Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 237 (2026)

Counterexamples to Beyond-Johnson Proximity Gaps over Binary Fields

Quang Dao* Scott Duke Kominers† Justin Thaler‡ Kai Zhe Zheng§

2 November 2026

Abstract

Many hash-based proof systems check that committed words are close to Reed–Solomon codewords by testing one random combination of them. Their soundness analysis uses a *proximity gap*: if the combination agrees with a codeword on many positions, so do the original words, on the same positions, except for a few *exceptional* challenges. Such gaps are known above the Johnson threshold, about $\sqrt{\rho}$ for rate ρ, and extending them below it would shrink proofs. Recent work does so in large characteristic, but not for the additive domains used over binary fields, where some of the fastest proof systems run. We show that on these domains, beyond-Johnson proximity gaps fail.

Our first construction applies to any additive domain (a linear subspace) filling a constant fraction of a containing binary field, such as the length-2^{27} domain of Binius64. Over a suitable extension challenge field and at rate $1/4$, it gives two words that can simultaneously match codewords on at most 25% of the positions, while their combinations approach the 50% Johnson threshold for superpolynomially many challenges. This rules out any $\mathrm{poly}(N)/|\mathbb{F}|$ bound on the exceptional probability below Johnson.

The construction also rules out polynomial-size decoding lists below Johnson: one word agrees with superpolynomially many codewords at agreement approaching 50%. Earlier superpolynomial lists needed the rate, or the agreement–rate gap, to vanish.

Our second and third constructions cover every additive domain, including the sparse domains used by LeanVM and Flock. At rate $1/16$, the second gives $(N-1)(N-2)/6$ exceptional challenges at the Johnson threshold itself, when the domain lies in a proper subfield of the challenge field.

The third construction trades agreement for larger exception counts: at rate $1/2$ and length 2^{22}, its combinations reach 53.125% agreement from common agreement 50%, with probability at least 2^{-20} over a 192-bit challenge field. Finally, at every fixed rate, some constant agreement above the rate makes every challenge exceptional, over $\mathrm{poly}(N)$-size challenge fields. All of our results are formally verified in Lean.

*Carnegie Mellon University. qvd@andrew.cmu.edu.

†Harvard University and a16z crypto research. kominers@fas.harvard.edu. This work was performed while Kominers was visiting the Technological Innovation, Entrepreneurship, and Strategic Management (TIES) Group at the MIT Sloan School of Management.

‡a16z crypto research and Georgetown University. justin.r.thaler@gmail.com.

§Simons Institute for the Theory of Computing. Part of this work was performed during an internship with a16z crypto research. kzzheng@mit.edu.

ISSN 1433-8092

Contents

1 Introduction **3**
- 1.1 Our results . . . 4
- 1.2 Comparison with prior results . . . 6

2 Technical overview **8**
- 2.1 Common framework: from polynomial families to counterexamples . . . 9
- 2.2 Construction 1: Gold moments on dense domains . . . 11
- 2.3 Construction 2: subspace locators on arbitrary additive domains . . . 14
- 2.4 Construction 3: decision trees for sparse domains . . . 15

3 Notation and common tools **17**
- 3.1 Notation and agreement . . . 17
- 3.2 Additive locators and pole reduction . . . 20
- 3.3 Individual agreement bounds . . . 22
- 3.4 Boolean polynomials and witnesses . . . 24
- 3.5 Padding and collision averaging . . . 25

4 Subspace-locator constructions **26**
- 4.1 Quadratically many exceptional challenges on arbitrary additive domains . . . 26
- 4.2 Every challenge exceptional at every fixed rate . . . 29
- 4.3 Exceptional probability approaching one at half agreement . . . 33

5 Gold constructions: superpolynomially many exceptions near Johnson **34**
- 5.1 The counting bound and its consequences . . . 34
- 5.2 Exceptional counts and probabilities near Johnson . . . 35
- 5.3 From quadratic functions to polynomials with many roots . . . 37
- 5.4 Counting matrices of rank $2t$ . . . 42
- 5.5 Proof of the counting bound . . . 43
- 5.6 Increasing agreement and rate by padding . . . 43
- 5.7 A concrete bound for Binius64 . . . 46
- 5.8 A concrete bound for Google's Longfellow . . . 47
- 5.9 Superpolynomial decoding lists and exceptional sets at further rates . . . 49

6 Decision-tree constructions at half agreement and half rate **51**
- 6.1 From unions of flats to exceptional challenges . . . 51
- 6.2 Counting balanced tree supports . . . 52
- 6.3 Rate one half: supports avoiding a subspace . . . 55
- 6.4 Concrete bounds for the parameters of LeanVM and Flock . . . 57

7 Summary of results and deployed systems **58**

8 Discussion and open questions **59**

Formal verification in Lean **60**

AI methodology **60**

A Deferred proofs **60**

1 Introduction

Many hash-based succinct proof systems (SNARKs) verify large computations by inspecting only a few entries of received words—vectors of field elements—purported to be close to Reed–Solomon codewords. A Reed–Solomon codeword lists the values of a polynomial of degree less than K on a fixed set D of N field elements, the *evaluation domain*; the code has rate $\rho = K/N$. The number of queries directly affects proof size, since each query adds field values and Merkle authentication paths to the proof. Some of the fastest provers for these systems work over binary fields (fields of characteristic two), including Binius [24], Flock [17], BinarySpartan [45], LeanVM [42], and Google's Longfellow [29].[1]

To check many words at once, the verifier combines two received words f, g, fixed before the challenge is drawn, into $f + zg$, for a random element z of a large *challenge field*, and tests only the combination. The standard soundness analysis uses a *proximity gap*: if the combination agrees with a codeword on many positions, the inputs must also agree with codewords on many common positions, except with small probability. The inputs may match different codewords, but the positions must be shared. The largest number of such positions is their *common agreement*. We call a challenge *exceptional* if the combination agrees with a codeword on more positions than this.

The Johnson threshold and beyond. Classical proximity-gap theorems, valid in every characteristic, require the fraction of matching positions to exceed the *Johnson agreement threshold*, approximately $\sqrt{\rho}$ for a code of rate ρ [6, 7]; counted in positions, the threshold is $\sqrt{N(K-1)}$. Capacity corresponds to agreement fraction ρ: interpolation lets any received word match a polynomial of degree less than K on any chosen K positions.

A proximity gap beyond Johnson, that is, at agreement below the Johnson threshold, would extend the soundness analysis of proof systems to words with more errors, which a random query is more likely to expose. The verifier could then make fewer queries, shrinking proofs at the same security level [4, 20].

How far below Johnson? Ben-Sasson, Carmon, Ishai, Kopparty, and Saraf [7, Conjecture 8.4] conjectured that proximity gaps hold all the way down to capacity: at every agreement fraction exceeding the rate ρ by some $\eta > 0$, the probability that a random challenge is exceptional would be at most a polynomial in N, $1/\rho$, and $1/\eta$, divided by the size of the challenge field. WHIR [4, Conjecture 4.12, item 2] states the corresponding conjecture on *smooth* domains (multiplicative subgroups of power-of-two size and their scalar multiples) for the stronger guarantee of *mutual correlated agreement* (MCA), which asks that whenever the combination matches a codeword on a sufficiently large set, the inputs match codewords on that same set, except with small probability. Implementations have used conjectured bounds of this kind to set query counts [7, Section 8.2], including a binary-field implementation by Ben-Sasson, Bentov, Horesh, and Riabzev [5, Appendix B.8].

The arbitrary-domain conjecture has now been disproved in every characteristic [19, 23, 41]. The counterexamples of Krachun, Kazanin, and Haböck [41] are on multiplicative subgroups of prime fields, the family of domains that contains the smooth ones. Those counterexamples, however, occur at agreement approaching capacity, or at vanishing rate. They leave open whether proximity gaps hold at fixed rate and agreement bounded away from capacity, including just below Johnson. The smooth-domain conjecture does not apply over binary fields: the multiplicative group of a binary field has odd order, so it has no nontrivial subgroup of power-of-two size. The binary analogue concerns additive domains, which we study here.

Following the result of Brakensiek, Chen, Putterman, Zhang, and Zheng that, over prime fields, list decoding approaching capacity runs in polynomial time on every evaluation set at every constant rate [15],

[1] Advantages of binary fields include efficient commitments to small values, fast arithmetic on modern hardware, and efficient representations of bitwise operations; see [12, 24].

proximity gaps beyond Johnson are now proved in sufficiently large characteristic [20, 35], after an earlier unpublished argument at low rate over prime fields [43].

These positive results do not apply to binary fields. For arbitrary evaluation domains, the polynomial bound on exceptional challenges known in every characteristic extends only a constant number of positions below the Johnson threshold [36], and guarantees up to capacity are known when the evaluation points are chosen at random [31] or by an explicit construction in extension fields of polynomial size [1], including binary ones. Binary-field SNARKs, however, evaluate on *additive domains*, $\mathbb{F}_2$-subspaces of a binary field, because these support fast Fourier transforms. For these structured domains, the central question remains:

Over binary fields, on the additive domains that SNARKs use, do proximity gaps hold below the Johnson threshold?

1.1 Our results

We answer this question in the negative, via three constructions.[2] The first, which we call the Gold construction, gives superpolynomially many exceptional challenges near Johnson on additive domains that fill a constant fraction of a binary field, such as the length-2^{27} domain of Binius64 [13]. The other two work on every additive domain, including the sparse domains of LeanVM [42] and Flock [25].

1.1.1 Dense domains: the Gold construction

We call additive domains of growing length *dense* if each lies in a binary field $\mathbb{B}$ with $|\mathbb{B}|/|D|$ bounded independently of the length. Our strongest results hold on dense domains, through a construction named after the power functions x^{2^i+1} studied by Gold [30]. We state them at rate $1/4$, with Johnson threshold 50%.

Theorem (Informal version of Corollary 5.2)**.** On every dense additive domain of sufficiently large size N, over a suitable extension challenge field, the Reed–Solomon code of rate $1/4$ has two fixed received words f, g such that:

1. The inputs can match codewords simultaneously on at most 25% of the positions.
2. For $N^{\Omega(\log N)}$ distinct challenges z, the combination $f + zg$ matches a codeword on a $1/2 - N^{-\Omega(1)}$ fraction of the positions.

The implied constants depend only on the density. When D fills at least an eighth of $\mathbb{B}$, the agreement is $N/2 - \Theta(N^{3/4})$ positions and the count is $N^{(1/8-o(1))\log_2 N}$.

The theorem rules out the conjectured form of a proximity gap below Johnson. A bound of the form $\mathrm{poly}(N)/|\mathbb{F}|$ on the exceptional probability limits the exceptional challenges to polynomially many, and the theorem gives $N^{\Omega(\log N)}$ of them over an extension of $\mathbb{B}$ of size $N^{\Theta(\log N)}$.

Theorem (Informal version of Theorem 5.4)**.** Fix $1/4 < \alpha < 1/2$ and a polynomial bound. For arbitrarily large N, there are a binary additive domain of size N, a binary challenge field of size polynomial in N, and two received words f, g for the rate-$1/4$ Reed–Solomon code, with common agreement exactly $N/4$, such that more challenges than the bound make $f + zg$ agree with a codeword on at least αN positions.

