness implies (closeness to) uniformity). *For every  $q, k \geq 2$  there exists  $\alpha_0 = \alpha_0(k, q)$  such that for every  $\delta \in (0, 1/2)$  and  $C < \infty$ , there exists  $\tau = \tau(q, k, \delta, C) > 0$  and  $s_0 = s_0(\delta) < \infty$  such that the following holds for every sufficiently large  $n$ :*

*Let  $B \subset \mathbb{Z}_q^n$  be a  $(C, s)$ -bounded set with  $|B| \geq q^{n-b}$ , for  $s_0 \leq b \leq s \leq \tau n$ . Let  $M$  be a random  $k$ -hypermatching of size  $m \leq \alpha_0 n$  and  $\mathbf{c}$  be a uniformly random sequence of centers for  $M$  and let  $A_{\mathbf{c}}$  denote the  $\mathbf{c}$  centered folded encoding of  $M$ . Then, with probability at least  $1 - \delta$  over the choice of  $M$  and  $\mathbf{c}$ , for every  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ , we have that*

$$1 - \delta < q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = \mathbf{z}_0] < 1 + \delta.$$

As a consequence, we also have (with probability at least  $1 - \delta$  over the choice of  $(M, \mathbf{c})$ ):

1.  $\|(A_{\mathbf{c}} \mathbf{x}) - U\|_{\text{tvd}} \leq \delta$  where  $\mathbf{x} \sim \text{Unif}(B)$  and  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)m})$ .
2. For every non-negative function  $f : \mathbb{Z}_q^{(k-1)m} \rightarrow \mathbb{R}^{\geq 0}$ ,

$$(1 - \delta) \leq \frac{\mathbb{E}_{\mathbf{x} \sim \text{Unif}(B)} [f(A_{\mathbf{c}} \mathbf{x})]}{\mathbb{E}_{\mathbf{z} \sim \text{Unif}(\mathbb{Z}_q^{(k-1)m})} [f(\mathbf{z})]} \leq (1 + \delta).$$

In the following, we denote  $m = \alpha n$  for simplicity. Let us start with defining a combinatorial quantity  $p(h, k, m, n)$  and showing an upper bound on it.

**Definition 6.13.** *Suppose  $k, m, n > 0$  are integers. We define  $p(h, k, m, n)$  to be the probability that a uniformly random  $k$ -hypermatching  $M$  on vertex set  $[n]$  with  $m$  hyperedges each of size  $k$ , the support of  $M$  contains  $[h]$  and further satisfies the condition that every hyperedge of  $M$  contains either 0 or at least two vertices from  $[h]$ .*

**Lemma 6.14** ([CGSV21a, Lemma 6.8]). *For every  $\beta_0 > 0$  and  $k$  there exists  $\alpha_0 > 0$  such that for all integers  $n, k, \alpha \in (0, \alpha_0]$ ,  $m = \alpha n$ , and  $0 \leq h \leq km$ , we have*

$$p(h, k, m, n) \leq \left( \frac{\beta_0 h}{n} \right)^{h/2}.$$

Furthermore,  $p(h, k, m, n) = 0$  if  $h > km$ .

We include a proof for convenience.

*Proof.* We prove the lemma for  $\alpha_0 = \beta_0 / (8e^3 k^5)$ . The definition of  $p(\dots)$  explores the probability that a fixed set  $H = [h]$  satisfies some conditions with respect to a random matching  $M$ . By symmetry we can instead view it as the probability that a uniformly random set  $H$  satisfies the same conditions with respect to a fixed matching  $M$  with edges  $e_1, \dots, e_m$ . (We abuse notation to also use  $M$  to denote  $\cup_{i \in [m]} e_i$ , i.e., the subset of vertices incident to the matching.)

Given a matching  $M$ , let  $\mathcal{F} = \{H \subseteq [n] \mid |H| = h, H \subseteq M, |H \cap e_i| \neq 1, \forall i \in [m]\}$ . We have  $p(h, k, m, n) = |\mathcal{F}| / \binom{n}{h}$ , and so it suffices to bound  $|\mathcal{F}|$  from above. Given  $H \in \mathcal{F}$ , let  $E(H) = \{i \in [m] \mid H \cap e_i \neq \emptyset\}$  denote the set of edges touching  $H$  and let  $\eta = |E(H)|$ . We have that  $h/k \leq \eta \leq h/2$  since every edge includes at least two vertices of  $H$ . To choose an  $H \in \mathcal{F}$  we may choose  $\eta \in [h/k, h/2]$ ,  $E \subseteq [m]$  of size  $\eta$  and then choose  $H$  of size  $h$  from the set of vertices incident to  $E$ . (There are further conditions that we will ignore to get the upper bound.) Given  $\eta$  there are  $\binom{m}{\eta}$  ways of choosing  $E$ , and given  $E$ , there are at most  $\binom{k\eta}{h}$  ways of choosing  $H$  from

the vertices touched by  $E$ . We thus get that  $|\mathcal{F}| \leq \sum_{\eta=h/k}^{h/2} \binom{m}{\eta} \binom{k\eta}{h}$ . Applying this we now get the following inequalities:

$$\begin{aligned}
p(h, k, m, n) &\leq \binom{n}{h}^{-1} \cdot \sum_{\eta=h/k}^{h/2} \binom{m}{\eta} \binom{k\eta}{h} \\
&\leq \sum_{\eta=h/k}^{h/2} \binom{m}{\eta} (ek\eta/h)^h (h/n)^h \quad (\text{Using } (a/b)^b \leq \binom{a}{b} \leq (ea/b)^b) \\
&\leq (ekh/n)^h \sum_{\eta=1}^{h/2} \binom{m}{\eta} \quad (\text{Using } \eta \leq h) \\
&\leq 2^h (ekh/n)^h (2ekm/h)^{h/2} \\
&= (8e^3 k^5 \alpha h/n)^{h/2},
\end{aligned}$$

where the last inequality uses  $\sum_{\eta=1}^{h/2} \binom{m}{\eta} \leq 2^h (2ekm/h)^{h/2}$  for every  $m$  and  $h \in [km]$ . (If  $h \leq m$  the final term is the largest and bounded by  $(2ekm/h)^{h/2}$  and so the entire sum is at most  $h(2ekm/h)^{h/2} \leq 2^h (2ekm/h)^{h/2}$ . If  $h \in (m, km]$ , then the sum is at most  $2^m$  while the RHS is at least  $2^h$  (in particular  $2ekm/h \geq 1$ .) So we have that  $p(h, k, m, n) \leq (8e^3 k^5 \alpha h/n)^{h/2} \leq (8e^3 k^5 \alpha_0 h/n)^{h/2} = (\beta_0 n/h)^{h/2}$  since  $\beta_0 = 8e^3 k^5 \alpha_0$ .  $\square$

The following lemma is an immediate corollary of [Lemma 6.14](#) and will be useful later in the proof of [Lemma 5.19](#).

**Lemma 6.15.** *For every  $k, q \geq 2$  there exists  $\alpha_0 > 0$  such that for every  $\delta \in (0, 1/2)$  and  $C < \infty$  there exists  $\tau > 0$  and  $s_0 < \infty$  such that for all integers  $n, s$  and  $m$  satisfying  $s_0 \leq s \leq \tau n$ ,  $m \leq \alpha_0 n$  we have:*

$$p(h, k, m, n) U_{C,s}(h) \leq \begin{cases} \delta^{2h} & , 1 \leq h \leq s \\ 2^{-h/2} & , s < h \leq km \\ 0 & , h > km \end{cases}.$$

Specifically,

$$\sum_{h=2}^n p(h, k, m, n) U_{C,s}(h) \leq \delta^2.$$

*Proof.* Let  $\beta_0 = \frac{1}{4q^2 e^2}$ , and let  $\alpha_0$  be as in [Lemma 6.14](#) for this choice of  $\beta_0$ . Let  $\tau = \delta^8 / (C^2 \beta_0^2)$  and  $s_0 = 4 \log_2(3/\delta)$ .

By [Lemma 6.14](#) and the definition of (strongly-)boundedness we have the following:

- If  $1 \leq h \leq s$ , then

$$p(h, k, m, n) U_{C,s}(h) \leq \left( \frac{\beta_0 h}{n} \right)^{h/2} \cdot \left( \frac{C \sqrt{sn}}{h} \right)^{h/2} = \left( \frac{\beta_0 C \sqrt{s}}{\sqrt{n}} \right)^{h/2} \leq (\beta_0 C \sqrt{\tau})^{h/2} \leq \delta^{2h},$$

where the second inequality uses  $s \leq \tau n$  and the third uses  $\beta_0 C \sqrt{\tau} \leq \delta^4$ .

- If  $s < h \leq km$ , then

$$p(h, k, m, n) U_{C,s}(h) \leq \left( \frac{\beta_0 h}{n} \right)^{h/2} \cdot \left( \frac{2q^2 e^2 n}{h} \right)^{h/2} = (\beta_0 2q^2 e^2)^{h/2} \leq 2^{-h/2},$$

where the final inequality uses  $\beta_0 2q^2 e^2 \leq 1/2$ .

- If  $h > km$ , we have  $p(h, k, m, n) = 0$  and hence  $p(h, k, m, n)U_{C,s}(h) = 0$ .

Finally, we have

$$\begin{aligned}
\sum_{h=2}^n p(h, k, m, n)U_{C,s}(h) &\leq \sum_{h=2}^s \delta^{2h} + \sum_{h=s+1}^{km} 2^{-h/2} \\
&\leq \frac{\delta^4}{1-\delta^2} + \frac{2^{-s-1/2}}{1-(1/\sqrt{2})} \\
&\leq \frac{\delta^2}{2} + \frac{2^{-s-1/2}}{1-(1/\sqrt{2})} \\
&\leq \frac{\delta^2}{2} + \frac{\delta^2}{2} \\
&= \delta^2,
\end{aligned}$$

where the second inequality uses  $\delta < 1/2$  and the third uses  $s \geq 4 \log_2(3/\delta)$ .  $\square$

Now, we are ready to prove the main lemma of this subsection.

*Proof of Lemma 5.19.* Given  $k, q \geq 2$  and  $\delta > 0$  and  $C < \infty$  let  $\alpha_0 = \alpha_0(k, q) > 0$  and  $\tau = \tau(k, q, \delta, C) > 0$  and  $s_0 = s_0(\delta)$  be as given by Lemma 6.15.

Let  $m \leq \alpha_0 n$ ,  $s_0 \leq b \leq s \leq \tau n$ , and let  $B \subset \mathbb{Z}_q^n$  be a  $(C, s)$ -bounded set with  $|B| \geq q^{n-b}$ . The goal is to prove that with probability at least  $1 - \delta$  over a uniform random choice of  $k$ -hypermatching  $M$  on  $m$  edges and a random choice of center sequence  $\mathbf{c}$  the following holds for every  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ ,

$$1 - \delta \leq q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = -\mathbf{z}_0] \leq 1 + \delta$$

(Recall that  $A_{\mathbf{c}}$  was defined in Eq. (3.3). Note that the switch from  $\mathbf{z}_0$  to  $-\mathbf{z}_0$  in the event described above does not alter the statement being proved since we are proving this for every vector  $\mathbf{z}_0$ .)