The domains are hyperplanes of a binary field $\mathbb{B}$ of size $2N$, a power of four, and the challenge field has fixed degree $e \geq 2$ over $\mathbb{B}$. A constant fraction of all challenges is then exceptional at agreement $1/2 - O(N^{-1/2})$ (Corollary 5.3).

[2] None of the current systems discussed here relies on beyond-Johnson proximity-gap conjectures; Section 7 explains the scope of our results for them.

The Gold pairs also violate two weaker guarantees. Guarantees with a *proximity loss* ϵ require the inputs to share agreement only ϵ below the combination's; at a fixed agreement fraction α between 25% and 50%, our pairs violate them for every loss below $\alpha - 1/4$, which approaches 25 percentage points as α approaches 50%. Other guarantees require only that each input be individually close to a codeword, but at rate $1/4$ each input of the pairs in these theorems agrees with every codeword on at most $3N/8$ positions (Lemma 3.13), while the combination reaches nearly $N/2$.

List decoding. The same polynomials give superpolynomial *decoding lists*, the sets of codewords agreeing with one received word at a given threshold.

Theorem (Informal version of Corollaries 5.2 and 5.23)**.**

1. On every dense additive domain, the rate-$1/4$ Reed–Solomon code over the containing field, of size $O(N)$, has a received word agreeing with $N^{\Omega(\log N)}$ codewords on a $1/2 - o(1)$ fraction of the positions.

2. In every characteristic p, for each fixed power b of p, on the full fields $\mathbb{F}_{b^{2n}}$, the rate-$1/b^2$ code has a received word agreeing with $N^{\Omega_b(\log N)}$ codewords on a $1/b - \Theta_b(N^{-1/4})$ fraction of the positions.

These codes therefore admit no polynomial list-size bound at any fixed agreement fraction below Johnson. At rate $1/4$ on full binary fields, Zhu independently obtains the same lists (Section 1.2).

Other rates. Superpolynomial exceptional counts also occur at every fixed rate $0 < \rho < 1$, on every sufficiently large dense additive domain and its affine translates. The inputs' common agreement is ρ, and the combination agreement is a constant strictly between ρ and $\sqrt{\rho}$ (Corollary 5.17). Sections 5.7 and 5.8 apply the Gold construction to the domains of Binius64 and of Google's Longfellow [28]; the latter are not additive but contain a large affine subspace.

1.1.2 Every domain: the subspace-locator construction

The second construction needs no density: it uses the vanishing polynomials, or *locators*, of subspaces of the domain. At rate $1/16$, where the Johnson agreement threshold is approximately 25%, it gives quadratically many exceptional challenges.

Theorem (Informal version of Theorem 4.1)**.** Let D be a binary additive domain of $N \geq 32$ points, contained in a proper subfield of the challenge field. The rate-$1/16$ Reed–Solomon code on D has two fixed received words f, g such that:

1. The inputs can match codewords simultaneously on fewer than 12.5% of the positions.

2. For exactly $(N-1)(N-2)/6$ distinct challenges z, the combination $f + zg$ matches a codeword on $N/4 - 1$ positions.

The combination agreement $N/4 - 1$ lies above the exact Johnson threshold $\sqrt{N(K-1)}$. Any MCA guarantee for these codes at or below Johnson must therefore have error at least $(N-1)(N-2)/(6|\mathbb{F}|)$, even if it gives up nearly $N/8$ positions of agreement.

Without the subfield condition, Corollary 4.2 still gives more than half of the $(N-1)(N-2)/6$ challenges on every additive domain in a field $\mathbb{F}$ with at least that many elements (Table 1). At length 2^{20} over a 128-bit challenge field, for example, the exceptional probability at Johnson and below exceeds $2^{-90.585}$. At rate $1/8$, the same construction applies to the domains of the 2018 implementation of Ben-Sasson, Bentov, Horesh, and Riabzev: with its two independent challenges from a 64-bit field, an analysis that counts each exceptional challenge as a failure can certify at most 57.17 of its targeted 60 bits (Section 4.2).

Every challenge, at every rate. We call the excess of the combination's agreement over the inputs' common agreement the *common-agreement gap*. At every fixed rate, the construction keeps this gap a constant fraction of the positions, and gives quadratically many exceptional challenges once $|\mathbb{F}| \geq N^2$.

Theorem (Informal version of Theorem 4.5)**.** Fix a rate $0 < \rho < 1$ and an exponent $a \geq 1$. There is a constant $\varepsilon > 0$ with $\rho + \varepsilon < \sqrt{\rho}$ such that, on every binary additive domain of sufficiently large size N, over every challenge field with at most N^a elements, the Reed–Solomon code of message length $\lfloor \rho N \rfloor$ has two fixed received words f, g such that:

1. The inputs can match codewords simultaneously on at most a ρ fraction of the positions.
2. For *every* challenge z, the combination $f + zg$ matches a codeword on at least a $\rho + \varepsilon$ fraction of the positions.

1.1.3 Every domain, larger counts: the decision-tree construction

In a 192-bit challenge field, such as LeanVM's, a quadratic count gives only a small exceptional probability: at length 2^{22} it is below 2^{42}, whereas probability above 2^{-128} requires more than 2^{64} exceptional challenges. Our third construction uses recursive Boolean decision trees to obtain much larger exceptional sets on every binary additive domain, at agreement farther below Johnson.

Theorem (Informal version of Theorem 6.10)**.** Fix $h \geq 3$. On every binary additive domain D of length $N \geq 2^{2^h - 1}$, over every challenge field of size $q > N$ that contains D, the rate-$1/2$ Reed–Solomon code has two fixed received words such that:

1. The inputs can match codewords simultaneously on at most 50% of the positions.
2. For $\Omega_h(\min\{N^{2^h - h - 1}, q/N\})$ distinct challenges, their combination matches a codeword on a $1/2 + 2^{-h-1}$ fraction of the positions.

For example, at length 2^{22} in $\mathbb{F}_{2^{192}}$, at least 2^{172} challenges reach agreement $17/32 = 53.125\%$.

Table 1 summarizes our results approaching or reaching Johnson; Section 7 gives the remaining results, and Section 6.4 gives concrete bounds for LeanVM and Flock.

1.2 Comparison with prior results

Earlier binary-field counterexamples. Ben-Sasson, Goldberg, Kopparty, and Saraf [8, Lemma 3.3] use hyperplane locators at rate $1/8$, with agreement above Johnson; Theorem 4.7 adds a pole to the same locators to reach Johnson at rate $1/4$. Ben-Sasson, Carmon, Haböck, Kopparty, and Saraf [6, Corollary 1.7] obtain nearly quadratically many exceptions at Johnson near rate $1/16$. Their construction also gives polynomial counts of arbitrarily large degree, but requires lowering the rate and agreement threshold [6, Theorem 1.6]; raising the rate back to a fixed value shrinks the common-agreement gap. Our Gold construction gives superpolynomial counts at fixed rate $1/4$, with agreement approaching Johnson and a constant common-agreement gap (Corollary 5.2).

Their construction chooses a suitable additive domain, and a domain fixed in advance by an implementation need not be one. Our subspace-locator construction covers every prescribed additive domain, including sparse ones, with a quadratic count at Johnson at rate $1/16$ (Theorem 4.1 and Corollary 4.2).

Result and rate	Domain and challenge field	Agreement of combination α	Common γ	Exceptional count
Superpolynomial count $\rho = 1/4$ Corollary 5.2	Every additive $D \subseteq \mathbb{B}$, $\lvert\mathbb{B}\rvert = 2^c N$, fixed $c \geq 0$; a suitable extension of size $q = N^{\Theta_c(\log N)}$	$1/2 - o(1)$	$1/4$	$N^{\Omega_c(\log N)}$
Arbitrary additive domains $\rho = 1/16$ Theorem 4.1; Corollary 4.2	Every $D \subseteq \mathbb{F}$. The full quadratic count holds if $D \subseteq \mathbb{B} \subsetneq \mathbb{F}$.	$1/4 - 1/N$	$1/8 - 1/N$	Proper subfield: $\geq M$ Any field: $\geq \left\lceil \frac{qM}{q+M-1} \right\rceil$ $M = (N-1)(N-2)/6$
Exact half agreement $\rho = 1/4$ Theorem 4.7	Every proper affine binary domain $D \subsetneq \mathbb{F}$, $N \geq 8$	$1/2$	$1/4$	$2N - 2$ exactly Equals $q - 2$ if $q = 2N$

Table 1: Counterexamples approaching or reaching the Johnson agreement threshold. Here $N = |D|$, $q = |\mathbb{F}|$, α is the agreement fraction of the combination, γ is the inputs' common agreement fraction, and the last column counts exceptional challenges for one fixed pair. Subscripts on asymptotic notation indicate parameters on which the implicit constants may depend. In the second row, $N \geq 32$ is a multiple of 16, and the same challenges are exceptional at every lower threshold down to $N/8 + 1$.

Near-capacity counterexamples. Crites and Stewart [19, Corollary 1] give examples in which every challenge is exceptional, in any characteristic and on arbitrary evaluation domains. At fixed rate and polynomial field size, their common-agreement gap tends to zero as the block length grows. On binary additive domains, our Theorem 4.5 keeps the gap constant under the same constraints.

Diamond and Gruen [23, Theorem 4.14] obtain superpolynomial exceptional counts with vanishing rate and agreement. Krachun, Kazanin, and Haböck [41, Theorem 1] obtain arbitrarily large polynomial counts at any fixed limiting rate on multiplicative subgroups of prime fields, but with a vanishing common-agreement gap; see also Kambiré [38], an earlier write-up of a sketch by Krachun and Kazanin. Our binary-field results keep both the rate and the common-agreement gap constant.

Upper bounds just beyond Johnson. Jo [36] bounds the exceptional count by $O(N^6)$ a fixed number of positions below Johnson, over every field and evaluation set, at each fixed rate $1/r$ for an integer $r \geq 2$. At rate $1/16$, our quadratic exceptional count remains valid at agreement $N/4 - 3$, the first integer below the exact Johnson threshold (Theorem 4.1), which leaves a gap between the exponents 2 and 6. Jo's bound excludes superpolynomial counts within a fixed number of positions of Johnson; ours occur $\Theta(N^{3/4})$ positions below it, at agreement fraction $(1 - o(1))\sqrt{\rho}$ with $\rho = 1/4$ on a full binary field (Corollary 5.2).

List-decoding lower bounds. Guruswami and Rudra [34], and Ben-Sasson, Kopparty, and Radhakrishnan [9], construct superpolynomial Reed–Solomon lists with vanishing rate. The latter also give constant-rate lower bounds, but their list-size exponent stays bounded at fixed rate and agreement fraction. Justesen and Høholdt [37] obtain linear-size lists at Johnson. Our lists have fixed rate and agreement approaching Johnson: rate $1/4$ on every dense additive domain (Corollary 5.2) and rate 4^{-k} over a field of size N (Corollary 5.23).

In the positive direction, in sufficiently large characteristic, Gabizon [26] and Dao, Kominers, and Thaler [20] prove linear list-size bounds at a constant agreement fraction below Johnson, and the latter give explicit polynomial list-size bounds at every fixed agreement above capacity. The superpolynomial list sizes also depend on the evaluation domain: randomly chosen evaluation points can achieve list-decoding capacity,

including in characteristic two [2, 16, 33]. Explicit evaluation points also suffice: Alrabiah, Goyal, and Guruswami [1] reach capacity over extension fields of polynomial size, and Chatterjee, Ghosh, Guo, Gurjar, Raj, and Zhang [18] give deterministic constructions beyond Johnson over larger fields.

General linear codes. Every linear code has proximity gaps up to the one-and-a-half Johnson radius, and Kominers, Thaler, and Zheng [40] show that this radius is tight for general linear codes. Reed–Solomon codes have proximity gaps up to the larger Johnson radius. Our results show that beyond it, whether they hold depends on the structure of the evaluation domain.

Our proof techniques in relation to prior work. The shared-coefficient method for constructing decoding lists comes from Ben-Sasson, Kopparty, and Radhakrishnan [9]. The conversion to exceptional challenges by division by a linear factor, and the counting argument for distinct challenges, appear in Ben-Sasson, Carmon, Haböck, Kopparty, and Saraf [6, Section 6] and Crites and Stewart [19, Theorem 2]. Gao, Yang, Xu, and Kan [27] give a general reduction from large decoding lists to MCA counterexamples. Our contribution is to construct superpolynomial lists at fixed rate and agreement approaching Johnson on dense additive binary domains, and to exploit their algebraic structure to obtain the exceptional-set bounds of Theorem 5.1, by bounding how often two list members give the same challenge (Section 2.2).

The agreement sets of Theorem 5.1, viewed in the containing full field, are supports of minimum-weight codewords of extended BCH codes, which were found through Gold's power functions [10, 11, 39]. We extend the equations that select these sets from full fields to every additive domain. Our degree bounds use an identity of Borges and Conceição [14, Lemma 4.1], and our counts of quadratic functions use identities of Delsarte and Goethals [22] and a family of Schmidt [44, Theorems 4.9 and 5.6]; Section 2 explains where each enters.

Concurrent and independent work. Zhu [46] independently constructs superpolynomial decoding lists for the full-length Reed–Solomon code over $\mathbb{F}_{2^h}$ at every fixed rate. His construction starts from the same objects as ours: supports of minimum-weight codewords of binary BCH codes, counted with Schmidt's enumeration of quadratic forms [44], are agreement sets for the received word $x \mapsto x^{N/2}$. At rate $1/4$ on the full field the two lists coincide, with $N^{(1/8-o(1))\log_2 N}$ codewords at agreement $(1/2 - o(1))N$. Zhu reaches other rates by passing to subspace quotients and by padding with common roots. Neither agreement envelope contains the other: Zhu's agreement is higher at rates in $(1/4, 1/2)$ when h is odd, while ours approaches Johnson at rate 4^{-k} when $2k$ divides h (Corollary 5.23).

Zhu's results concern decoding lists on the full field and on its dense subsets. Ours also apply to every prescribed dense additive domain, give proximity-gap counterexamples with explicit exceptional counts, and extend to every characteristic at rates $1/b^2$ (Theorem 5.22). For a fixed odd characteristic and growing extension degree, the last result answers at these rates a question that Zhu raises. Alrabiah, Goyal, and Guruswami [1] announce a companion paper showing that, without restrictions on the field or on the evaluation points, Reed–Solomon list sizes can grow superpolynomially just beyond the Johnson radius. They cite Zhu's work and ours as concurrent results of this kind.

Formal verification. All of our results are formally verified in Lean. The end of the paper describes the formalization and how AI models were used.

2 Technical overview

Our goal is to construct one fixed pair of words f, g for which many challenges z make $f + zg$ agree with a codeword on more positions than f, g can simultaneously agree with codewords. We start with polynomials that have many roots in the evaluation domain and share most of their high-degree coefficients. We turn

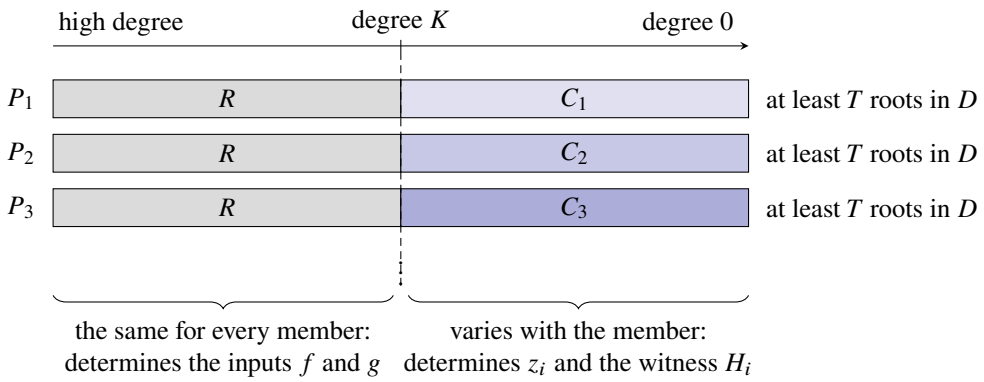


Figure 1: The input to pole reduction, drawn as coefficient vectors. Every member $P_i = R + C_i$ of the family has at least T roots in D, and all members have the same coefficients above degree K. The shared part determines the two input words, which are fixed before the challenge is sampled. The varying part has degree at most K and determines only the challenge and its witness. When $T > K$, each member gives an exceptional challenge. Throughout the figures, gray marks data shared by the whole family and blue marks data that depends on the member.

each polynomial into an identity expressing $f + zg$ minus a codeword; its roots then become agreement positions. Shared coefficients let us use the same f, g throughout the family. The remaining task is to ensure that many family members give different challenges. The full proofs come in a different order from this overview: Section 4 proves the subspace-locator results before Section 5 proves the Gold results, because the Gold proofs use its tools.

2.1 Common framework: from polynomial families to counterexamples

Choosing the inputs and codewords. Let $\mathbb{F}$ be the challenge field, let $D \subseteq \mathbb{F}$ be the evaluation domain, and put $N = |D|$. Fix a message length $1 \le K < N$: codewords are evaluations on D of polynomials over $\mathbb{F}$ of degree strictly less than K. Inputs f, g are functions $D \to \mathbb{F}$, and $f + zg$ means the function $x \mapsto f(x) + zg(x)$. A polynomial of degree less than K that agrees with a combination $f + zg$ on a specified set of positions is called an *explaining polynomial*, or *witness*, for that agreement. Suppose we can construct a family $\mathcal{P}$ of polynomials

$$P_i = R + C_i, \qquad \deg C_i \le K, \qquad i = 1, \dots, |\mathcal{P}|,$$

in which every P_i has at least T roots in D for some $T > K$, the polynomial R is fixed, and the C_i are distinct. We call C_i the *correction* to R in P_i. The degree condition says that all family members have the same coefficients above degree K (Figure 1).

Assume $\mathbb{F}$ contains a point outside D. Choose such a point β, called the *pole*, and fix

$$f(x) = \frac{R(x)}{x - \beta}, \qquad g(x) = \frac{1}{x - \beta} \qquad (x \in D).$$

For the ith family member, take $z_i = C_i(\beta)$ and

$$H_i(X) = -\frac{C_i(X) - C_i(\beta)}{X - \beta}.$$

The numerator vanishes at β and is therefore divisible by $X - \beta$. Division reduces its degree by one, making H_i a polynomial of degree strictly less than K. At every $x \in D$,

$$f(x) + z_i\, g(x) - H_i(x) = \frac{R(x) + C_i(x)}{x - \beta} = \frac{P_i(x)}{x - \beta}.$$

Hence $f + z_i g$ agrees with the codeword of H_i at every root of P_i in D, that is, on at least T positions. Only the challenge and the witness depend on C_i. We call the conversion of the family $P_i = R + C_i$ into the fixed inputs f, g, challenges z_i, and witnesses H_i *pole reduction* (Lemma 3.11).

Common agreement. Write $\mathrm{CA}_K(f, g)$ for the common agreement of f and g, and $\mathrm{agr}_K(g)$ for the largest number of positions on which g matches one codeword. If g agrees with a polynomial h of degree less than K, each agreement point is a root of $(X - \beta)h(X) - 1$, a polynomial of degree at most K with value -1 at β. Being nonzero, it has at most K roots. Thus $\mathrm{CA}_K(f, g) \le \mathrm{agr}_K(g) \le K$. Conversely, on any chosen K positions we can interpolate f and g separately by polynomials of degree less than K, which gives

$$\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K.$$

Since $T > K$, every challenge constructed above makes the combination agree with a codeword on more positions than the two inputs can share.

Counting distinct challenges. The construction gives at least as many exceptional challenges as there are distinct values among the z_i, which can be fewer than $|\mathcal{P}|$. Two family members give the same challenge exactly when β is a root of $C_i - C_j$, a nonzero polynomial of degree at most K, and each pair thus collides at no more than K of the $q - N$ possible poles, where q is the challenge-field size. Averaging at most $K\binom{|\mathcal{P}|}{2}$ collisions over the poles, some pole has at most $K\binom{|\mathcal{P}|}{2}/(q - N)$ colliding pairs. Keeping just one polynomial per challenge discards at most one polynomial per colliding pair, and the rest give distinct challenges. Lemma 3.19 also gives a stronger bound when there are many collisions.

Where the families come from. An *affine subspace* is a translate $W + a = \{w + a : w \in W\}$ of a linear subspace W. The *vanishing polynomial*, or *locator*, of any finite set S is $L_S(X) = \prod_{s \in S}(X - s)$: its leading coefficient is one, and its roots are exactly the points of S, each occurring once. When $S = W$ is an $\mathbb{F}_2$-subspace, its locator is *linearized* [9], meaning that its exponents are powers of two (Section 3.2 recalls why):

$$L_W = X^{|W|} + a_W X^{|W|/2} + b_W X^{|W|/4} + \cdots + c_W X.$$

Since a linearized polynomial is additive, translating W by a changes its locator only by the constant $-L_W(a)$. All affine subspaces of size $|W|$ thus have locators with leading term $X^{|W|}$ and all remaining terms of degree at most $|W|/2$. This *gap* below the leading term is what gives us shared high-degree coefficients.

Example: hyperplanes. Let W range over the $2N - 2$ affine hyperplanes of D. Each locator has the form $L_W = X^{N/2} + a_W X^{N/4} +$ (terms of degree at most $N/8$). Take $R = X^{N/2}$ and $C_W = L_W - R$, which has degree at most $N/4$. Pole reduction with $K = N/4$ gives common agreement $N/4$ and a challenge $C_W(\beta)$ at agreement $N/2$ for each hyperplane. At rate $1/4$ the Johnson threshold is also about $N/2$. Up to a translation of the challenges, this is the pair of Theorem 4.7, which shows that these $2N - 2$ challenges are distinct and are the only ones at agreement $N/2$.