Now, for a fixed  $k$ -hypermatching  $M$  and fixed choice of centers  $\mathbf{c}$ , let us expand the marginal probability as follows. Let  $f : \mathbb{Z}_q^n \rightarrow \{0, 1\}$  be the indicator function of the set  $B$ . For a fixed  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ , let  $g = g_{A_{\mathbf{c}}, \mathbf{z}_0} : \mathbb{Z}_q^n \rightarrow \{0, 1\}$  be the function given by  $g(\mathbf{x}) = \mathbf{1}_{A_{\mathbf{c}} \mathbf{x} = \mathbf{z}_0}$ . Letting  $g = g_{A_{\mathbf{c}}, \mathbf{z}_0}$ , we have

$$\begin{aligned}
q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = -\mathbf{z}_0] &= \frac{q^{(k-1)m}}{|B|} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} f(\mathbf{x})g(-\mathbf{x}) \\
&= \frac{q^{(k-1)m}}{|B|} (f \star g)(0) \\
&= \frac{q^{(k-1)m}}{|B|} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{f \star g}(\mathbf{u}) \\
&= \frac{q^{(k-1)m+n}}{|B|} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{f}(\mathbf{u})\widehat{g}(\mathbf{u}) \quad (\text{By Lemma 2.8}) \\
&= 1 + \frac{q^{n+(k-1)m}}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \mathbf{u} \neq \mathbf{0}^n}} \widehat{f}(\mathbf{u})\widehat{g}(\mathbf{u}) \tag{6.16}
\end{aligned}$$

(Since  $q^n \widehat{f}(0) = |B|$  and  $q^n \widehat{g}(0) = q^{n-(k-1)m}$ ).

We now analyze the Fourier coefficients of  $g$  and use this to bound the right hand side above. Roughly the claim below establishes basic properties of the function  $g$  that show that  $g$  is also a somewhat reduced function (as in [Definition 5.17](#)). This, combined with the boundedness of  $B$  allows us to establish the near-uniformity of the posterior distribution.

**Claim 6.17.** *Let  $M$  be a  $k$ -hypermatching of size  $m$ ,  $\mathbf{c}$  be centers, and  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ . Let  $g(\mathbf{x}) = \mathbf{1}_{A_{\mathbf{c}}\mathbf{x}=\mathbf{z}_0}$ . For every  $\mathbf{u} \in \mathbb{Z}_q^n$ , the following conditions hold:*

1. *If  $\text{supp}(\mathbf{u}) \not\subseteq \text{supp}(M)$  then  $\widehat{g}(\mathbf{u}) = 0$ .*<sup>12</sup>
2. *If there exists  $i \in [m]$  such that  $\langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$  where  $\mathbf{e}_i$  denotes the  $i$ -th hyperedge of  $M$ , then  $\widehat{g}(\mathbf{u}) = 0$ .*
3.  *$|\widehat{g}(\mathbf{u})| \leq q^{-(k-1)m}$ .*

*Proof of Claim 6.17.* Recall that  $q^n \widehat{g}(\mathbf{u}) = \sum_{\mathbf{x}} g(\mathbf{x}) \omega^{\mathbf{u}^\top \mathbf{x}}$ .

1. If  $\text{supp}(\mathbf{u}) \not\subseteq \text{supp}(M)$ , then there exists  $i \in [n]$  such that  $u_i \neq 0$  but the  $i$ -th column of  $A_{\mathbf{c}}$  is zero. For each  $\mathbf{x} \in \mathbb{Z}_q^n$ , for every  $a \in \mathbb{Z}_q$  we have  $g(\mathbf{x}) = g(\mathbf{x} + a\boldsymbol{\delta}_i)$ , where  $\boldsymbol{\delta}_i \in \mathbb{Z}_q^n$  denotes the coordinate vector in the  $i$ -th direction (i.e.,  $\boldsymbol{\delta}_i = 0^{i-1}10^{n-i}$ ). Also, note that  $\sum_{a \in \mathbb{Z}_q} \omega^{\mathbf{u}^\top (\mathbf{x} + a\boldsymbol{\delta}_i)} = \omega^{\mathbf{u}^\top \mathbf{x}} \sum_{a \in \mathbb{Z}_q} \omega^{u_i a} = 0$ . This implies  $\widehat{g}(\mathbf{u}) = 0$ .
2. Suppose  $\langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$ . For each  $\mathbf{x} \in \mathbb{Z}_q^n$  and  $a \in \mathbb{Z}_q$ , note that  $g(\mathbf{x}) = g(\mathbf{x} + a\mathbf{e}_i)$  because  $a^k$  lies in the kernel of the folded matrix of this hyperedge. Second, since  $\langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}$ , we have  $\sum_{a \in \mathbb{Z}_q} \omega^{\mathbf{u}^\top \mathbf{x} + a\langle \mathbf{u}, \mathbf{e}_i \rangle} = \omega^{\mathbf{u}^\top \mathbf{x}} \sum_{a \in \mathbb{Z}_q} \omega^{a \langle \mathbf{u}, \mathbf{e}_i \rangle} = 0$ . This implies  $\widehat{g}(\mathbf{u}) = 0$ .
3. By definition, we have  $q^n \widehat{g}(\mathbf{u}) = \sum_{\mathbf{x}} \mathbf{1}_{A_{\mathbf{c}}\mathbf{x}=\mathbf{z}_0} \omega^{\mathbf{u}^\top \mathbf{x}}$ . Note that for fixed  $M, \mathbf{c}, \mathbf{z}_0$ , there are at most  $q^{n-(k-1)m}$   $\mathbf{x}$  such that  $g(\mathbf{x}) = 1$ . Thus, we have  $|\widehat{g}(\mathbf{u})| \leq q^{-(k-1)m}$  as desired.

□

Now, we can use [Claim 6.17](#) to further upper bound [Equation 6.16](#) as follows. Recall that  $\odot$  stands for the coordinate-wise product of vectors.

$$\frac{q^{n+(k-1)m}}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \mathbf{u} \neq 0^n}} \widehat{f}(\mathbf{u}) \widehat{g}(\mathbf{u}) \leq \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \mathbf{u} \neq 0^n \\ \mathbf{u} \text{ is matched by } M \\ \|\mathbf{u} \odot \mathbf{e}_i\|_1 \equiv 0 \pmod{q} \forall i \in [m]}} |\widehat{f}(\mathbf{u})|.$$

One key observation here is that the above bound is independent of  $\mathbf{z}_0$  and therefore holds even if we take the maximum of the left hand side over all  $\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}$ . We thus get, for every  $M$  and  $\mathbf{c}$ :

$$\max_{\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}} \left| q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}}\mathbf{x} = -\mathbf{z}_0] - 1 \right| \leq \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \mathbf{u} \neq 0^n \\ \mathbf{u} \text{ is contained in } M \\ \|\mathbf{u} \odot \mathbf{e}_i\|_1 \equiv 0 \pmod{q} \forall i \in [m]}} |\widehat{f}(\mathbf{u})|$$

<sup>12</sup>Recall that  $\text{supp}(\mathbf{u}) = \{i | u_i \neq 0\}$  and  $\text{supp}(M)$  is the subset of  $[n]$  consisting of vertices that are incident to some hyperedge in the matching  $M$ .

Finally, let us take the expectation of the above quantity over the randomness of  $M$  and  $\mathbf{c}$ .

$$\mathbb{E}_{M, \mathbf{c}} \left[ \max_{\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}} \left| q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = -\mathbf{z}_0] - 1 \right| \right] \leq \mathbb{E}_{M, \mathbf{c}} \left[ \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \mathbf{u} \neq \mathbf{0}^n \\ \mathbf{u} \text{ is contained in } M \\ \|\mathbf{u} \odot \mathbf{e}_i\|_1 \equiv 0 \pmod{q} \forall i \in [m]}} |\widehat{f}(\mathbf{u})| \right].$$

Next, we partition the summation according to the  $\ell_0$ -norm of the Fourier coefficients.

$$\leq \sum_{h=1}^n \mathbb{E}_{M, \mathbf{c}} \left[ \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h \\ \mathbf{u} \text{ is contained in } M \\ \|\mathbf{u} \odot \mathbf{e}_i\|_1 \equiv 0 \pmod{q} \forall i \in [m]}} |\widehat{f}(\mathbf{u})| \right]$$

Observe that the event  $\|\mathbf{u} \odot \mathbf{e}_i\|_1 \equiv 0 \pmod{q}$  implies that either  $\|\mathbf{u} \odot \mathbf{e}_i\|_0 = 0$  or  $\|\mathbf{u} \odot \mathbf{e}_i\|_0 \geq 2$  holds. Hence, the above summation can be replaced with a summation beginning at  $h = 2$ , and the equation becomes

$$\leq \sum_{h=2}^n \mathbb{E}_{M, \mathbf{c}} \left[ \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h \\ \mathbf{u} \text{ is contained in } M \\ \|\mathbf{u} \odot \mathbf{e}_i\|_0 = 0 \text{ or } \|\mathbf{u} \odot \mathbf{e}_i\|_0 \geq 2 \forall i \in [m]}} |\widehat{f}(\mathbf{u})| \right] \leq \sum_{h=2}^n p(h, k, m, n) \frac{q^n}{|B|} \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ \|\mathbf{u}\|_0 = h}} |\widehat{f}(\mathbf{u})|$$

When  $B$  is  $(C, s)$ -bounded, we can further upper bound the above quantity as follows.

$$\leq \sum_{h=2}^n p(h, k, m, n) \cdot U_{C, s}(h) \leq \delta^2,$$

where the last inequality is due to [Lemma 6.15](#). Thus, when  $\mathbf{x} \sim \text{Unif}(B)$  and  $U \sim \text{Unif}(\mathbb{Z}_q^{(k-1)\alpha n})$ , we have

$$\mathbb{E}_{M, \mathbf{c}} \left[ \max_{\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}} \left| q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = -\mathbf{z}_0] - 1 \right| \right] \leq \delta^2.$$

By Markov's inequality, we have

$$\max_{\mathbf{z}_0 \in \mathbb{Z}_q^{(k-1)m}} \left| q^{(k-1)m} \Pr_{\mathbf{x} \sim \text{Unif}(B)} [A_{\mathbf{c}} \mathbf{x} = -\mathbf{z}_0] - 1 \right| \leq \delta$$

with probability at least  $1 - \delta$ . This yields the main part of the lemma. The consequences follow directly from the main part (since pointwise bounds on the distance between distributions imply total variation distance as well as expectation of a non-negative weight).

This completes the proof of [Lemma 5.19](#).  $\square$

## 6.5 Proof of the “induction step” lemma

The goal of this section is to prove the “induction step” lemma. By Markov’s inequality, it suffices to prove the following lemma which is the expectation version of [Lemma 5.20](#). We first show how [Lemma 6.18](#) implies [Lemma 5.20](#) and then focus on proving the former in the rest of this subsection.

**Lemma 6.18** (Induction step in expectation). *For every  $q, k \in \mathbb{N}$  there exist  $\alpha_0 > 0$  and  $C_0 > 0$  such that for every  $C > C_0$ , there exist  $\tau_0 \in (0, 1)$  and  $C'' > 0$  such that the following holds: For every  $n, m, s, h \in \mathbb{N}$  satisfying  $m \leq \alpha_0 n$  and  $0 < s < \tau_0 n$  and  $1 \leq h \leq s$ , and every  $B \subset \mathbb{Z}_q^n$  that is  $(C, s)$ -strongly-bounded we have:*

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \mathbb{E}_M \left[ \max_{B'} \left\{ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \right\} \right] \leq W_{C'', s}(h),$$

where the expectation is taken over a uniform random  $k$ -hypermatching  $M$  on  $m$  hyperedges, and the maximum is taken over all  $B'$  that are  $(M, C_0, s)$ -reduced.

We first restate and prove [Lemma 5.20](#) using [Lemma 6.18](#).