How close to Johnson a family can get. Suppose the root sets have T points and their locators share all coefficients above degree $T - w$. Pole reduction then works at message length $K = T - w$, and the agreement T reaches the Johnson threshold, approximately $\sqrt{NK}$, only if $T^2 \ge N(T - w)$, that is,

$$\frac{w}{T} \ge 1 - \frac{T}{N}.$$

An affine subspace has $w = T/2$, which meets this bound only for hyperplanes. Unions of smaller affine subspaces, which the decision-tree construction uses to obtain many more sets, have a smaller ratio w/T and

stay well below Johnson. The Gold construction uses polynomials of degree $N/2$ that are not locators, with roots on sets of size just below $N/2$ (Section 2.2). The subspace-locator construction reaches Johnson with smaller subspaces by changing the conversion instead (Section 2.3).

2.2 Construction 1: Gold moments on dense domains

The hyperplanes of the previous example are the only affine subspaces of D with $N/2$ points, and they give only $2N - 2$ challenges. To obtain superpolynomially many just below $N/2$, we need many more agreement sets. We take the *level sets* of quadratic Boolean functions, the sets on which a function $D \to \{0, 1\}$ that is quadratic in binary coordinates (defined below) takes a given value. Let $D \subseteq \mathbb{B} = \mathbb{F}_{2^m}$ be a binary additive subspace of dimension d, put $N = 2^d$ and $K = N/4$, and let $\lambda \neq 0$ be the coefficient of X in L_D. The polynomials are defined over $\mathbb{B}$; challenges may come from a larger field $\mathbb{F} \supseteq \mathbb{B}$.

A word with many close codewords. Squaring is additive and bijective on $\mathbb{B}$. Every element therefore has exactly one square root, and $x \mapsto \sqrt{\lambda x}$ is a word on D. A polynomial C of degree $k \geq 1$ agrees with this word exactly at the roots in D of $C^2 + \lambda X$, a nonzero polynomial of degree $2k$, and hence on at most $2k$ points. Equality holds exactly when $C^2 + \lambda X$ is a scalar multiple of the locator of the agreement set E, that is, when

$$L_E = U^2 + c_E X \qquad \text{for a polynomial } U \text{ and a scalar } c_E \neq 0.$$

In characteristic two, this condition says that L'_E is the nonzero constant c_E. Each such set with $|E| < N/2$ gives the codeword $C_E = \sqrt{\lambda/c_E}\, U$, of degree $|E|/2 < K$, which agrees with the word on all of E. To find many codewords at agreement just below $N/2$, we therefore need many sets of size just below $N/2$ whose locators have constant derivative.

The word is itself a polynomial: on D it equals $R = \sqrt{L_D - \lambda X}$, of degree $N/2$. In the language of Section 2.1, the polynomials $P_E = R + C_E$ vanish on E and share all their coefficients above degree K. On $D = \mathbb{F}_N$ the word is $x^{N/2}$. For example, on $\mathbb{F}_{16}$ the set $E_0 = \{0\} \cup \{x : x^5 = 1\}$ has locator $X^6 + X = (X^3)^2 + X$, and the codeword x^3 therefore agrees with the word x^8 on all six points of E_0.

One pair of inputs for the whole list. Fix $\beta \in \mathbb{F} \setminus D$ and take

$$g(x) = \frac{1}{x - \beta}, \qquad f(x) = \sqrt{\lambda g(x)} = \sqrt{\frac{\lambda}{x - \beta}} \qquad (x \in D).$$

For a challenge z and a polynomial h of degree less than K, put $V = (X - \beta)h + z + \sqrt{\lambda\beta}$, which has degree at most K. Multiplying the equation $f(x) + zg(x) = h(x)$ by $x - \beta$ and squaring shows that it holds exactly when $V(x)^2 = \lambda x$. Hence $f + zg$ agrees with a codeword on T points if and only if some polynomial V of degree at most K, with $V(\beta) = z + \sqrt{\lambda\beta}$, agrees with the word $\sqrt{\lambda x}$ on T points. The exceptional challenges are thus the values at β of the decoding list of this word, translated by $\sqrt{\lambda\beta}$. A set E with $L_E = U^2 + c_E X$ gives $V = C_E$ and the challenge

$$z_E = C_E(\beta) + \sqrt{\lambda\beta} = \sqrt{\lambda L_E(\beta)/c_E}.$$

The inputs share little: $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$ by the argument of Section 2.1, and $\mathrm{agr}_K(f) \leq 3N/8 - 1$ (Lemma 3.13). The first input differs from the one that pole reduction builds from the family $P_E = R + C_E$ by $\sqrt{\lambda\beta}\, g$, which translates every challenge by $\sqrt{\lambda\beta}$.

Sets whose locators have constant derivative. Let $E \subseteq D$ have even size $T < N/2$, and let H be the polynomial of degree less than N that is one on E and zero on $D \setminus E$. It has $N - T$ roots, and hence $\deg H \geq N - T$. If equality holds, then H is a scalar multiple of $L_{D\setminus E}$, and $L_D = \mu H L_E$ for a scalar $\mu \neq 0$. Differentiating gives $\lambda = \mu(H' L_E + H L'_E)$. At every point of E this says $L'_E = \lambda/\mu$, and since $\deg L'_E < T$, the derivative L'_E is constant. We therefore look for sets whose indicator polynomial has the smallest possible degree.

By Newton's identities, L'_E is constant exactly when $\sum_{a\in E} a^j = 0$ for $1 \leq j \leq T - 2$. On a full field, such sets are the supports of minimum-weight codewords of extended binary BCH codes, and many are known to be level sets of quadratic functions [10, 11, 39].

The degree of a polynomial with values in $\{0, 1\}$ on D is controlled by its derivative. Put $\Lambda = L_D/\lambda$, so that $\Lambda' = 1$. Since $H^2 + H$ vanishes on D, we can write $H^2 + H = \Lambda S$ with $\deg S < N$. Differentiating gives $H' = S + \Lambda S'$. Both H' and S have degree less than N, which forces $S' = 0$. Hence

$$H^2 + H = \Lambda H', \qquad \deg H = \frac{N + \deg H'}{2}$$

for every nonconstant such H (compare Borges and Conceição [14, Lemma 4.1] and Lemma 5.6). If H represents a linear function, then H' is constant and $\deg H = N/2$: its level sets are the hyperplanes. The next case is a quadratic function. Its polynomial has derivative J plus a constant, where J is linearized (Lemma 5.6), and $\deg J$ is a power of two. A quadratic function of rank $2t$ has a level set of size $T = N/2 - N/2^{t+1}$, as we show next, and $\deg H = N - T$ then means $\deg J = N/2^t$.

Quadratic functions. Choose a binary basis of D. Each point then has coordinates $x_1, \ldots, x_d \in \mathbb{F}_2$. A *quadratic Boolean function* is a function $\psi : D \to \mathbb{F}_2$ given by a polynomial of degree at most two in these coordinates. Its cross terms $x_i x_j$ with $i < j$ form a symmetric binary matrix A with zero diagonal, the matrix of the bilinear form $\psi(x + y) + \psi(x) + \psi(y) + \psi(0)$. Such a matrix has even rank over $\mathbb{F}_2$, say $2t$. After an affine change of coordinates, ψ is $x_1x_2 + \cdots + x_{2t-1}x_{2t}$ plus a linear function of the other coordinates and a constant. A nonzero linear part makes ψ take each value equally often, and we use the functions without one:

$$\psi(x) = x_1x_2 + x_3x_4 + \cdots + x_{2t-1}x_{2t} + \kappa, \qquad \kappa \in \mathbb{F}_2.$$

Each product is zero on three of the four inputs and one on the fourth. Its number of zeros minus its number of ones, $\sum_{u,v\in\mathbb{F}_2}(-1)^{uv}$, is therefore 2. Multiplying these sums over the t independent pairs and counting the $d - 2t$ unused coordinates gives an absolute difference $2^t 2^{d-2t} = N/2^t$ between the numbers of zeros and ones. Choosing κ makes the ones the smaller class, of size

$$T = \frac{N}{2} - \frac{N}{2^{t+1}}.$$

This set is a union of translates of the subspace where the first $2t$ coordinates vanish, of size $N/2^{2t}$. Increasing t brings T toward $N/2$. The rank alone does not give $\deg J = N/2^t$; the Gold equations select the quadratic functions for which it holds.

The Gold equations. The coefficients of J are $\mathbb{F}_2$-linear in the bits A_{ij}. Requiring the coefficients of J above $X^{N/2^t}$ to vanish therefore gives linear equations on A. On the full field $D = \mathbb{B} = \mathbb{F}_{2^d}$ with $d = 2n$, these equations have a simple meaning. Every quadratic function there is a sum of terms $\mathrm{Tr}(a_i x^{2^i+1})$, where Tr is the trace to $\mathbb{F}_2$, with $1 \leq i \leq n$, plus a linear function and a constant; for $i = n$ the coefficient a_n lies in $\mathbb{F}_{2^n}$ and the trace is taken from $\mathbb{F}_{2^n}$. The polynomial of $\mathrm{Tr}(a_i x^{2^i+1})$ has a derivative whose only terms are X^{2^i} and $X^{2^{d-i}}$ (compare Proposition 5.21). The condition $\deg J \leq N/2^t$ thus says exactly that $a_i = 0$ for $i < t$:

only the exponents $2^i + 1$ with $i \geq t$, studied by Gold [30], remain. On $\mathbb{F}_{16}$ with $t = 2$, these are the functions $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(ax^5)$, and the set E_0 above is where $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(x^5)$ vanishes.

A general additive domain has no multiplication of its own, and we work in coordinates. Represent the coordinate $x \mapsto x_i$ by its linearized polynomial ℓ_i of degree at most $N/2$, and let its *label* ω_i be the square root of the coefficient of X in ℓ_i (Lemma 5.5). On a full field the squares ω_i^2 form the dual basis of the coordinate basis under the pairing $(x, y) \mapsto \mathrm{Tr}(xy)$. Since $\ell_i' = \omega_i^2$, the product rule makes $J = \sum_{i<j} A_{ij}(\omega_i^2 \ell_j + \omega_j^2 \ell_i)$ linearized and linear in A; reducing modulo L_D changes a derivative only by a constant. The equations become

$$M_k(A) := \sum_{i<j} A_{ij}\left(\omega_i \omega_j^{2^k} + \omega_j \omega_i^{2^k}\right) = 0, \qquad k = 1, \ldots, t-1 \tag{2.1}$$

(Lemma 5.8). We call $M_k(A)$ the kth *Gold moment*. For $t = 2$, write $\omega_a = \sum_i a_i \omega_i$ for $a \in \mathbb{F}_2^d$. The function $(a \cdot x)(b \cdot x)$ contributes $\omega_a \omega_b (\omega_a + \omega_b)$, the product of the three nonzero labels in the plane spanned by a and b. When a, b, a', b' are linearly independent, the rank-four function $(a \cdot x)(b \cdot x) + (a' \cdot x)(b' \cdot x)$ therefore solves the equation exactly when its two planes have equal label products. Lemma 5.12 turns each solution of rank $2t$ into 2^{2t} polynomials $P = R + C$ with $\deg C = T/2$, one for each linear part that makes ψ vanish on the kernel of A. Their roots in D are level sets of size T.

Why there are many solutions on dense domains. The unknowns are the $\binom{d}{2}$ bits A_{ij}, and each of the $t - 1$ equations costs at most m bits. At least $2^{\binom{d}{2} - m(t-1)}$ matrices therefore solve them. By the degree count, every nonzero solution has rank at least $2t$, and we need many of rank exactly $2t$. Delsarte and Goethals [22] proved a Singleton-type bound for alternating matrices (symmetric binary matrices with zero diagonal, like A): a linear space of such $d \times d$ matrices whose nonzero members all have rank at least $2t + 2$ has at most $2^{(d-\iota)(n-t)}$ elements, where $n = \lfloor d/2 \rfloor$ and $d - \iota$ is the largest odd integer at most d. Our solution space exceeds this bound by a factor of at least 2^Δ, where $\Delta = m - t(m - d + \iota)$, and therefore contains matrices of rank $2t$ when $\Delta \geq 1$.

A moment identity from the same paper [22, Eq. (29)] turns this excess into a count: at least $(2^\Delta - 1)\begin{bmatrix} n \\ t \end{bmatrix}_4$ such matrices, where the Gaussian binomial counts the t-dimensional subspaces of $\mathbb{F}_4^n$ (Lemma 5.13). Up to the factor $1 - 2^{-\Delta}$, this is the number one expects after imposing $m(t-1)$ random linear conditions on the roughly $2^{2td - 2t^2 - t}$ such matrices of rank $2t$.

Raising t by one adds an equation, costing m bits, and lowers the Singleton bound by $d - \iota$ bits. The net cost $m - d + \iota$ is small only when D fills a constant fraction of $\mathbb{B}$. When D fills at least an eighth of $\mathbb{B}$, we can take t near $d/4$, and the family has $N^{(1/8 - o(1))\log_2 N}$ members at agreement $N/2 - \Theta(N^{3/4})$ (Corollary 5.2). A sparser domain with $m = d + c$ for a constant $c > 3$ needs t near $d/(c+1)$, and the exponent $1/8$ becomes $(c-1)/(c+1)^2$. With $t = d/2 - O(1)$, the family has polynomial size, at agreement $N/2 - O(\sqrt{N})$, but it is large enough to make a constant fraction of a challenge field of polynomial size exceptional (Corollary 5.3).

Distinct challenges. Two sets $E \neq E'$ give the same challenge when C_E and $C_{E'}$ take the same value at β. For a general family this happens at up to K poles per pair (Section 2.1). Two members of the Gold family take the same value at no more than $\delta = N/2^{2t}$ points outside D (Lemma 5.12). Outside D, the identity $P'(P^2 + L_D) = \lambda P$ makes $P(\beta)$ determine $P'(\beta) = U(\beta)/\eta$, where $U^2 = H'$ and η depends only on D. For two members, $U_1 + U_2$ is the 2^{t-1}th power of a nonzero polynomial of degree at most $N/2^{2t}$.

Averaging over poles gives a pole with at least $\frac{1}{2}\min\{|\mathcal{G}|, (q - N)/\delta\}$ distinct challenges, where $\mathcal{G}$ is the Gold family (Lemma 3.19). For $t = d/2 - O(1)$, δ is a constant. When $q \gg N$ and $|\mathcal{G}| \geq q/\delta$, at least about $1/(2\delta)$ of the field is exceptional, approaching $1/\delta$ as $|\mathcal{G}|/q$ grows. On $D = \mathbb{F}_N$ with $q = N^2$, for example, $\delta = 4$ and agreement $N/2 - \sqrt{N}$ has probability at least $1/4 - o(1)$ (Corollary 5.3); the generic bound gives only order $1/N$.

2.3 Construction 2: subspace locators on arbitrary additive domains

Our second construction works directly with subspaces and does not require a dense domain. Subspaces of codimension two give about $N^2/6$ root sets, far more than the hyperplanes, but pole reduction places them below Johnson. We explain why, and how reading the challenge from a coefficient recovers Johnson.

Let D have size $N = 16K$, with $K \geq 2$, and first suppose it lies in a proper subfield $\mathbb{B}$ of the challenge field $\mathbb{F}$. There are $(N-1)(N-2)/6$ subspaces $W \leq D$ of codimension two, meaning dimension two less than D. Each has size $N/4 = 4K$, and its locator is

$$L_W = X^{4K} + a_W X^{2K} + b_W X^K + V_W, \qquad \deg V_W \leq K/2.$$

In pole reduction every varying coefficient belongs to the correction, which here has degree at most $2K$, so we take message length $2K = N/8$. At rate $1/8$ the Johnson threshold is about $0.35N$, well above the agreement $N/4$.

Reading the challenge from a coefficient. Only one varying coefficient lies above degree K, namely a_W. If it becomes the challenge instead of part of the witness, message length K suffices. Since W is a linear subspace, L_W is linearized and has no constant term, and every term is divisible by X. Put

$$f = X^{4K-1}, \qquad g = X^{2K-1}, \qquad H_W = (b_W X^K + V_W)/X.$$

Here f, g denote the evaluations of these polynomials on D; division by X is polynomial division before evaluation, and both words are defined even at $x = 0$. Then H_W has degree less than K, and $f + a_W g - H_W = L_W/X$ vanishes on $W \setminus \{0\}$. As in pole reduction, division by a linear factor turns the family into one pair of inputs. Here the factor is X, whose root lies in D, and we lose that agreement point. In exchange, the challenge is a single coefficient instead of the value of the whole correction, and the message length is half as large. The price appears in the common agreement: g is a polynomial of degree $2K-1$, and $\mathrm{CA}_K(f, g)$ can be as large as $2K-1$ instead of K. Subtracting a polynomial of degree less than K from $g = X^{2K-1}$ leaves a nonzero polynomial of degree $2K-1$, with at most that many roots, and Theorem 4.1 shows that this number of common agreements is attained. At rate $1/16$, the exact Johnson threshold $\sqrt{N(K-1)}$ lies between $N/4 - 3$ and $N/4 - 2$, just below the agreement $N/4 - 1$.

One challenge for two coefficients. The coefficient a_W lies in $\mathbb{B}$ and need not determine W. The pair (a_W, b_W) does determine W. Indeed, two codimension-two subspaces intersect in codimension at most four, and their intersection has at least $N/16 = K$ points. If their locators have the same a_W, b_W, their difference has degree at most $K/2$ and vanishes at all these points. A nonzero polynomial cannot have more roots than its degree, and the locators are therefore equal (Lemma 3.9). To place both coefficients in one challenge, we move a_W into a fixed position. For $v \in D \setminus W$, the locator of the hyperplane $W \cup (W + v)$ is $L_W^2 + L_W(v) L_W$ (Section 3.2). We replace $L_W(v)$ by $a_W^2 + \theta$, the value that makes the coefficient of X^{4K} equal to a fixed $\theta \in \mathbb{F} \setminus \mathbb{B}$:

$$P_W = L_W^2 + (a_W^2 + \theta) L_W = X^{8K} + \theta X^{4K} + z_W X^{2K} + C_W, \qquad z_W = a_W^3 + b_W^2 + \theta a_W, \qquad \deg C_W \leq K.$$

On D, the factor $L_W + a_W^2 + \theta$ takes values in $\mathbb{B} + \theta$ and never vanishes. The roots of P_W in D are therefore exactly the points of W, as for a hyperplane whose second coset lies outside D. The polynomial P_W is again linearized, and the same conversion gives

$$f = X^{8K-1} + \theta X^{4K-1}, \qquad g = X^{2K-1}, \qquad H_W = C_W/X,$$

with $f + z_W g - H_W = P_W/X$. The rate, the agreement $N/4 - 1$ on $W \setminus \{0\}$, and the common agreement $2K - 1$ are as before.

The challenges are distinct because 1 and θ are linearly independent over $\mathbb{B}$. In $z_W = (a_W^3 + b_W^2) + \theta a_W$, the coefficient of θ recovers a_W; the remaining coefficient then recovers b_W^2, and squaring is one-to-one in $\mathbb{B}$. Thus z_W determines a_W, b_W and hence W. If no proper subfield contains D, this argument for distinctness is unavailable. But each pair of subspaces gives the same challenge for at most one choice of θ: equality is a linear equation in θ, or is impossible if the a_W coefficients agree. Averaging these collisions over $\theta \in \mathbb{F}$ gives at least $\lceil qM/(q + M - 1) \rceil$ distinct challenges, where $M = (N - 1)(N - 2)/6$ and $q = |\mathbb{F}|$ (Corollary 4.2).

Higher counts and arbitrary rates. For fixed s, subspaces of codimension s provide a number of root sets proportional to N^s, with constants depending on s. A similar cancellation encodes their first s coefficients into one challenge. It uses $P_W = A_W(L_W)$, where A_W is a linearized polynomial of degree 2^{s-1} chosen so that all coefficients of P_W above degree $2K$ are the same for every W. For $s = 2$, $A_W(Y) = Y^2 + (a_W^2 + \theta)Y$ gives the polynomial P_W above. The encoding is one-to-one when the challenge field has degree at least $s + 1$ over a field containing D; otherwise the averaging argument above bounds the collisions. Increasing s gives larger counts at lower agreement fractions (Lemma 4.3). To reach other rates, we build such a pair on a smaller subspace and multiply its inputs and witnesses by a vanishing polynomial, adding a fixed set of agreement points. This preserves a positive common-agreement gap while setting the desired rate.

Here M denotes the number of root sets in this higher-codimension family. If the challenge field has size $q \le N^a$ for a fixed exponent a, choosing $s > 2a$ makes $M > (q - 1)^2$ for all sufficiently large N. The same collision-counting argument gives more than $q - 1$ distinct challenges, since $qM/(q + M - 1) > q - 1$. Every element of the field is therefore a challenge. Combining this choice with the preceding multiplication step gives, at every fixed rate, a pair for which every challenge is exceptional, with a fixed positive common-agreement gap (Theorem 4.5). The gap depends on the rate and a; it need not be close to Johnson.

2.4 Construction 3: decision trees for sparse domains

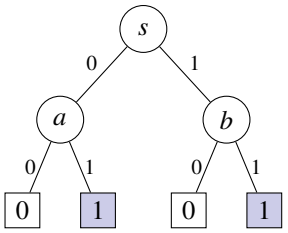
Decision trees give much larger families on sparse domains: different branches of a tree test different linear functions $D \to \mathbb{F}_2$. A point $x \in D$ follows a branch according to whether each tested function is zero or one at x; the final output is also zero or one. A leaf represents all points following one path. Its tests are linear equations, and that set is therefore an affine subspace. We use the points with output one as the root set.