**Lemma 5.20** (Induction step). *For every  $q, k \in \mathbb{N}$  there exist  $\alpha_0 > 0$  and  $C_0 < \infty$  such that for every  $C \geq C_0$ , and  $\delta \in (0, 1/2)$ , there exist  $\tau_0 = \tau_0(q, k, \delta, C) \in (0, 1)$  and  $C' = C'(q, k, \delta, C) > 0$  such that the following holds. For every  $n, b, b', s, m \in \mathbb{N}$ , satisfying  $m \leq \alpha_0 n$ ,  $0 < b, b', s < \tau_0 n$  and every  $(C, s)$ -bounded set  $B \subset \mathbb{Z}_q^n$  satisfying  $|B| \geq q^{n-b}$ , we have that with probability at least  $1 - 4\delta$  over a uniformly random  $k$ -hypermatching  $M$  of size  $m$  and every  $(M, C_0, s)$ -reduced set  $B' \subset \mathbb{Z}_q^n$  satisfying  $|B'| \geq q^{n-b'}$  and  $|B \cap B'| \geq (1 - \delta) \cdot |B| \cdot |B'| / q^n \geq q^{n-s}$ , we have  $B \cap B'$  is  $(C', s)$ -bounded.*

*Proof of Lemma 5.20.* Let  $\alpha_0, C_0$  be as in [Lemma 6.18](#). Given  $C$  and  $\delta$ , let  $C''$  and  $\tau_0$  be the constants given by [Lemma 6.18](#). Let  $C'$  be the constant from [Lemma 6.5](#) for  $C = C''/\delta^2$  and  $\varepsilon_0 = \tau_0$ . We prove our lemma with these choices of parameters.

For every matching  $M$ , fix a set  $B' = B'(M)$  that is  $(M, C_0, s)$ -reduced and satisfies  $|B'| \geq q^{n-b'}$  and  $|B \cap B'| \geq (1 - \delta) \cdot |B| \cdot |B'| / q^n \geq q^{n-s}$ . We prove the lemma for every such fixing. (In particular  $B'$  below is short for  $B'(M)$ .)

Fix  $s \leq \tau_0 n$ . For every  $h \in \{1, \dots, s\}$ , by the convolution theorem (see [Lemma 2.8](#)) for Fourier coefficients, we have

$$\begin{aligned} \sum_{\substack{\mathbf{v} \in \mathbb{Z}_q^n \\ \|\mathbf{v}\|_0 = h}} \frac{q^n}{|B \cap B'|} \left| \widehat{\mathbf{1}}_{B \cap B'}(\mathbf{v}) \right| &= \sum_{\substack{\mathbf{v} \in \mathbb{Z}_q^n \\ \|\mathbf{v}\|_0 = h}} \frac{q^n}{|B \cap B'|} \left| \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \widehat{\mathbf{1}}_B(\mathbf{u}) \widehat{\mathbf{1}}_{B'}(\mathbf{v} - \mathbf{u}) \right| \\ &\leq \sum_{\substack{\mathbf{v} \in \mathbb{Z}_q^n \\ \|\mathbf{v}\|_0 = h}} \frac{q^n}{|B \cap B'|} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \cdot \left| \widehat{\mathbf{1}}_{B'}(\mathbf{v} - \mathbf{u}) \right| \\ &= \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u}' + \mathbf{u}\|_0 = h}} \frac{q^n}{|B \cap B'|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \cdot \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \\ &= \frac{|B| \cdot |B'|}{q^n \cdot |B \cap B'|} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \end{aligned}$$

$$\leq \frac{1}{1-\delta} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right|,$$

where the first inequality above is from the triangle inequality and the second from the assumption in the lemma statement on the cardinality of  $B \cap B'$ .

For  $h \in [s]$ , let  $F(h)$  denote the event that the random matching  $M$  is such that

$$\frac{1}{1-\delta} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| > \frac{1}{\delta^h} \cdot W_{C'',s}(h) = W_{C''/\delta^2,s}(h).$$

Further, for  $h \in (s, \tau_0 n]$ , let  $F(h)$  denote the event that the random matching  $M$  is such that

$$\frac{1}{1-\delta} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| > \frac{1}{\delta^h} \cdot W_{C'',h}(h) = W_{C''/\delta^2,h}(h). \quad (6.19)$$

Let  $F = \cup_{h \in [\tau_0 n]} F(h)$  be the union of these events. Note that if  $F$  does not hold, then, for every  $s' \in [s, \tau_0 n]$ ,  $B \cap B'$  is  $(C''/\delta^2, s')$ -weakly-bounded, and so, by [Lemma 6.5](#),  $B \cap B'$  is  $(C', s)$ -strongly-bounded as desired. So we turn to bounding the probability of  $F$ .

For  $h \in [s]$ , an application of Markov's inequality to [Lemma 6.18](#) yields that

$$\Pr[F(h)] \leq \frac{W_{C'',s}(h)}{(1-\delta) \cdot W_{C''/\delta^2,s}(h)} = \frac{W_{C'',s}(h)}{(1-\delta) \cdot \frac{1}{\delta^h} W_{C'',s}(h)} \leq \frac{\delta^h}{1-\delta}.$$

For  $h \in (s, \tau_0 n]$ , we first note that since  $B$  is  $(C, s)$ -bounded then it is also  $(C, h)$ -bounded (by Item (2) of [Lemma 6.4](#)). Similarly we also have that  $B'$  is  $(M, C_0, h)$ -reduced. This allows us to invoke [Lemma 6.18](#) with  $s_{\text{Lemma 6.18}} = h$  and then proceed as in the case above. Specifically for this choice of  $s_{\text{Lemma 6.18}}$  we get by [Lemma 6.18](#) that the expected value of the LHS of [Eq. \(6.19\)](#) is at most  $W_{C'',h}(h)/(1-\delta)$ . Now an application of Markov's inequality yields:

$$\Pr[F(h)] \leq \frac{W_{C'',h}(h)}{(1-\delta) \cdot W_{C''/\delta^2,h}(h)} = \frac{W_{C'',h}(h)}{(1-\delta) \cdot \frac{1}{\delta^h} W_{C'',h}(h)} \leq \frac{\delta^h}{1-\delta}.$$

We thus get  $\Pr[F] \leq \sum_{h \in [\tau_0 n]} \Pr[F(h)] \leq \frac{1}{1-\delta} \sum_h \delta^h \leq 4\delta$  where the final step uses the fact that  $\delta < 1/2$ . We conclude that with probability at least  $1 - 4\delta$  over the randomness of  $M$ , the event  $F$  does not hold and  $B \cap B'$  is  $(C', s)$ -bounded.  $\square$

Now we turn to proving [Lemma 6.18](#). The proof involves three steps. In the first step we partition the inner sum over  $\mathbf{u}'$  based on a combinatorial structure that allows us to say how much the expected contribution of  $\mathbf{u}'$  would be, based on a few parameters. In the second step we give bounds on these expected contributions in different cases and analyze the probability of each case. In the final step we then combine these different bounds to prove the lemma.

**Step 1: Partitioning the inner sum via a combinatorial structure.** We start by defining the following combinatorial quantity, based on intersection properties of a random  $k$ -hypermatching.

**Definition 6.20.** Let  $n, q, k, u \in \mathbb{N}$  and  $\alpha \in (0, 1/k)$ . Let  $\mathbf{u} \in (\mathbb{Z}_q \setminus \{0\})^u \times 0^{n-u}$  be a vector that is non-zero on exactly the first  $u$  coordinates. For a  $k$ -hypermatching  $M$  of size  $m$ , let  $K_{\mathbf{u}}(M) := \{i \in [m] \mid \langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}\}$  be the set of edges with “odd intersection” (formally non-zero inner product mod  $q$ ) with  $\mathbf{u}$ . Let  $E_{\mathbf{u}}(M) := \{j \in [n] \mid u_j \neq 0, \exists i \notin K_{\mathbf{u}}(M), j \in e_i\}$  denote the set of vertices in the support of  $\mathbf{u}$  that are in “even” edges.<sup>13</sup> Finally, let  $O_{\mathbf{u}}(M) := \{j \in [n] \mid u_j \neq 0, \exists i \in K_{\mathbf{u}}(M), j \in e_i\}$  be the vertices in the support of  $\mathbf{u}$  from odd edges. For  $o, \eta, \kappa \in \mathbb{N}$ , we define

$$p_{q,\alpha}(n, u, o, \eta, \kappa) := \max_{\mathbf{u} \in (\mathbb{Z}_q \setminus \{0\})^u \times 0^{n-u}} \Pr_M[|K_{\mathbf{u}}(M)| = \kappa, |E_{\mathbf{u}}(M)| = \eta, |O_{\mathbf{u}}(M)| = o], \quad (6.21)$$

where  $M$  is a uniformly random  $k$ -hypermatching of size  $\alpha n$ . (In other words  $p_{q,\alpha}$  is the maximum probability of a vector  $\mathbf{u}$  of support size  $u$  having  $\kappa$  odd edges,  $\eta$  even vertices and  $o$  odd vertices when the matching  $M$  is drawn at random.)

Fig. 4 illustrates some of the parameters in the definition above. We remark that  $p_{q,\alpha}(\dots)$  should not be confused with the function  $p(\dots)$  defined in Definition 6.13, which is a similar combinatorial quantity but not the same.

Note that as each edge in  $K_{\mathbf{u}}(M)$  contributes at least one element to  $O_{\mathbf{u}}(M)$ , we have  $o \geq \kappa$ .

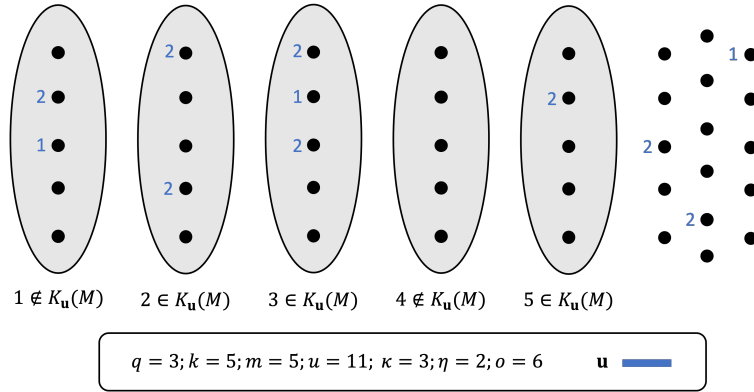


Figure 4: A graphical intuition for the parameters appeared in Definition 6.20.

We now show how to bound a certain expected value of the sum of Fourier coefficients of a fixed “level” from above in terms of the combinatorial quantity defined in Definition 6.20.

**Lemma 6.22.** Let  $n, q, k, u \in \mathbb{N}$ ,  $\alpha \in (0, 1/k)$ ,  $0 \leq s \leq n$ , and  $C > 0$ . For every  $\mathbf{u} \in \mathbb{Z}_q^n$  with  $u = |\text{supp}(\mathbf{u})|$  and  $h \in [s]$ , we have

$$\begin{aligned} & \mathbb{E}_M \left[ \max_{\substack{B' \subset \mathbb{Z}_q^n \\ B' \text{ is } (M, C, s)\text{-reduced}}} \left\{ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} |\widehat{\mathbf{1}_{B'}}(\mathbf{u}')| \right\} \right] \\ & \leq \sum_{o, \eta, \kappa} p_{q,\alpha}(n, u, o, \eta, \kappa) \cdot (h + 1) \cdot q^{k\kappa} \cdot U_{C,s}(h + o + \eta - (u + \kappa)), \end{aligned}$$

where the summation is taken over  $0 \leq o, \eta, \kappa \leq n$  satisfying conditions (1)  $u \geq \eta + o$ , (2)  $\kappa \leq o \leq k \cdot \kappa$  and (3)  $h + \eta + o - (u + \kappa) \geq 0$ .

<sup>13</sup>Informally we refer to edges as “even” (or “odd”) which would be the right terminology if  $q = 2$ . For  $q \neq 2$  these words are formalized as having zero (or non-zero) inner product with  $\mathbf{u}$ .