Branching creates more choices. For example, choose three independent binary linear functions s, a, b on D. Test s first; if it is zero, output a, and otherwise output b. The set on which this rule outputs one is

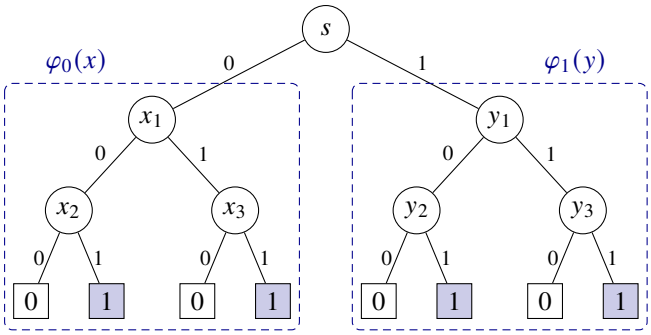
$$A = \{x \in D : s(x) = 0,\ a(x) = 1\} \cup \{x \in D : s(x) = 1,\ b(x) = 1\}.$$

Each part is an affine subspace of size $N/4$. The parts are disjoint, and $|A| = N/2$. Each path uses two tests, although the tree uses three independent functions (Figure 2).

For $h \ge 2$, a full tree of height h makes h tests on each path and uses $2^h - 1$ linear functions altogether. As in the example, its output is the value of the last tested function; more generally, each branch may output that value or its complement. We require all these functions to be linearly independent, which is possible when $\dim_{\mathbb{F}_2} D \ge 2^h - 1$. Every path fixes h independent bits, leaving $N/2^h$ points. Half of the 2^h leaves output one. The root set A is thus a union of 2^{h-1} disjoint affine subspaces and has size $N/2$. The count of distinct sets, rather than just distinct choices of tests, is $\Theta_h(N^{2^h-1})$ (Lemma 6.6). Different trees can give the same set, but only in a bounded number of ways: the set determines the span of the tested functions, and for $h \ge 3$ it determines the root test and the two subtrees, while for $h = 2$ the ambiguity is a fixed constant. The point of branching is this difference between the path length h, which controls leaf size, and the number $2^h - 1$ of functions, which controls the count.



height 2: paths test 2 functions, the tree uses 3



height 3: paths test 3 functions, the tree uses 7

Figure 2: Decision trees of heights two and three. Each circle tests one binary linear function on D, and all functions appearing in a tree are linearly independent. A point of D follows one path from the root, and the support A consists of the points that reach a shaded leaf. Every leaf is an affine subspace cut out by the tests on its path: at height h it has $N/2^h$ points, and the 2^{h-1} shaded leaves together contain $N/2$ points. The whole tree uses $2^h - 1$ independent functions. The dashed boxes mark the two children in the recursion $\varphi = (1 + s)\varphi_0(x) + s\varphi_1(y)$.

Large leaves give the shared coefficients. Each output-one leaf has a locator with leading term $X^{N/2^h}$ and remaining degree at most $N/2^{h+1}$. Since these leaves are disjoint, multiplying their locators gives the locator of A. The product of their leading terms is $X^{N/2}$. Every other term uses a lower-degree term from at least one factor, reducing the degree by at least $w = N/2^{h+1}$. Hence

$$L_A = X^{N/2} + C_A, \qquad \deg C_A \le N/2 - w.$$

Pole reduction now gives agreement $N/2$ at message length $K_0 = N/2 - w$. Distinct sets give distinct locators, and the generic collision bound from Section 2.1 converts their count into a count of challenges. Unlike the Gold construction, this argument needs no density assumption.

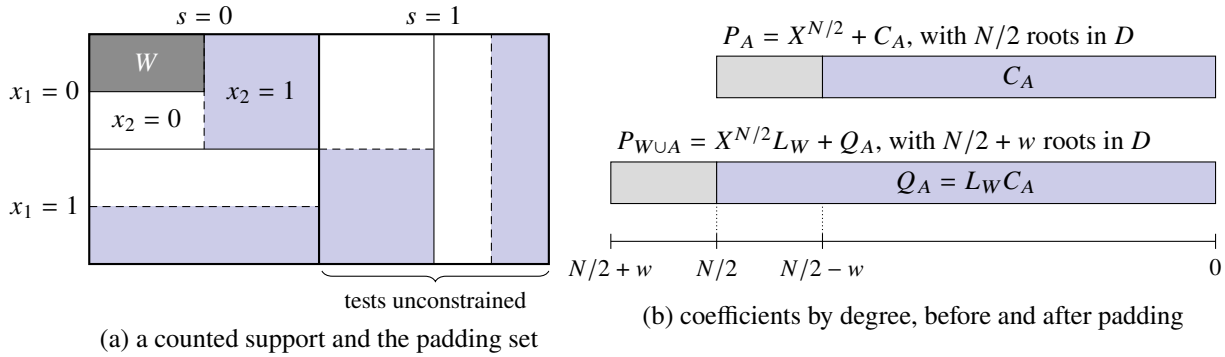
The degree gap uses only that A is a disjoint union of affine subspaces of one size, and trees produce many such unions. Two affine subspaces are disjoint exactly when some linear test is constant on each of them, with different values. In a tree, the test where two paths split separates their leaves, and each test separates many pairs of leaves at once. For two affine subspaces of codimension two, every disjoint union is either the root set of a height-two tree or an affine hyperplane.

Reaching rate one half. If we simply increased the message length to $N/2$, interpolation would make the common agreement at least $N/2$, erasing the gap above it. Instead, we add agreement points while raising the rate. Fix a subspace $W \le D$ of size w, retain sets A disjoint from W, and multiply the inputs and witnesses by L_W. At every point of W, both multiplied inputs and every multiplied witness are zero, which gives w new agreement positions, while multiplication raises the witness degree by w. The new parameters are

$$K = K_0 + w = N/2, \qquad T = N/2 + w,$$

with common agreement exactly K. The argument is that of Section 2.1, with $(X - \beta)h - L_W$ in place of $(X - \beta)h - 1$; its value at β is $-L_W(\beta) \neq 0$.

To ensure that A avoids W, require all h tests on the all-zero path to vanish on W, and let that path output the value of its last test (Figure 3). Every point of W then follows that path and receives output zero. The other tests remain free, subject to linear independence. Since W has codimension $h + 1$, there are only 2^{h+1} linear functions vanishing on it, instead of N linear functions on D. Restricting h tests therefore costs a factor



(a) a counted support and the padding set

(b) coefficients by degree, before and after padding

Figure 3: Padding to rate $1/2$. (a) The padding set W is a fixed linear subspace with w points. In the family we count, the functions tested along the all-zero path vanish on W, so W is half of the rejected leaf at the end of that path and every shaded leaf avoids it. The tests on all other branches are unconstrained. (b) Multiplying by L_W adds the w roots in W and raises every degree by at most w. The shared coefficients move from the degrees above $N/2 - w$ to the degrees above $N/2$, where they are those of the fixed polynomial $X^{N/2}L_W$. The message length rises from $N/2 - w$ to $N/2$ and the agreement from $N/2$ to $N/2 + w$, so the gap of w positions between common agreement and the agreement of the combinations is preserved at rate exactly $1/2$.

of order N^h for fixed h. The resulting number of distinct sets is $\Theta_h(N^{2^h-h-1})$. After discarding colliding challenges, Theorem 6.10 gives

$$\Omega_h\big(\min\{N^{2^h-h-1}, q/N\}\big)$$

exceptional challenges at agreement fraction $1/2 + 2^{-h-1}$, where q is the challenge-field size. The minimum reflects collisions: a family much smaller than q/N loses few challenges to them, and a larger one still gives on the order of q/N.

After these restrictions, height three gives a family of order N^4 at agreement $9/16$; height four gives order N^{11} at agreement $17/32$. Thus taller trees give larger families while bringing the combination agreement closer to the common agreement $1/2$.

3 Notation and common tools

This section fixes notation and proves the tools shared by Sections 4 to 6. Only the Gold construction uses Section 3.4.

3.1 Notation and agreement

All fields in this paper are finite. Throughout this section, let $\mathbb{F}$ be a field, let $D \subseteq \mathbb{F}$ have size $N \geq 2$, and fix a message length $1 \leq K < N$. Most constructions use characteristic two; Section 5.9 also treats other characteristics.

Definition 3.1 (Reed–Solomon code and received words)**.** The *Reed–Solomon code* on D with message length K is

$$C_K(D;\mathbb{F}) = \{(P(x))_{x\in D} : P \in \mathbb{F}[X],\ \deg P < K\}.$$

Its length is N, its message length (dimension) is K, and its *rate* is $\rho = K/N$. A *received word* is any function $f : D \to \mathbb{F}$, without a promise that it belongs to $C_K(D;\mathbb{F})$.

We measure agreement in numbers of coordinates.

Definition 3.2 (Individual and common agreement)**.** For received words $f, g : D \to \mathbb{F}$, their *individual agreement* and *common agreement* with the code are

$$\mathrm{agr}_K(f) = \max_{\substack{F \in \mathbb{F}[X] \\ \deg F < K}} |\{x \in D : f(x) = F(x)\}|,$$

$$\mathrm{CA}_K(f, g) = \max_{\substack{F, G \in \mathbb{F}[X] \\ \deg F, \deg G < K}} |\{x \in D : f(x) = F(x),\ g(x) = G(x)\}|.$$

The corresponding *agreement fractions* are $\mathrm{agr}_K(f)/N$ and $\mathrm{CA}_K(f, g)/N$. The relative Hamming distance of f to the code is $1 - \mathrm{agr}_K(f)/N$. The *two-word interleaved code* consists of the words $x \mapsto (c_1(x), c_2(x))$ with $c_1, c_2 \in C_K(D; \mathbb{F})$, viewed over alphabet $\mathbb{F}^2$.

The two input words are chosen before the challenge is sampled.

Definition 3.3 (Received line and exceptional challenges)**.** For fixed *inputs* $f, g : D \to \mathbb{F}$, the *received line* is $\{f + zg : z \in \mathbb{F}\}$. The scalar z is called a *challenge*. At an integer agreement threshold T, define

$$\mathrm{Bad}_T(f, g) = \{z \in \mathbb{F} : \mathrm{agr}_K(f + zg) \geq T\}.$$

Its elements are the *exceptional challenges* at threshold T. Their *exceptional probability* under uniform sampling is $|\mathrm{Bad}_T(f, g)|/|\mathbb{F}|$.

We use this set as a counterexample when $T > \mathrm{CA}_K(f, g)$. Its size counts distinct challenges for one fixed received pair, even if several polynomials explain the same combination. Mutual correlated agreement at threshold T requires that, outside a small set of challenges, f and g agree with codewords on the very set where $f + zg$ does. In particular it requires $\mathrm{CA}_K(f, g) \geq T$ as soon as one such challenge exists. So when $T > \mathrm{CA}_K(f, g)$, every challenge in $\mathrm{Bad}_T(f, g)$ violates this conclusion, and it also violates the weaker conclusion that f and g agree with codewords on some common set of size T. List decoding counts a different object: distinct codewords close to one fixed word.