*Proof.* As suggested by the right hand side, we consider the various possibilities for  $o, \eta, \kappa$  and bound the left hand side conditioned on the event in Eq. (6.21), i.e.,  $|K_{\mathbf{u}}(M)| = \kappa, |E_{\mathbf{u}}(M)| = \eta$ , and  $|O_{\mathbf{u}}(M)| = o$ .

Let  $u = |\text{supp}(\mathbf{u})|$ . Consider a fixed matching  $M = \{e_1, \dots, e_m\}$  with  $m = \alpha n$  and  $|K_{\mathbf{u}}(M)| = \kappa, |E_{\mathbf{u}}(M)| = \eta$ , and  $|O_{\mathbf{u}}(M)| = o$  (see the relevant definitions in Definition 6.20). Given  $M$ , let  $A = \text{supp}(\mathbf{u}) \setminus (E_{\mathbf{u}}(M) \cup O_{\mathbf{u}}(M))$  be the set of unmatched vertices of  $\text{supp}(\mathbf{u})$ . Furthermore, let  $a = |A|$ , so that  $a = u - (\eta + o)$ . For ease of notation, we drop the dependence on  $\mathbf{u}$  and  $M$  and simply write  $E = E_{\mathbf{u}}(M)$  and  $O = O_{\mathbf{u}}(M)$ . We also abuse notation and often use  $M$  to denote the subset of  $[n]$  given by  $\cup_{i \in [m]} e_i$ . (The distinction is hopefully clear from context.)

Note that since  $|A| \geq 0$  we must have  $u - (\eta + o) \geq 0$  for such a matching to exist. This shows it suffices to restrict the summation to triples  $(o, \eta, \kappa)$  satisfying condition (1). Note further that each edge in  $K_{\mathbf{u}}(M)$  contributes at least one vertex, and at most  $k$  vertices, to  $O$  and so  $\kappa \leq o \leq k \cdot \kappa$  establishing the sufficiency of summing over triples satisfying condition (2). We now proceed to proving the rest of the lemma (and will prove sufficiency of condition (3) along the way).

Let  $B' \subset \mathbb{Z}_q^n$  be an  $(M, C, s)$ -reduced set. We give an upper bound on

$$\sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} |\widehat{\mathbf{1}}_{B'}(\mathbf{u}')|$$

in terms of the parameters  $o, \eta, \kappa$ , which will suffice to establish the lemma. We start by establishing some conditions that are necessary to get  $\widehat{\mathbf{1}}_{B'}(\mathbf{u}') \neq 0$ .

We start with some more notation: For a set  $S \subseteq [n]$ , we define the restriction of  $\mathbf{u}$  with respect to  $S$  to be the vector  $\mathbf{u}|_S \in \mathbb{Z}_q^n$  where  $(\mathbf{u}|_S)_j = \mathbf{u}_j$  if  $j \in S$ ; otherwise  $(\mathbf{u}|_S)_j = 0$ . We define the closure of  $S$  (with respect to the matching  $M$ ) to be the set  $\bar{S} = \cup_{\{i \in [m] \mid S \cap e_i \neq \emptyset\}} e_i$ , i.e.,  $\bar{S}$  takes all the vertices that are contained in edges that touch  $S$ . (We only apply the notion of the closure to sets  $S \subseteq M$ .)

**Claim 6.23.** *For every  $\mathbf{u}$  there exists a vector  $\tilde{\mathbf{u}}$  such that for every vector  $\mathbf{u}' \in \mathbb{Z}_q^n$  satisfying  $\|\mathbf{u} + \mathbf{u}'\|_0 = h$ , we have  $\widehat{\mathbf{1}}_{B'}(\mathbf{u}') \neq 0$  only if there exists  $\mathbf{z} = \mathbf{z}(\mathbf{u}') \in \mathbb{Z}_q^n$  with  $\text{supp}(\mathbf{z}) \subseteq \bar{O}$  and  $\tau = \tau(\mathbf{u}') \in [\kappa, h - a]$  such that  $\|\mathbf{u}' + (\mathbf{z} + \tilde{\mathbf{u}})\|_0 = h - a - \tau$ . In particular,  $\kappa \leq h - a$ .*

Before proving the claim we note that the claim establishes that for there to exist  $\mathbf{u}'$  such that  $\|\mathbf{u} + \mathbf{u}'\|_0 = h$  and  $\widehat{\mathbf{1}}_{B'}(\mathbf{u}') \neq 0$  we must have  $h - a - \kappa \geq 0$ . Combining with  $a = u - \eta - o$ , this allows us to restrict the summation in the RHS of Lemma 6.22 to triples  $(o, \eta, \kappa)$  satisfying  $h + \eta + o - (u + \kappa) = h - a - \kappa \geq 0$ , thereby establishing the sufficiency of condition (3).

We now prove the claim.

*Proof.* We prove the claim for  $\tilde{\mathbf{u}} := \mathbf{u}|_{[n] \setminus A}$ . Note that for every vector  $\mathbf{v}$  and set  $S \subseteq [n]$  we can write  $\mathbf{v} = \mathbf{v}|_S + \mathbf{v}|_{[n] \setminus S}$ , and we also have  $\|\mathbf{v}\|_0 = \|\mathbf{v}|_S\|_0 + \|\mathbf{v}|_{[n] \setminus S}\|_0$ . We use this to decompose  $\mathbf{u} = \mathbf{u}|_A + \tilde{\mathbf{u}}$ .

Now consider  $\mathbf{u}' \in \mathbb{Z}_q^n$  such that  $\widehat{\mathbf{1}}_{B'}(\mathbf{u}') \neq 0$  and  $\|\mathbf{u} + \mathbf{u}'\|_0 = h$ . First, as  $B'$  is  $(M, C, s)$ -reduced, by Lemma 6.1 we have  $\text{supp}(\mathbf{u}') \subseteq M$ . Again we write  $\mathbf{u}' = \mathbf{u}'|_A + \mathbf{u}'|_{[n] \setminus A}$ . Since  $A \cap M = \emptyset$  we must have  $\mathbf{u}'|_A = 0$ . Thus we get that  $\tilde{\mathbf{u}} + \mathbf{u}' = \mathbf{u}|_{[n] \setminus A} + \mathbf{u}'|_{[n] \setminus A}$  and so

$$\|\tilde{\mathbf{u}} + \mathbf{u}'\|_0 = \|\mathbf{u}|_{[n] \setminus A} + \mathbf{u}'|_{[n] \setminus A}\|_0 = \|\mathbf{u} + \mathbf{u}'\|_0 - \|\mathbf{u}|_A + \mathbf{u}'|_A\|_0 = h - a,$$

where the final equality uses  $\|\mathbf{u}|_A + \mathbf{u}'|_A\|_0 = \|\mathbf{u}|_A\|_0$  which equals  $a$  since  $A \subseteq \text{supp}(\mathbf{u})$ .

We show now that for  $\mathbf{z} := -(\tilde{\mathbf{u}} + \mathbf{u}')|_{\bar{O}}$  and  $\tau := \|\tilde{\mathbf{u}}|_{\bar{O}} + \mathbf{u}'|_{\bar{O}}\|_0$ , we have  $\|(\tilde{\mathbf{u}} + \mathbf{z}) + \mathbf{u}'\|_0 = h - a - \tau$ .

Note that the definition of  $\mathbf{z}$  is such that we have  $(\tilde{\mathbf{u}} + \mathbf{z} + \mathbf{u}')|_{\overline{O}} = 0$ . This ensures

$$\|(\tilde{\mathbf{u}} + \mathbf{z}) + \mathbf{u}'\|_0 = \|\tilde{\mathbf{u}}|_{[n]\setminus\overline{O}} + \mathbf{u}'|_{[n]\setminus\overline{O}}\|_0 = \|\tilde{\mathbf{u}} + \mathbf{u}'\|_0 - \|\tilde{\mathbf{u}}|_{\overline{O}} + \mathbf{u}'|_{\overline{O}}\|_0 = h - a - \tau.$$

Finally, we would like to bound the range of possible values for  $\tau$ . For the upper bound, we have

$$\tau := \|\tilde{\mathbf{u}}|_{\overline{O}} + \mathbf{u}'|_{\overline{O}}\|_0 \leq \|\tilde{\mathbf{u}} + \mathbf{u}'\|_0 = h - a.$$

For the lower bound we for claim that  $\|\mathbf{u}|_{e_i} + \mathbf{u}'|_{e_i}\|_0 \geq 1$  for every edge  $e_i$  with  $i \in K$ . This is so since  $\langle \mathbf{u}, e_i \rangle \neq 0$  (definition of  $K$ ) and  $\langle \mathbf{u}', e_i \rangle = 0$  (since  $\widehat{\mathbf{1}}_{B'}(\mathbf{u}') \neq 0$ ), and together they imply  $\langle \mathbf{u} + \mathbf{u}', e_i \rangle \neq 0$  which can only happen if  $(\mathbf{u} + \mathbf{u}')|_{e_i} \neq 0$ , which in turn implies  $\|\mathbf{u}|_{e_i} + \mathbf{u}'|_{e_i}\|_0 = \|(\mathbf{u} + \mathbf{u}')|_{e_i}\|_0 \geq 1$ .

From the above claim it follows that

$$\|\tilde{\mathbf{u}}|_{\overline{O}} + \mathbf{u}'|_{\overline{O}}\|_0 = \|\mathbf{u}|_{\overline{O}} + \mathbf{u}'|_{\overline{O}}\|_0 = \sum_{i \in K} \|\mathbf{u}|_{e_i} + \mathbf{u}'|_{e_i}\|_0 \geq \sum_{i \in K} 1 = \kappa.$$

This concludes the proof of the claim.  $\square$

We now return to analyzing the summation in the LHS of the lemma statement. Let  $\tilde{\mathbf{u}}$  be as given by [Claim 6.23](#). We have:

$$\begin{aligned} \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| &= \sum_{\tau = \kappa}^{h-a} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_q^n \\ \text{supp}(\mathbf{z}) \subseteq \overline{O}}} \left[ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \mathbf{z}(\mathbf{u}') = \mathbf{z}, \tau(\mathbf{u}') = \tau \\ \|\mathbf{z} + \tilde{\mathbf{u}} + \mathbf{u}'\|_0 = h - a - \tau}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \right] \\ &\quad \text{(Using [Claim 6.23](#))} \\ &\leq \sum_{\tau = \kappa}^{h-a} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_q^n \\ \text{supp}(\mathbf{z}) \subseteq \overline{O}}} \left[ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{z} + \tilde{\mathbf{u}} + \mathbf{u}'\|_0 = h - a - \tau}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \right] \\ &\leq \sum_{\tau = \kappa}^{h-a} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_q^n \\ \text{supp}(\mathbf{z}) \subseteq \overline{O}}} U_{C,s}(h - a - \tau) \\ &\quad \text{(Using the } (C, s)\text{-reducedness of } B' \text{ with respect to the vector } \mathbf{v} := \tilde{\mathbf{u}} + \mathbf{z}) \\ &\leq \sum_{\tau = \kappa}^{h-a} q^{k\kappa} \cdot U_{C,s}(h - a - \tau) \\ &\quad \text{(Using } |\overline{O}| = k\kappa \text{ to get } |\{\mathbf{z} \mid \text{supp}(\mathbf{z}) \subseteq \overline{O}\}| \leq q^{k\kappa}) \\ &\leq \sum_{\tau = \kappa}^{h-a} q^{k\kappa} \cdot U_{C,s}(h - a - \kappa) \\ &\quad \text{(Using monotonicity of } U_{C,s}(h) \text{ when } h \in [s] \text{ by [Lemma 6.4](#))} \\ &= (h - a - \kappa + 1) \cdot q^{k\kappa} \cdot U_{C,s}(h - a - \kappa) \\ &\leq (h + 1) \cdot q^{k\kappa} \cdot U_{C,s}(h + \eta + o - (u + \kappa)). \end{aligned}$$

This proves the lemma.  $\square$

**Step 2: Useful inequalities about the boundedness parameters and the combinatorial structure.** In order to quantify the upper bound in Lemma 6.22, we need to obtain an upper bound for the combinatorial quantity  $p_{q,\alpha}(n, u, o, \eta, \kappa)$ .