Definition 3.4 (Explaining polynomials, witnesses, and decoding lists)**.** An *explaining polynomial* for a word f on a set $A \subseteq D$ is a polynomial $H \in \mathbb{F}[X]$ with $\deg H < K$ and $H(x) = f(x)$ for all $x \in A$. A *witness* for $z \in \mathrm{Bad}_T(f, g)$ is an explaining polynomial for $f + zg$ on at least T coordinates. The *decoding list* of f at threshold T is

$$\mathcal{L}_T(f) = \{c \in C_K(D; \mathbb{F}) : |\{x \in D : f(x) = c(x)\}| \geq T\}.$$

Its *list size* is $|\mathcal{L}_T(f)|$.

Since $K < N$, distinct polynomials of degree less than K give distinct codewords. Thus counting polynomials in a decoding list is equivalent to counting its codewords.

Definition 3.5 (Agreement thresholds and gaps)**.** At rate $\rho = K/N$, the *Johnson agreement threshold* is $\sqrt{N(K-1)}$ coordinates, with limiting agreement fraction $\sqrt{\rho}$. We call ρ the *capacity threshold* in agreement fraction. For an agreement target T, its *Johnson deficit* is $\sqrt{\rho} - T/N$. It is measured against the limiting fraction $\sqrt{\rho}$, not against the exact finite threshold. For inputs f, g, the *common-agreement gap* at this target is

$$\frac{T - \mathrm{CA}_K(f, g)}{N}.$$

An input f is *individually far* at threshold T if $\mathrm{agr}_K(f) < T$.

The common-agreement gap. Put $C = \mathrm{CA}_K(f, g)$. The distance of (f, g) to the interleaved code is $1 - C/N$, whereas a combination agreeing on T coordinates has distance at most $1 - T/N$. Such a combination exceeds the proximity loss ϵ^* of the formulation of Ben-Sasson, Carmon, Haböck, Kopparty, and Saraf [6, Definition 1.1] whenever

$$\epsilon^* < \frac{T - C}{N}.$$

This is a different quantity from the Johnson deficit $\sqrt{\rho} - T/N$. A large exceptional set with only one coordinate between T and C does not exclude a fixed positive fractional loss.

Field and polynomial notation. We write $\mathbb{B}$ for a field containing the domain before extending the challenge field to $\mathbb{F}$. For $\mathbb{B} = \mathbb{F}_{b^m}$, the field trace to $\mathbb{F}_b$ is $\mathrm{Tr}_{\mathbb{B}/\mathbb{F}_b}(x) = \sum_{i=0}^{m-1} x^{b^i}$. We write $\mathrm{lc}(P)$ for the leading coefficient of a nonzero polynomial P.

Definition 3.6 (Canonical polynomial representative)**.** For a function $u : \mathbb{B} \to \mathbb{B}$ on a finite field $\mathbb{B}$, its *canonical representative* is the unique polynomial $H \in \mathbb{B}[X]$ of degree less than $|\mathbb{B}|$ with $H(x) = u(x)$ for all $x \in \mathbb{B}$. If P is any polynomial representing u on $\mathbb{B}$, then H is its remainder modulo $X^{|\mathbb{B}|} - X$. More generally, for a function $u : D \to \mathbb{B}$ on a subset $D \subseteq \mathbb{B}$, its canonical representative is the unique polynomial of degree less than $|D|$ that agrees with u on D; it is the remainder modulo the vanishing polynomial $\prod_{x \in D}(X - x)$ of any polynomial representing u on D.

This reduction preserves values on $\mathbb{B}$, but can change values in an extension field. When evaluating outside $\mathbb{B}$, we always use the specified polynomial representative. Subscripts on asymptotic notation indicate parameters on which the implicit constants may depend; the variable tending to infinity is the code length. Table 2 collects the symbols that keep one meaning throughout the paper.

Gaussian binomial coefficients. For a prime power q and integers $a \geq 0$ and b, the *Gaussian binomial coefficient* $\begin{bmatrix} a \\ b \end{bmatrix}_q$ is the number of b-dimensional subspaces of $\mathbb{F}_q^a$. It is zero when $b < 0$ or $b > a$, and otherwise

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{i=0}^{b-1} \frac{q^{a-i} - 1}{q^{b-i} - 1}.$$

The subscript is the size of the field over which dimensions are counted, so $\begin{bmatrix} a \\ b \end{bmatrix}_4$ counts subspaces over $\mathbb{F}_4$. We use four consequences of the product formula.

- *Size.* Let $0 \leq b \leq a$. Each factor is at least q^{a-b}, and $\prod_{j \geq 1}(1 - q^{-j})^{-1} < 4$, so

$$q^{b(a-b)} \leq \begin{bmatrix} a \\ b \end{bmatrix}_q < 4\, q^{b(a-b)}.$$

  Thus $\log_q \begin{bmatrix} a \\ b \end{bmatrix}_q = b(a - b) + O(1)$, with an absolute constant.

- *Symmetry.* $\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{bmatrix} a \\ a-b \end{bmatrix}_q$.

- *Removing one dimension.* For $0 \leq b < a$,

$$\frac{q^{a-b} - 1}{q^a - 1} \begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{bmatrix} a - 1 \\ b \end{bmatrix}_q.$$

- *Small cases over* $\mathbb{F}_2$. With $N = 2^d$,

$$\begin{bmatrix} d \\ 1 \end{bmatrix}_2 = N - 1, \qquad \begin{bmatrix} d \\ 2 \end{bmatrix}_2 = \frac{(N-1)(N-2)}{6}, \qquad \begin{bmatrix} d \\ 3 \end{bmatrix}_2 = \frac{(N-1)(N-2)(N-4)}{168}.$$

Symbol	Meaning
$\mathbb{F}$, q	Challenge field and its size; all words take values in $\mathbb{F}$
$\mathbb{B}$	Field containing the domain, before any extension to $\mathbb{F}$
D, N, d	Evaluation domain, its size, and its dimension when D is additive
K, ρ	Message length (degrees are less than K) and rate K/N
T, α	Agreement threshold for the combination, in coordinates and as a fraction
agr_K, CA_K, γ	Individual agreement, common agreement, and (in the summary tables) the common-agreement fraction $\mathrm{CA}_K(f,g)/N$
$\mathrm{Bad}_T(f,g)$, z	Exceptional challenges at threshold T; a challenge
$\begin{bmatrix} a \\ b \end{bmatrix}_q$	Number of b-dimensional subspaces of $\mathbb{F}_q^a$ (Gaussian binomial coefficient)
L_S	Locator of a finite set S
λ, λ_0	The constant derivative L'_D of the locator of an additive domain
β	Pole outside the domain in a received pair $R(x)/(x-\beta)$, $1/(x-\beta)$
R, C_i	Common part and distinct low-degree parts of the polynomials $R + C_i$
w	Number of padded coordinates; for decision trees, also the degree gap $N/2^{h+1}$ of the same size

Table 2: Notation used throughout. Other letters are local to the statement or proof that introduces them.

3.2 Additive locators and pole reduction

We recall the properties of subspace locators behind the shared high-degree coefficients of our constructions.

Definition 3.7 (Additive domains and affine flats)**.** In characteristic two, a *binary additive domain* is a vector subspace of $\mathbb{F}$ over $\mathbb{F}_2$. Its dimension is measured over $\mathbb{F}_2$. An *affine flat* is a translate of a linear subspace; an *affine domain* is such a flat used as the evaluation domain. More generally, when $\mathbb{F}_b \subseteq \mathbb{F}$, an affine $\mathbb{F}_b$-space is a translate of an $\mathbb{F}_b$-linear subspace of $\mathbb{F}$.

Definition 3.8 (Locators and linearized polynomials)**.** For a finite set $S \subseteq \mathbb{F}$, its *locator*, or vanishing polynomial, is

$$L_S(X) = \prod_{x \in S} (X - x).$$

In characteristic two, a *binary linearized polynomial* is a polynomial of the form $L(X) = \sum_i a_i X^{2^i}$ with $a_i \in \mathbb{F}$. We call a polynomial *additive* if it satisfies the polynomial identity $L(X+Y) = L(X) + L(Y)$.

The locator is monic and has exactly the points of S as its roots, each with multiplicity one. As discussed in the technical overview (Section 2.1), the locator L_W of a binary linear space W is linearized [9]. To see this, build W one basis vector at a time. The locator of $\{0\}$ is X. If L_W is linearized and $v \notin W$, then the locator of $W \cup (W + v)$ is

$$L_W(X)\, L_W(X+v) = L_W(X)^2 + L_W(v)\, L_W(X),$$

and squares and scalar multiples of linearized polynomials are linearized. Every binary linearized polynomial is additive, since taking a power of two commutes with addition in characteristic two. Translating W changes only the constant term of its locator. An affine flat of size 2^r with $r \geq 1$ therefore has locator X^{2^r} plus terms of degree at most 2^{r-1}. Its roots are simple, so its derivative is a nonzero constant c; every exponent other than one is even, so adding cX gives the square of a polynomial of degree 2^{r-1}.

Section 4 uses two further facts about locators.

Lemma 3.9 (Leading coefficients determine the subspace)**.** Let D be a binary additive domain of dimension d, and let $s \geq 1$ with $d \geq 2s$. For a subspace $W \leq D$ of codimension s, write

$$L_W = X^{2^{d-s}} + \sum_{i=1}^{d-s} a_i(W)\, X^{2^{d-s-i}}.$$

Then W is determined by $a_1(W), \ldots, a_s(W)$.

Proof. Let W, W' have the same first s coefficients. If $d = 2s$, these are all the coefficients, so $L_W = L_{W'}$. If $d > 2s$, the difference $L_W - L_{W'}$ has degree at most 2^{d-2s-1} and vanishes on $W \cap W'$, which has codimension at most $2s$ in D and hence at least 2^{d-2s} points. The difference is therefore zero. In both cases $W = W'$. □

Lemma 3.10 (Inner polynomials of additive compositions)**.** Let $L, A, P \in \mathbb{F}[X]$ satisfy $L = A \circ P$, that is, $L(X) = A(P(X))$. If L and A are additive, $A \neq 0$, and $P(0) = 0$, then P is additive. In particular, the roots of P in $\mathbb{F}$ form an additive subgroup.

Proof. Put $\Phi(X, Y) = P(X+Y) - P(X) - P(Y)$. Since L and A are additive, $A(\Phi) = 0$. If Φ were nonconstant, the highest-degree term of $A(\Phi)$ could not cancel. Thus Φ is constant, and $\Phi(X, 0) = -P(0) = 0$ makes it zero. □

We also apply Lemma 3.10 to the locator of an affine flat, after subtracting the constant terms of L and P.

The next lemma is the *pole reduction* of Section 2.1. Division by a linear factor in this way also appears in the work of Ben-Sasson, Carmon, Haböck, Kopparty, and Saraf [6, Section 6] and Crites and Stewart [19, Theorem 2].