**Lemma 6.24.** *For every  $q, k \in \mathbb{N}$  there exists a constant  $C$  such that for every  $\alpha \in (0, 1/k]$  and every  $n, u, \kappa, o, \eta \in \mathbb{N}$  we have:*

$$p_{q,\alpha}(n, u, o, \eta, \kappa) \leq \alpha^{(o+\eta)/k} \cdot C^u \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o.$$

*Proof.* We prove the lemma for  $C = 2qe^3k$ . We start by establishing some (significant amount of) notation for the proof. The proof consists of two steps: (i) upper bounding  $p_{q,\alpha}(\dots)$  by  $\sum_{d=\eta/\kappa}^{\eta/2} N_q(u, d, o, \eta, \kappa) / \binom{n}{u}$  where  $N_q(\dots)$  is a certain well-defined combinatorial quantity and (ii) upper bounding  $N_q(\dots)$ .

**Step (i) of the proof for Lemma 6.24.** For  $\mathbf{u} = (\mathbf{u}_1, \dots, \mathbf{u}_n) \in \mathbb{Z}_q^n$ , let  $\text{supp}(\mathbf{u}) \subseteq [n]$  denote the subset of non-zero coordinates of  $\mathbf{u}$ . Further, for  $i \in \mathbb{Z}_q$ , let  $\text{supp}_i(\mathbf{u})$  denote the subset  $\{j \in [n] \mid \mathbf{u}_j = i\}$ . Now given non-negative integers  $u_1, \dots, u_{q-1}$  and  $u = u_1 + \dots + u_{q-1}$ , let  $S_{u_1, \dots, u_{q-1}} = \{\mathbf{u} \in \mathbb{Z}_q^n \mid |\text{supp}_i(\mathbf{u})| = u_i \forall i \in [q-1]\}$  and let  $S_u = \{\mathbf{u} \in \mathbb{Z}_q^n \mid |\text{supp}(\mathbf{u})| = u\}$ .

Given a vector  $\mathbf{u} \in \mathbb{Z}_q^n$  and hypermatching  $M$  containing  $m = \alpha n$  hyperedges  $e_1, \dots, e_m$  where each  $e_i$  is viewed as a subset of  $[n]$  of size  $k$ , we define four associated sets below. Let:

- $K = \{i \in [m] \mid \langle \mathbf{u}, \mathbf{e}_i \rangle \not\equiv 0 \pmod{q}\}$ ,
- $O = \{j \in \text{supp}(\mathbf{u}) \mid \exists i \in K, j \in e_i\}$ ,
- $E = \{j \in \text{supp}(\mathbf{u}) \mid \exists i \in [m] \setminus K, j \in e_i\}$ , and
- $D = \{i \in [m] : E \cap e_i \neq \emptyset\}$ .

Note that  $p_{q,\alpha}(\dots)$  bounds the maximum over  $\mathbf{u}$  with  $|\text{supp}(\mathbf{u})| = u$  of the probability, over a random hypermatching  $M$ , that  $|K| = \kappa$ ,  $|O| = o$  and  $|E| = \eta$ . By symmetry however we can fix the matching  $M$  and consider the maximum, over  $u_1, \dots, u_{q-1}$  s.t.  $u_1 + \dots + u_{q-1} = u$ , of the probability that  $|K| = \kappa$ ,  $|O| = o$  and  $|E| = \eta$ , when  $\mathbf{u}$  is chosen uniformly from  $S_{u_1, \dots, u_{q-1}}$ . In notation, we have

$$p_{q,\alpha}(n, u, o, \eta, \kappa) = \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathcal{E}(\mathbf{u}, o, \eta, \kappa)] \right\}$$

where  $\mathcal{E}(\mathbf{u}, o, \eta, \kappa)$  is the event that  $|K| = \kappa$ ,  $|O| = o$ , and  $|E| = \eta$ . Now let  $\mathcal{E}_d(\mathbf{u}, o, \eta, \kappa)$  denote the event that  $|K| = \kappa$ ,  $|O| = 0$ ,  $|E| = \eta$ , and  $|D| = d$ . Note that each hyperedge in  $D$  contributes at least two elements to  $E$  (since  $\langle \mathbf{u}, \mathbf{e}_i \rangle \equiv 0 \pmod{q}$  for  $i \in D$ ). Hence,  $d \leq \eta/2$ . Moreover, as each edge in  $D$  can contribute at most  $k$  elements to  $E$ , we also have  $d \geq \eta/k$ . Thus we get:

$$\begin{aligned} p_{q,\alpha}(n, u, o, \eta, \kappa) &= \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ \sum_{d=\eta/k}^{\eta/2} \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathcal{E}_d(\mathbf{u}, o, \eta, \kappa)] \right\} \\ &\leq \sum_{d=\eta/k}^{\eta/2} \left( \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathcal{E}_d(\mathbf{u}, o, \eta, \kappa)] \right\} \right). \end{aligned}$$

Define  $T^+((u_1, \dots, u_{q-1}), d, o, \eta, \kappa)$  to be the set  $\{\mathbf{u}_0 \in S_{u_1, \dots, u_{q-1}} \mid |K| = \kappa, |O| = o, |E| = \eta, |D| = d\}$ , let  $T_q(u, d, o, \eta, \kappa) = \cup_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} T^+((u_1, \dots, u_{q-1}), d, o, \eta, \kappa)$ . Intuitively,  $T_q$  is the set that contains all the possible  $\mathbf{u}_0$  in the event  $\mathcal{E}_d$  while  $T^+$  forms a partition for  $T_q$ . For every  $u_1, \dots, u_{q-1}$  we have

$$\Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathcal{E}_d(\mathbf{u}, o, \eta, \kappa)] = \sum_{\mathbf{u}_0 \in T^+((u_1, \dots, u_{q-1}), d, o, \eta, \kappa)} \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathbf{u} = \mathbf{u}_0].$$

The final probability above  $\Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathbf{u} = \mathbf{u}_0]$  is upper bounded by  $1/\binom{n}{u}$ . ( $\mathbf{u}$  is chosen by picking disjoint sets  $U_1, \dots, U_{q-1}$  uniformly subject to  $|U_i| = u_i$ . The event  $\mathbf{u} = \mathbf{u}_0$  holds iff  $U_i = \text{supp}_i(\mathbf{u}_0)$  which in turn happens only if  $\cup_i U_i = \text{supp}(\mathbf{u}_0)$  which in turn happens with probability  $1/\binom{n}{u}$ .) Finally let  $N_q(u, d, o, \eta, \kappa) = |T_q(u, d, o, \eta, \kappa)|$ . We thus have

$$\begin{aligned} p_{q,\alpha}(n, u, o, \eta, \kappa) &\leq \sum_{d=\eta/k}^{\eta/2} \left( \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathcal{E}_d(\mathbf{u}, o, \eta, \kappa)] \right\} \right) \\ &\leq \sum_{d=\eta/k}^{\eta/2} \left( \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ \sum_{\mathbf{u}_0 \in T^+((u_1, \dots, u_{q-1}), d, o, \eta, \kappa)} \Pr_{\mathbf{u} \in S_{u_1, \dots, u_{q-1}}} [\mathbf{u} = \mathbf{u}_0] \right\} \right) \\ &\leq \sum_{d=\eta/k}^{\eta/2} \left( \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ |T^+((u_1, \dots, u_{q-1}), d, o, \eta, \kappa)| \cdot \frac{1}{\binom{n}{u}} \right\} \right) \\ &\leq \sum_{d=\eta/k}^{\eta/2} \left( \max_{\{u_1, \dots, u_{q-1} \mid u_1 + \dots + u_{q-1} = u\}} \left\{ N_q(u, d, o, \eta, \kappa) \cdot \frac{1}{\binom{n}{u}} \right\} \right) \\ &= \sum_{d=\eta/k}^{\eta/2} \frac{N_q(u, d, o, \eta, \kappa)}{\binom{n}{u}}. \end{aligned} \tag{6.25}$$

Thus to upper bound  $p_{q,\alpha}(\dots)$  it suffices to upper bound  $N_q(\dots)$ .

**Step (ii) of the proof for Lemma 6.24.** A vector  $\mathbf{u} \in T_q(u, d, o, \eta, \kappa)$  can be specified by specifying the sets  $O, E, \text{supp}(\mathbf{u}) - (O \cup E)$ , and then by specifying  $\mathbf{u}|_{\text{supp}(\mathbf{u})}$  i.e., the restriction of  $\mathbf{u}$  to  $\text{supp}(\mathbf{u})$ . There are  $(q-1)^u$  choices of  $\mathbf{u}|_{\text{supp}(\mathbf{u})}$ . So we turn to counting the number of possible  $O$ 's and  $E$ 's.  $O$  may be specified by first specifying  $K$  and then selecting  $O$  from  $\cup_{i \in K} e_i$ . (There are further restrictions on the choices of  $O$  which we will ignore to get an upper bound.) There are  $\binom{m}{\kappa}$  choices of  $K$  and at most  $\binom{k\kappa}{o}$  choices of  $O$  given  $K$ . Similarly for  $E$  we have at most  $\binom{m}{d}$  choices of  $D$  and then at most  $\binom{kd}{\eta}$  choices of  $E$  given  $D$ . Finally, there are at most  $\binom{n-km}{u-o-\eta}$  choices of  $\text{supp}(\mathbf{u}) \setminus (O \cup E)$ , since they must be a set of  $u - o - \eta$  vertices outside the  $m$  edges of our hypermatching. Putting all this together we get the following upper bound on  $N_q(\dots)$ :

$$N_q(u, d, o, \eta, \kappa) \leq \binom{\alpha n}{\kappa} \binom{\alpha n}{d} \binom{k\kappa}{o} \binom{kd}{\eta} \binom{n(1-\alpha k)}{u-o-\eta} (q-1)^u.$$

Using the bounds  $\left(\frac{a}{b}\right)^b \leq \binom{a}{b} \leq \left(\frac{ea}{b}\right)^b$ , we have that

$$\frac{N_q(u, d, o, \eta, \kappa)}{\binom{n}{u}} \leq \left(\frac{e\alpha n}{\kappa}\right)^\kappa \left(\frac{e\alpha n}{d}\right)^d \left(\frac{ek\kappa}{o}\right)^o \left(\frac{ekd}{\eta}\right)^\eta \frac{(n(1-\alpha k))^{u-o-\eta}}{(u-o-\eta)!} (q-1)^u \cdot \left(\frac{u}{n}\right)^u$$

$$\leq n^{\kappa+d-\eta-o} \kappa^{-\kappa} d^{-d} \frac{u^u}{(u-o-\eta)!} \left( \alpha^{\kappa+d} e^{\kappa+d+o+\eta} k^{o+\eta} (q-1)^u \left(\frac{\kappa}{o}\right)^o \left(\frac{d}{\eta}\right)^\eta (1-k\alpha)^{u-o-\eta} \right).$$

Recall from [Lemma 6.22](#) and step (i) of the proof that  $\kappa \leq o$ ,  $2d \leq \eta$ , and  $o + \eta \leq u$ . Hence, we have that  $0 \leq \kappa/o, d/\eta \leq 1$  and  $e^{\kappa+d+o+\eta} k^{o+\eta} (q-1)^u \leq e^{2u} \cdot ((q-1)k)^u \leq (qe^2k)^u$ . Moreover,

$$\frac{u^{u-o-\eta}}{(u-o-\eta)!} \leq e^u.$$

Therefore, letting  $C_k = qe^3k$ , we have

$$\frac{N_q(u, d, o, \eta, \kappa)}{\binom{n}{u}} \leq C_k^u \alpha^{\kappa+d} \cdot n^{\kappa+d-\eta-o} \kappa^{-\kappa} d^{-d} u^{o+\eta} = \left(\frac{\alpha n}{d}\right)^d \cdot C_k^u \alpha^\kappa \cdot n^{\kappa-\eta-o} \kappa^{-\kappa} u^{o+\eta}.$$

Hence, by [\(6.25\)](#), we have that for  $C = 2C_k = 2qe^3k$ ,

$$\begin{aligned} p_{q,\alpha}(n, u, o, \eta, \kappa) &\leq C_k^u \alpha^\kappa \cdot n^{\kappa-\eta-o} \kappa^{-\kappa} u^{o+\eta} \sum_{d=\eta/k}^{\eta/2} \left(\frac{\alpha n}{d}\right)^d \\ &\leq C_k^u \alpha^{\kappa+\frac{\eta}{k}} \cdot n^{\kappa-\eta-o} \kappa^{-\kappa} u^{o+\eta} \sum_{d=\eta/k}^{\eta/2} \left(\frac{n}{d}\right)^d \\ &\leq C_k^u \alpha^{\frac{\eta+o}{k}} \cdot n^{\kappa-\eta-o} \kappa^{-\kappa} u^{o+\eta} \cdot \frac{\eta}{2} \left(\frac{2n}{\eta}\right)^{\eta/2} \quad (\text{Using } o \leq k \cdot \kappa \text{ from } \a href="#">\text{Lemma 6.22}) \\ &\leq \alpha^{\frac{\eta+o}{k}} \cdot C^u \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o, \end{aligned}$$

where the second-to-last inequality follows from the fact that  $n/d \geq e$  and  $x^{1/x}$  is a decreasing function of  $x$  on  $x \in (e, \infty)$ . This completes the proof of [Lemma 6.24](#).  $\square$

Finally, we prove an additional inequality about the boundedness parameters. This will simplify the final proof of [Lemma 6.18](#).

**Lemma 6.26.** *For every  $q, k \in \mathbb{N}$ , there exists  $\alpha_0 \in (0, 1/k)$  so that the following holds. For every  $C_1, C_2 > 0$  there exists  $\varepsilon_0 > 0$  and  $C_3 > 0$  such that for every  $\alpha \in (0, \alpha_0)$ ,  $\varepsilon \in (0, \varepsilon_0)$  and  $s, n, u, h, \eta, o, \kappa \in \mathbb{N}$  with  $s = \varepsilon n \leq \varepsilon_0 n$  and  $h \in [s]$  and  $u \in [n]$ , we have*

$$U_{C_1, s}(u) \cdot p_{q,\alpha}(n, u, o, \eta, \kappa) \cdot h \cdot q^{k\kappa} \cdot U_{C_2, s}(h + \eta + o - (u + \kappa)) \leq 4^{-u-2} W_{C_3, s}(h),$$

for every  $0 \leq o, \eta, \kappa \leq n$  satisfying (1)  $u \geq \eta + o$ , (2)  $\kappa \leq o \leq k \cdot \kappa$  and (3)  $h + \eta + o - (u + \kappa) \geq 0$ .

*Proof.* Given  $q$  and  $k$ , let  $C$  be the constant from [Lemma 6.24](#). Let  $C_0 = \sqrt{2} \cdot 4e \cdot q \cdot C \cdot q^k$ , and let  $\alpha_0 = 1/(e^2 C_0)^k$ . Now given  $C_1, C_2$ , let  $C_4 = 4 \cdot \sqrt{C_1} \cdot C \cdot q^k$ ,  $C_5 = \max\{1, 2\sqrt{C_2}, 2C_2\}$  and  $C_6 = eC_5$  (where  $e$  is the base of the natural logarithm). Now let  $\varepsilon_0 = \min\left\{\frac{1}{(e^2 C_4)^4}, \frac{1}{(2e^2 C_4)^4}, (e^{-2}/C_4)^{16}\right\}$  and  $C_3 = \max\{(16e^3 C_4 C_6)^2, (16C_6/\varepsilon_0^{1/4})^2, (32C_6/\alpha_0^{1/k})^2, 256C_6^2, (16C_6/\alpha_0^{1/k})^2\}$ . We prove the lemma for this choice of  $\alpha_0$ ,  $\varepsilon_0$  and  $C_3$ . Note in particular that this choice of  $\alpha_0$  depends only on  $q$  and  $k$  but not on  $C_1$  and  $C_2$  (as required).

Let  $h' = h + \eta + o - (u + \kappa)$ . By the conditions (1) and (3) in the lemma statement we have  $0 \leq h' \leq h$ .

We divide the analysis into five cases depending on the choice of  $u$ . (The cases differ first because  $U_{C_1, s}(u)$  differs in behavior depending on whether  $u \leq s$  or not. Further differences arise in the analysis depending on the relationship between  $u$  and  $h$ , as also how close  $u$  is to  $s$ .) The five cases are: (1)  $1 \leq u \leq h$ , (2)  $h < u \leq s$ , (3)  $s < u \leq 16s$ , (4)  $16s < u \leq \sqrt{\varepsilon}n$ , and (5)  $\sqrt{\varepsilon}n < u \leq n$ .

**Case 1:  $1 \leq u \leq h$ :** Expanding the definition of  $U_{C_1,s}(u)$ ,  $U_{C_2,s}(h')$ ,  $W_{C_3,s}(h)$  and invoking the upper bound on  $p_{q,\alpha}(n, u, o, \eta, \kappa)$  from [Lemma 6.24](#), we have that it suffices to prove that:

$$\begin{aligned} & \left( C_1^{u/2} ((sn)/u^2)^{u/4} \right) \left( \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \right) \left( C_2^{h'/2} (sn/h'^2)^{h'/4} \right) \cdot h \cdot q^{k\kappa} \\ & \leq 4^{-u-2} \cdot C_3^{h/2} \cdot (sn/h^2)^{h/4} = 4^{-u-2} \cdot U_{C_3,s}(h), \end{aligned} \quad (6.27)$$

We multiply the LHS above by  $4^{u+2}(h^2/sn)^{h/4}$  and show it is upper bounded by  $C_3^{h/2}$ :

$$\begin{aligned} L_1 & := 16(16C_1)^{u/2} (sn/u^2)^{u/4} \cdot \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\ & \leq 16C_4^u C_5^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h'^2)^{h'/4} \cdot (h^2/(sn))^{h/4} \\ & \quad \text{(Using } \alpha \leq \alpha_0 \leq 1, h' \leq h, h \leq 2^h, \kappa \leq o \leq u, C_4 \geq 4\sqrt{C_1} \cdot C \cdot q^k, C_5 \geq 2\sqrt{C_2}\text{)} \\ & \leq 16C_4^u C_6^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(h-h')/4} \\ & \quad \text{(Using } (h/h')^{h'/2} \leq e^h \text{ and } C_6 \geq eC_5\text{)} \\ & = 16C_4^u C_6^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(u+\kappa-(\eta+o))/4} \\ & = 16C_4^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^3 / (s\kappa^4))^{\kappa/4} \cdot (su^4 / (n\eta^2 h^2))^{\eta/4} \cdot (su^4 / n^3 h^2)^{o/4} \\ & = 16C_4^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\varepsilon\kappa^4))^{\kappa/4} \cdot (\varepsilon u^4 / (\eta^2 h^2))^{\eta/4} \cdot (\varepsilon u^4 / (n^2 h^2))^{o/4} \\ & =: S_1. \end{aligned}$$

Thus far we have not used  $u \leq h$ . (We have only used  $u \leq s$  and this was to establish our goal as [Eq. \(6.27\)](#).) We now use  $u \leq h$  to analyze  $S_1$ .

$$\begin{aligned} S_1 & = 16C_4^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\varepsilon\kappa^4))^{\kappa/4} \cdot (\varepsilon u^4 / (\eta^2 h^2))^{\eta/4} \cdot (\varepsilon u^4 / (n^2 h^2))^{o/4} \\ & = 16C_4^u C_6^h \cdot \varepsilon^{-(\kappa+\eta+o)/4} \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / \kappa^4)^{\kappa/4} \cdot (u^4 / (\eta^2 h^2))^{\eta/4} \cdot (u^4 / (n^2 h^2))^{o/4} \\ & \quad \text{(Collecting } \varepsilon \text{ terms)} \\ & \leq 16C_4^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\kappa^4))^{\kappa/4} \cdot (u^4 / (\eta^2 h^2))^{\eta/4} \cdot (u^4 / (n^2 h^2))^{o/4} \\ & \quad \text{(Using } \eta \geq 0, o \geq \kappa \text{ and } \varepsilon \leq 1\text{)} \\ & \leq 16(e^2 C_4)^u C_6^h \cdot (h/u)^{u/2} \cdot (hn/(u^2))^{\kappa/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{o/2} \\ & \quad \text{(Using } (u/\kappa)^\kappa \leq e^u \text{ and } (u/\eta)^\eta \leq e^u\text{)} \\ & = 16(e^2 C_4)^u C_6^h \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{(o-\kappa)/2} \\ & \leq 16(e^2 C_4)^u C_6^h \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} \cdot (u/h)^{(o-\kappa)/2} \\ & \quad \text{(Using } u \leq n \text{ and } o \geq \kappa\text{)} \\ & = 16(e^2 C_4)^u C_6^h \cdot (h/u)^{(u-\eta-o+\kappa)/2} \\ & \leq 16(e^2 C_4 C_6)^h \cdot (h/u)^{(u-\eta-o+\kappa)/2} \quad \text{(Using } u \leq h \text{ and } e^2 C_4 \geq C_4 \geq 1\text{)} \\ & \leq 16(e^2 C_4 C_6)^h \cdot (h/u)^{u/2} \\ & \quad \text{(Using } h \geq u \text{ and } u \geq u - o + \kappa - \eta \text{ since } o \geq \kappa \text{ and } \eta \geq 0\text{)} \\ & \leq 16(e^2 C_4 C_6)^h \cdot e^h \\ & \quad \text{(Using } (h/u)^{u/2} \leq e^{h/2} \leq e^h\text{)} \\ & \leq 16\left(\frac{1}{256} C_3\right)^{h/2} \quad \text{(Using } C_3 \geq (16e^3 C_4 C_6)^2\text{)} \\ & \leq C_3^{h/2} \quad \text{(Using } h \geq 1\text{)}. \end{aligned}$$

This yields [Eq. \(6.27\)](#) in the range  $u \in [h]$ .

**Case 2:**  $h < u \leq s$ : Here again our goal is to prove Eq. (6.27) and we still have  $L_1 \leq S_1$ . We proceed as follows:

$$\begin{aligned}
S_1 &= 16C_4^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\varepsilon \kappa^4))^{\kappa/4} \cdot (\varepsilon u^4 / (\eta^2 h^2))^{\eta/4} \cdot (\varepsilon u^4 / (n^2 h^2))^{o/4} \\
&\leq 16C_4^u C_6^h \varepsilon^{(u-h)/4} \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\kappa^4))^{\kappa/4} \cdot (u^4 / (\eta^2 h^2))^{\eta/4} \cdot (u^4 / (n^2 h^2))^{o/4} \\
&\quad \text{(Collecting } \varepsilon \text{ terms and using } \eta + o - \kappa \geq u - h) \\
&\leq 16C_4^u C_6^h \varepsilon_0^{(u-h)/4} \cdot (h^2/u^2)^{u/4} \cdot (h^2 n^2 / (\kappa^4))^{\kappa/4} \cdot (u^4 / (\eta^2 h^2))^{\eta/4} \cdot (u^4 / (n^2 h^2))^{o/4} \\
&\quad \text{(Using } \varepsilon \leq \varepsilon_0 \text{ and } h \leq u) \\
&\leq 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \cdot (h/u)^{u/2} \cdot (hn/(u^2))^{\kappa/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{o/2} \\
&\quad \text{(Using } (u/\kappa)^\kappa \leq e^u \text{ and } (u/\eta)^\eta \leq e^u) \\
&= 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{(o-\kappa)/2} \\
&\leq 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} \cdot (u/h)^{(o-\kappa)/2} \\
&\quad \text{(Using } u \leq n \text{ and } o \geq \kappa) \\
&= 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \cdot (h/u)^{(u-\eta-o+\kappa)/2} \\
&\leq 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \quad \text{(Since } h \leq u \text{ and } u - \eta - o + \kappa \geq u - \eta - o \geq 0) \\
&\leq 16(C_6 / \varepsilon_0^{1/4})^h \quad \text{(Using } \varepsilon_0 \leq \frac{1}{(e^2 C_4)^4}) \\
&\leq C_3^{h/2} \quad \text{(Using } C_3 \geq (16C_6 / \varepsilon_0^{1/4})^2, h \geq 1).
\end{aligned}$$

This concludes Eq. (6.27) in Case 2.

**Case 3:**  $s < u \leq 16s$ : The form for  $U_{C_1,s}(u)$  now changes and forces a change in our goal. Using  $U_{C_1,s}(u) \leq C_1^{u/2} (n/u)^{u/4}$  our new goal becomes:

$$\begin{aligned}
&\left( C_1^{u/2} (n/u)^{u/4} \right) \left( \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \right) \left( C_2^{h'/2} (sn/h'^2)^{h'/4} \right) \cdot h \cdot q^{k\kappa} \\
&\leq 4^{-u-2} \cdot C_3^{h/2} \cdot (sn/h^2)^{h/4} = 4^{-u-2} \cdot U_{C_3,s}(h), \tag{6.28}
\end{aligned}$$

Again multiplying the LHS by  $4^{u+2} (h^2/sn)^{h/4}$  we get the quantity  $L_3$  below which we show to be upper bounded by  $C_3^{h/2}$ . We have:

$$\begin{aligned}
L_3 &:= 16(16C_1)^{u/2} (n/u)^{u/4} \cdot \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\
&= (u/s)^{u/4} 16(16C_1)^{u/2} (sn/u^2)^{u/4} \cdot \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\
&= (u/s)^{u/4} L_1 \\
&\leq 16^{u/4} L_1
\end{aligned}$$

We now use the fact that the inequality  $L_1 \leq S_1$  in Case 1, did not use  $u \leq s$ . We thus conclude  $L_3 \leq 16^{u/4} L_1 \leq 16^{u/4} S_1$ . Similarly the inequality  $S_1 \leq 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h$  from Case 2 also did not use  $u \leq s$ . So we get  $L_3 \leq 16^{u/4} S_1 \leq 16^{u/4} \cdot 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h$  which we simplify below. We have:

$$\begin{aligned}
L_3 &\leq 16^{u/4} \cdot 16(e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h \\
&= 16(2e^2 \varepsilon_0^{1/4} C_4)^u (C_6 / \varepsilon_0^{1/4})^h
\end{aligned}$$

$$\begin{aligned}
&\leq 16(C_6/\varepsilon_0^{1/4})^h \quad (\text{Using } \varepsilon_0 \leq \frac{1}{(2e^2C_4)^4}) \\
&\leq C_3^{h/2} \quad (\text{Using } C_3 \geq (16C_6/\varepsilon_0^{1/4})^2, h \geq 1).
\end{aligned}$$

This concludes Case 3.

**Case 4:**  $16s < u \leq \sqrt{\varepsilon}n$ : Here again it suffices to prove Eq. (6.28) which is equivalent to proving  $L_3 \leq C_3^{h/2}$ . We have

$$\begin{aligned}
L_3 &= 16(16C_1)^{u/2}(un/u^2)^{u/4} \cdot \alpha^{(o+n)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\
&= 16(16C_1)^{u/2}(u/s)^{u/4}(sn/u^2)^{u/4} \cdot \alpha^{(o+n)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\
&\leq 16(16C_1)^{u/2}\varepsilon^{-u/8}(sn/u^2)^{u/4} \cdot \alpha^{(o+n)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\
&\quad (\text{Using } s = \varepsilon n \text{ and } u \leq \sqrt{\varepsilon}n \text{ yielding } u/s \leq \sqrt{\varepsilon}/\varepsilon = \varepsilon^{-1/2}) \\
&\leq 16(C_4/\varepsilon^{1/8})^u C_5^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h'^2)^{h'/4} \cdot (h^2/(sn))^{h/4} \\
&\quad (\text{Using } \alpha \leq \alpha_0 \leq 1, h' \leq h, h \leq 2^h, \kappa \leq o \leq u, C_4 \geq 4\sqrt{C_1} \cdot C \cdot q^k, C_5 \geq \max\{1, 2C_2, 2\sqrt{C_2}\}) \\
&\leq 16(C_4/\varepsilon^{1/8})^u C_6^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(h-h')/4} \\
&\quad (\text{Using } (h/h')^{h'/2} \leq e^h \text{ and } C_6 \geq eC_5) \\
&= 16(C_4/\varepsilon^{1/8})^u C_6^h \cdot (sn/u^2)^{u/4} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(u+\kappa-(\eta+o))/4} \\
&= 16(C_4/\varepsilon^{1/8})^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2n^3/(s\kappa^4))^{\kappa/4} \cdot (su^4/(n\eta^2h^2))^{\eta/4} \cdot (su^4/n^3h^2)^{o/4} \\
&= 16(C_4/\varepsilon^{1/8})^u C_6^h \cdot (h^2/u^2)^{u/4} \cdot (h^2n^2/(\varepsilon\kappa^4))^{\kappa/4} \cdot (\varepsilon u^4/(\eta^2h^2))^{\eta/4} \cdot (\varepsilon u^4/(n^2h^2))^{o/4} \\
&= 16C_4^u C_6^h \cdot \varepsilon^{-u/8-\kappa/4+\eta/4+o/4} \cdot (h^2/u^2)^{u/4} \cdot (h^2n^2/\kappa^4)^{\kappa/4} \cdot (u^4/(\eta^2h^2))^{\eta/4} \cdot (u^4/(n^2h^2))^{o/4} \\
&\quad (\text{Collecting } \varepsilon \text{ terms}) \\
&\leq 16C_4^u C_6^h \varepsilon^{u/8-h} \cdot (h^2/u^2)^{u/4} \cdot (h^2n^2/(\kappa^4))^{\kappa/4} \cdot (u^4/(\eta^2h^2))^{\eta/4} \cdot (u^4/(n^2h^2))^{o/4} \\
&\quad (\text{Using } \eta + o - \kappa \geq u - h) \\
&\leq 16C_4^u C_6^h \varepsilon^{u/16} \cdot (h^2/u^2)^{u/4} \cdot (h^2n^2/(\kappa^4))^{\kappa/4} \cdot (u^4/(\eta^2h^2))^{\eta/4} \cdot (u^4/(n^2h^2))^{o/4} \\
&\quad (\text{Using } u \geq 16s \geq 16h \text{ in the form } h \leq u/16 \text{ to conclude } u/8 - h \geq u/16.) \\
&\leq 16C_4^u C_6^h \varepsilon_0^{u/16} \cdot (h^2/u^2)^{u/4} \cdot (h^2n^2/(\kappa^4))^{\kappa/4} \cdot (u^4/(\eta^2h^2))^{\eta/4} \cdot (u^4/(n^2h^2))^{o/4} \\
&\quad (\text{Using } \varepsilon \leq \varepsilon_0) \\
&\leq 16(e^2\varepsilon_0^{1/16}C_4)^u C_6^h \cdot (h/u)^{u/2} \cdot (hn/(u^2))^{\kappa/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{o/2} \\
&\quad (\text{Using } (u/\kappa)^\kappa \leq e^u \text{ and } (u/\eta)^\eta \leq e^u) \\
&= 16(e^2\varepsilon_0^{1/16}C_4)^u C_6^h \cdot (h/u)^{(u+\kappa-\eta-o)/2} \cdot (u/n)^{(o-\kappa)/2} \\
&\leq 16(e^2\varepsilon_0^{1/16}C_4)^u C_6^h \cdot (h/u)^{(u+\kappa-\eta-o)/2} \quad (\text{Using } u \leq n) \\
&\leq 16(e^2\varepsilon_0^{1/16}C_4)^u C_6^h \quad (\text{Using } h \leq u \text{ and } u + \kappa - \eta - o \geq \kappa \geq 0) \\
&\leq 16C_6^h \quad (\text{Using } \varepsilon_0 \leq (e^{-2}/C_4)^{16}) \\
&\leq 16(C_3^{1/2}/16)^h \quad (\text{Using } C_3 \geq 256C_6^2) \\
&\leq C_3^{h/2} \quad (\text{Using } h \geq 1).
\end{aligned}$$

This establishes Eq. (6.28) in Case 4.

**Case 5:**  $\sqrt{\varepsilon}n < u \leq n$ : Here we use  $U_{C_1,s}(u) \leq (2q^2e^2n/u)^{u/2}$ . With this modification we need to prove:

$$\begin{aligned} & \left( (2q^2e^2)^{u/2} (n/u)^{u/2} \right) \left( \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \right) \left( C_2^{h'/2} (sn/h'^2)^{h'/4} \right) \cdot h \cdot q^{k\kappa} \\ & \leq 4^{-u-2} \cdot C_3^{h/2} \cdot (sn/h^2)^{h/4} = 4^{-u-2} \cdot U_{C_3,s}(h), \end{aligned} \quad (6.29)$$

Multiplying the LHS by  $4^{u+2}(h^2/sn)^{h/4}$  we get the term  $L_5$  defined below which we wish to upper bound by  $C_3^{h/2}$ .

$$\begin{aligned} L_5 & := 16 \cdot 4^u (2q^2e^2)^{u/2} (n/u)^{u/2} \alpha^{(o+\eta)/k} C^u (n/\kappa)^\kappa (u/\sqrt{n\eta})^\eta (u/n)^o \cdot C_2^{h'/2} (sn/h'^2)^{h'/4} \cdot h \cdot q^{k\kappa} \cdot (h^2/(sn))^{h/4} \\ & \leq 16C_0^u C_5^h \alpha^{(o+\eta)/k} \cdot (n/u)^{u/2} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h'^2)^{h'/4} \cdot (h^2/(sn))^{h/4} \\ & \quad \text{(Using } h' \leq h \leq 2^h, \kappa \leq u, C_0 \geq \sqrt{2} \cdot 4e \cdot q \cdot C \cdot q^k, C_5 \geq 2\sqrt{C_2}\text{)} \\ & \leq 16C_0^u C_6^h \alpha^{(o+\eta)/k} \cdot (n/u)^{u/2} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(h-h')/4} \\ & \quad \text{(Using } (h/h')^{h'/2} \leq e^h \text{ and } C_6 \geq eC_5\text{)} \\ & = 16C_0^u C_6^h \alpha^{(o+\eta)/k} \cdot (n/u)^{u/2} \cdot (n/\kappa)^\kappa \cdot (u/\sqrt{n\eta})^\eta \cdot (u/n)^o \cdot (sn/h^2)^{-(u+\kappa-(\eta+o))/4} \\ & = 16C_0^u C_6^h \alpha^{(o+\eta)/k} \cdot (nh^2/(su^2))^{u/4} \cdot (h^2n^3/(s\kappa^4))^{\kappa/4} \cdot (su^4/(n\eta^2h^2))^{\eta/4} \cdot (su^4/n^3h^2)^{o/4} \\ & = 16C_0^u C_6^h \alpha^{(o+\eta)/k} \cdot (h^2/(\varepsilon u^2))^{u/4} \cdot (h^2n^2/(\varepsilon\kappa^4))^{\kappa/4} \cdot (\varepsilon u^4/(\eta^2h^2))^{\eta/4} \cdot (\varepsilon u^4/(n^2h^2))^{o/4} \\ & = 16C_0^u C_6^h \alpha^{(o+\eta)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h^2/(u^2))^{u/4} \cdot (h^2n^2/(\kappa^4))^{\kappa/4} (u^4/(\eta^2h^2))^{\eta/4} (u^4/(n^2h^2))^{o/4} \\ & \leq 16(e^2C_0)^u C_6^h \alpha^{(o+\eta)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h/u)^{u/2} \cdot (hn/(u^2))^{\kappa/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{o/2} \\ & \quad \text{(Using } (u/\kappa)^\kappa \leq e^u \text{ and } (u/\eta)^\eta \leq e^u\text{)} \\ & = 16(e^2C_0)^u C_6^h \alpha^{(o+\eta)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} \cdot (u^2/(nh))^{(o-\kappa)/2} \\ & \leq 16(e^2C_0)^u C_6^h \alpha^{(o+\eta)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h/u)^{u/2} \cdot (u/h)^{\eta/2} (u/h)^{(o-\kappa)/2} \\ & \quad \text{(Using } u \leq n \text{ and } o \geq \kappa\text{)} \\ & \leq 16(e^2C_0)^u C_6^h \alpha^{(u-h)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h/u)^{(u-\eta-o+\kappa)/2} \\ & \quad \text{(Using } \alpha \leq 1 \text{ and } u-h \leq \eta+o\text{)} \\ & \leq 16(e^2C_0)^u C_6^h \alpha_0^{(u-h)/k} \cdot \varepsilon^{(-u-\kappa+\eta+o)/4} \cdot (h/u)^{(u-\eta-o+\kappa)/2} \\ & \quad \text{(Using } \alpha \leq \alpha_0 \text{ and } u-h \geq 0\text{)} \\ & = 16(\alpha_0^{1/k} e^2 C_0)^u (C_6/\alpha_0^{1/k})^h (h^2/(\varepsilon u^2))^{(u-\eta-o+\kappa)/4} \\ & \leq 16(\alpha_0^{1/k} e^2 C_0)^u (C_6/\alpha_0^{1/k})^h \\ & \quad \text{(Using } h \leq s = \varepsilon n \text{ and } u \geq \sqrt{\varepsilon}n \text{ to conclude } h^2/(\varepsilon u^2) \leq 1. \text{ Also using } u-\eta-o+\kappa \geq 0\text{)} \\ & \leq 16(C_6/\alpha_0^{1/k})^h \quad \text{(Using } \alpha_0 \leq 1/(e^2 C_0)^k\text{)} \\ & \leq 16(C_3^{1/2}/16)^h \quad \text{(Using } C_3 \geq (16C_6/\alpha_0^{1/k})^2\text{)} \\ & \leq C_3^{h/2} \quad \text{(Using } h \geq 1\text{)}. \end{aligned}$$

This concludes the analysis of Case 5 and proves the lemma.  $\square$

**Step 3: Proof of Lemma 6.18.** We are now ready to combine the ingredients from the previous steps to prove Lemma 6.18.

*Proof of Lemma 6.18.* Let  $\alpha_0$  be the as given by Lemma 6.26. Let  $\varepsilon_0$  and  $C_3$  be the parameters given by Lemma 6.26 for  $C_1 = C$  and  $C_2 = C_0$ . We prove the lemma for  $C'' = C_3$  and  $\tau_0 = \varepsilon_0$ .

Let  $\alpha \leq \alpha_0$  and  $m = \alpha n$ . For every  $s \leq \varepsilon_0 n$ , we prove that the LHS in the lemma statement is upper bounded by  $W_{C_3,s}(h)$  for every  $h \in [s]$ . In the following, for every matching  $M$  of size  $m$ , we fix a  $B' = B'(M)$  that is  $(M, C_0, s)$ -reduced. (The inequalities hold for every such fixing.) We have

$$\begin{aligned} & \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \mathbb{E}_M \left[ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \right] \\ &= \sum_{u=0}^n \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ |\text{supp}(\mathbf{u})|=u}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \mathbb{E}_M \left[ \sum_{\substack{\mathbf{u}' \in \mathbb{Z}_q^n \\ \|\mathbf{u} + \mathbf{u}'\|_0 = h}} \frac{q^n}{|B'|} \left| \widehat{\mathbf{1}}_{B'}(\mathbf{u}') \right| \right] \\ &\leq \sum_{u=0}^n \sum_{\substack{\mathbf{u} \in \mathbb{Z}_q^n \\ |\text{supp}(\mathbf{u})|=u}} \frac{q^n}{|B|} \left| \widehat{\mathbf{1}}_B(\mathbf{u}) \right| \cdot \sum_{o,\eta,\kappa} p_{q,\alpha}(n, u, o, \eta, \kappa) \cdot h \cdot 2^{k\kappa} \cdot U_{C_0,s}(h + o + \eta - (u + \kappa)) \quad (6.30) \end{aligned}$$

$$\leq \sum_{u=0}^n \sum_{o,\eta,\kappa} U_{C,s}(u) \cdot p_{q,\alpha}(n, u, o, \eta, \kappa) \cdot h \cdot 2^{k\kappa} \cdot U_{C_0,s}(h + o + \eta - (u + \kappa)) \quad (6.31)$$

$$\leq \sum_{u=0}^n \sum_{o,\eta,\kappa} 4^{-u-2} W_{C_3,s}(h) \quad (6.32)$$

$$\begin{aligned} &\leq \sum_{u=0}^n (u+1)^3 \cdot 4^{-u-2} \cdot W_{C_3,s} \\ &\leq W_{C_3,s}(h), \end{aligned}$$

where (6.30) follows from Lemma 6.22 and the fact that  $B'$  is  $(M, C_0, s)$ -reduced, (6.31) follows from the fact that  $B$  is  $(C, s)$ -bounded, and (6.32) follows from Lemma 6.26 for  $C_3$  as defined above. This proves the lemma.  $\square$

## Acknowledgments

Thanks to Raghuvansh Saxena for pointing out errors in previous versions of this paper including a significant error in a previous proof of Lemma 6.26. Thanks to Noah Singer for many valuable comments on the paper including pointing out the use of inconsistent and ambiguous notation and some significant errors (that are hopefully fixed in this version). Thanks to an anonymous conference referee for pointing out some errors in the proof of Lemma 2.13. Thanks to the anonymous SICOMP referees for the careful reading of the paper and for the helpful and detailed comments.

## References

- [ABFS25] Amir Azarmehr, Soheil Behnezhad, Shane Ferrante, and Mohammad Saneian. Half-Approximating Maximum Dicut in the Streaming Setting. *arXiv:2512.22729*, 2025.
- [AKL16] Sepehr Assadi, Sanjeev Khanna, and Yang Li. Tight bounds for single-pass streaming complexity of the set cover problem. In *STOC 2016*, pages 698–711, 2016.

- [AKSY20] Sepehr Assadi, Gillat Kol, Raghuvansh R. Saxena, and Huacheng Yu. Multi-Pass Graph Streaming Lower Bounds for Cycle Counting, MAX-CUT, Matching Size, and Other Problems. In *FOCS 2020*, pages 354–364, 2020.
- [AN21] Sepehr Assadi and Vishvajeet N. Graph streaming lower bounds for parameter estimation and property testing via a streaming XOR lemma. In *STOC 2021*, pages 612–625, 2021.
- [BHP<sup>+</sup>22] Joanna Boyland, Michael Hwang, Tarun Prasad, Noah Singer, and Santhoshini Velusamy. On sketching approximations for symmetric boolean CSPs. In *APPROX 2022*, volume 245, pages 38:1–38:23. LIPIcs, 2022.
- [CGSV21a] Chi-Ning Chou, Alexander Golovnev, Madhu Sudan, and Santhoshini Velusamy. Approximability of all finite CSPs with linear sketches. In *FOCS 2021*, pages 1197–1208. IEEE, 2021.
- [CGSV21b] Chi-Ning Chou, Alexander Golovnev, Madhu Sudan, and Santhoshini Velusamy. Approximability of all Boolean CSPs with linear sketches. *CoRR*, abs/2102.12351v3, 14th April 2021.
- [CGV20] Chi-Ning Chou, Alexander Golovnev, and Santhoshini Velusamy. Optimal streaming approximations for all Boolean Max-2CSPs and Max- $k$ SAT. In *FOCS 2020*, pages 330–341. IEEE, 2020.
- [GKK<sup>+</sup>09] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2009.
- [GT19] Venkatesan Guruswami and Runzhou Tao. Streaming hardness of unique games. In *APPROX 2019*, pages 5:1–5:12. LIPIcs, 2019.
- [GVV17] Venkatesan Guruswami, Ameya Velingker, and Santhoshini Velusamy. Streaming complexity of approximating Max 2CSP and Max Acyclic Subgraph. In *APPROX 2017*, pages 8:1–8:19. LIPIcs, 2017.
- [KK19] Michael Kapralov and Dmitry Krachun. An optimal space lower bound for approximating MAX-CUT. In *STOC 2019*, pages 277–288. ACM, 2019.
- [KKS15] Michael Kapralov, Sanjeev Khanna, and Madhu Sudan. Streaming lower bounds for approximating MAX-CUT. In *SODA 2015*, pages 1263–1282. SIAM, 2015.
- [KKSV17] Michael Kapralov, Sanjeev Khanna, Madhu Sudan, and Ameya Velingker.  $(1 + \omega(1))$ -approximation to MAX-CUT requires linear space. In *SODA 2017*, pages 1703–1722. SIAM, 2017.
- [O’D14] Ryan O’Donnell. *Analysis of Boolean functions*. Cambridge University Press, 2014.
- [Sin23] Noah G. Singer. Oblivious algorithms for the Max- $k$ AND problem. In *APPROX 2023*, volume 275, pages 15:1–15:19. LIPIcs, 2023.
- [SSSV23] Raghuvansh R. Saxena, Noah G. Singer, Madhu Sudan, and Santhoshini Velusamy. Improved streaming algorithms for maximum directed cut via smoothed snapshots. In *FOCS 2023*, pages 855–870. IEEE, 2023.

- [SSSV25] Raghuvansh R. Saxena, Noah G. Singer, Madhu Sudan, and Santhoshini Velusamy. Streaming algorithms via local algorithms for maximum directed cut. In *SODA 2025*, pages 3392–3408. SIAM, 2025.
- [SSV21] Noah Singer, Madhu Sudan, and Santhoshini Velusamy. Streaming approximation resistance of every ordering CSP. In *APPROX 2021*, volume 207, pages 17:1–17:19. LIPIcs, 2021.
- [VY11] Elad Verbin and Wei Yu. The streaming complexity of cycle counting, sorting by reversals, and other problems. In *SODA 2011*, pages 11–25. SIAM, 2011.
- [Yao77] Andrew Chi-Chih Yao. Probabilistic computations: Toward a unified measure of complexity. In *FOCS 1977*, pages 222–227. IEEE, 1977.