Lemma 3.11 (From common high coefficients to a received line)**.** Let $1 \leq K < N$, and suppose $R + C_i \in \mathbb{F}[X]$, for i in a nonempty index set, have at least T roots on D, where the C_i are distinct and $\deg C_i \leq K$. For any $\beta \in \mathbb{F} \setminus D$, put

$$f(x) = \frac{R(x)}{x - \beta}, \qquad g(x) = \frac{1}{x - \beta}, \qquad z_i = C_i(\beta), \qquad H_i(X) = -\frac{C_i(X) - C_i(\beta)}{X - \beta}.$$

Then $\deg H_i < K$ and $f + z_i g$ agrees with H_i on at least T coordinates. Moreover $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$. If each $R + C_i$ has degree $T > K$ and all its roots lie in D, one may instead take

$$\widetilde{f}(X) = \frac{R(X) - R(\beta)}{X - \beta}, \qquad \widetilde{z}_i = (R + C_i)(\beta).$$

The same witnesses and common-agreement bound apply, every $\widetilde{z}_i$ is nonzero, and $\mathrm{agr}_K(\widetilde{f}) \leq T - 1$.

More generally, for $1 \leq J < N$ and a polynomial A with $\deg A \leq J$ and $A(\beta) \neq 0$, the word $g_A(x) = A(x)/(x - \beta)$ satisfies $\mathrm{agr}_J(g_A) = \mathrm{CA}_J(u, g_A) = J$ for every received word u.

Proof. The numerator defining H_i vanishes at β, and at every $x \in D$,

$$f(x) + z_i\, g(x) - H_i(x) = \frac{R(x) + C_i(\beta) + C_i(x) - C_i(\beta)}{x - \beta} = \frac{R(x) + C_i(x)}{x - \beta}.$$

If g agrees with a polynomial G of degree less than K, the agreement points are roots of $(X - \beta)G - 1$. This polynomial is nonzero, has degree at most K, and takes value -1 at β. It has at most K roots. Interpolating both words on any K points gives equality for common agreement as well as individual agreement. For the second pair, $\widetilde{f} + \widetilde{z}_i g = f + z_i g$. The challenges $\widetilde{z}_i$ are nonzero since $\beta \notin D$, and $\widetilde{f}$ is a polynomial of degree $T - 1 \geq K$. Its difference from any codeword polynomial therefore has at most $T - 1$ roots. Finally, if g_A agrees with a polynomial h of degree less than J, the agreement points are roots of $(X - \beta)h - A$. This polynomial has degree at most J and takes the nonzero value $-A(\beta)$ at β, so it has at most J roots. Interpolating u and g_A on any J points gives both equalities. □

3.3 Individual agreement bounds

A bound on common agreement limits the positions where both inputs can be explained at once. It need not limit either input on its own. We give two ways to obtain individual bounds: change the pair after extending the field, or bound the inputs directly in the existing field.

Lemma 3.12 (Equal individual and common agreement)**.** Let $f, g : D \to \mathbb{F}_0$, where $D \subseteq \mathbb{F}_0$, put $C = \mathrm{CA}_K(f, g)$, and choose $s \in \mathbb{F} \setminus \mathbb{F}_0$ in a proper finite extension. The pair

$$F = f + sg, \qquad G = f + (s+1)g$$

satisfies $\mathrm{agr}_K(F) = \mathrm{agr}_K(G) = \mathrm{CA}_K(F, G) = C$. For $T > C$, every old exceptional challenge $y \in \mathbb{F}_0$ gives the distinct nonzero exceptional challenge

$$z = \frac{y - s}{s + 1 - y}.$$

These are all the exceptional challenges except possibly $z = -1$, which is exceptional exactly when $\mathrm{agr}_K(g) \geq T$.

Proof. Since f and g take values in $\mathbb{F}_0$, we can expand an explaining polynomial over $\mathbb{F}$ in a basis over $\mathbb{F}_0$ beginning with $1, z$, for $z \notin \mathbb{F}_0$. Taking the coefficients of these two basis elements gives

$$\mathrm{agr}_{K,\mathbb{F}}(f + zg) = \mathrm{CA}_{K,\mathbb{F}_0}(f, g). \tag{3.1}$$

An explaining polynomial for $f + zg$ projects to explaining polynomials for f and g on the same set; conversely, two such polynomials combine. Apply (3.1) with challenges s and $s + 1$ to obtain $\mathrm{agr}_K(F) = \mathrm{agr}_K(G) = C$. Explaining polynomials over $\mathbb{F}_0$ for f and g on a common set of C positions combine into explaining polynomials for F and G on that set, so $\mathrm{CA}_K(F, G) \geq C$, and $\mathrm{CA}_K(F, G) \leq \mathrm{agr}_K(F) = C$. The challenge map is injective and nonzero, and

$$F + zG = \frac{f + yg}{s + 1 - y}.$$

For any $z \neq -1$, write $F + zG = (1 + z)(f + yg)$ with $y = s + z/(1 + z)$. If $y \in \mathbb{F}_0$, projection preserves the old agreement; otherwise (3.1) gives agreement exactly C. The remaining case is $F - G = -g$. □

A quadratic extension suffices, but the exceptional probability is at most $(|\mathbb{F}_0| + 1)/|\mathbb{F}|$. For pole constructions on additive domains, we avoid this cost by changing the first input within the same field, which translates the exceptional set and preserves its size (Lemma 3.13). The binary case of that lemma gives the individual bound in the Binius64 example, including after multiplication by a polynomial to add agreement points. This multiplication is called *padding* (Section 3.5).

A prime denotes the formal derivative. In the lemma, b is a power of the characteristic, so taking a bth power is a bijection on the finite field; $c^{1/b}$ denotes its unique bth root. The locator of an affine $\mathbb{F}_b$-space is a constant plus terms with exponents $1, b, b^2, \ldots$, so its derivative is a nonzero constant λ. Removing λX leaves only exponents divisible by b; taking roots of the coefficients then defines the polynomial $(L_D - \lambda X)^{1/b}$.

At a point $x \in D$ this polynomial takes the value $(-\lambda x)^{1/b}$. A polynomial C of degree $m \geq 1$ therefore agrees with it on at most bm points of D: the polynomial $C^b + \lambda X$ vanishes at every such point, has degree bm, and is nonzero because every exponent of C^b is divisible by b. At rate $1/b^2$, agreement equal to b times the message length is N/b, the asymptotic Johnson value; the exact threshold is $\sqrt{N(N/b^2 - 1)}$. This explains the rates $1/b^2$: the constructions below approach agreement fraction $1/b = \sqrt{\rho}$ from below.

Lemma 3.13 (Two individually far inputs)**.** Let b be a prime power, let $\mathbb{F} \supseteq \mathbb{F}_b$ be finite, and let $D \subseteq \mathbb{F}$ be an affine $\mathbb{F}_b$-space of size $N = b^d$, with $d \geq 3$. Put $K = N/b^2$, $\lambda = L'_D$, and $R = (L_D - \lambda X)^{1/b}$. For any $\beta \in \mathbb{F} \setminus D$, the pair

$$f(x) = \frac{(-\lambda(x-\beta))^{1/b}}{x-\beta}, \qquad g(x) = \frac{1}{x-\beta}$$

satisfies

$$\operatorname{agr}_K(f) \leq \frac{(b+1)K}{2} - 1, \qquad \operatorname{agr}_K(g) = \operatorname{CA}_K(f,g) = K.$$

Replacing the first word of Lemma 3.11, with this R, by f translates its challenge set by $-(\lambda\beta)^{1/b}$. The number of exceptional challenges is unchanged, and zero is not exceptional when $T \geq (b+1)K/2$. For $b = 2$, the first input is $f(x) = \sqrt{\lambda/(x-\beta)}$ and its bound is $3N/8 - 1$. In this binary case, let A be any polynomial of degree w with $A(\beta) \neq 0$ and $3w \leq K - 1$. At the same message length K, the padded pair also satisfies

$$\operatorname{agr}_K(Af) \leq \lfloor (3K + w - 1)/2 \rfloor, \qquad \operatorname{agr}_K(Ag) = \operatorname{CA}_K(Af, Ag) = K.$$

Proof. Lemma 3.11 already bounds the agreement of g and the common agreement. For f, we construct a nonzero polynomial in which every agreement point is a double root. Its degree then bounds twice the number of agreements. Put $S = R + (\lambda\beta)^{1/b}$. On D, we have $S(x)^b = -\lambda(x-\beta)$, so $f(x) = S(x)/(x-\beta)$. For a polynomial h of degree less than K, its agreements with f are the roots on D of

$$P = S - (X-\beta)h.$$

This is monic of degree $bK = N/b$, with lower terms of degree at most K. A root bound on P alone would be too large. To obtain the double roots, set

$$Q = P^b - L_D, \qquad \Omega = P'Q + \lambda P.$$

Since $S^b = L_D - \lambda(X-\beta)$, the entire L_D contribution cancels:

$$Q = -\lambda(X-\beta) - (X-\beta)^b h^b, \qquad \deg Q \leq bK.$$

The derivative of S is constant, since its terms have exponents $0, 1, b, b^2, \ldots$. The term of degree K in $(X-\beta)h$ has zero derivative, since the characteristic divides K. Hence $\deg P' \leq K - 2$ and $\deg \Omega \leq (b+1)K - 2$. Also $Q' = -\lambda$ gives $\Omega' = P''Q$. At every agreement point $P = L_D = 0$, both Ω and Ω' vanish. Each such point is therefore a double root. But $P(\beta)^b = L_D(\beta) \neq 0$, so $\Omega(\beta) = \lambda P(\beta) \neq 0$. Hence Ω is nonzero and has at most $\deg \Omega/2 \leq (b+1)K/2 - 1$ distinct agreement points. This proves the individual bound for f. Finally $f(x) = R(x)/(x-\beta) + (\lambda\beta)^{1/b} g(x)$ on D proves the challenge shift.

For the binary padding assertion, we use the same double-root argument after accounting for the multiplier A. Put $F = AS - (X-\beta)h$, $Q = F^2 + A^2 L_D$, and $D_0 = AF' - A'F$. Since S' is constant,

$$D_0 = A^2 S' - A\big(h + (X-\beta)h'\big) + A'(X-\beta)h, \qquad \deg D_0 \leq w + K - 1.$$

The last bound uses $\deg h < K$ and $2w \leq w + K - 1$. Every second derivative is zero in characteristic two, so $D'_0 = 0$ without any restriction on A'. Also $Q = \lambda A^2(X-\beta) + (X-\beta)^2 h^2$, so $\deg Q \leq 2K$ and $Q' = \lambda A^2$. Thus

$$\Omega = D_0 Q + \lambda A^3 F$$

has derivative zero and degree at most $\max\{w + 3K - 1, N/2 + 4w\} \leq w + 3K - 1$. Every agreement point is a root of Ω, hence a double root, whereas $\Omega(\beta) = \lambda A(\beta)^4 S(\beta) \neq 0$. This gives at most $\lfloor (w + 3K - 1)/2 \rfloor$ agreement points, as claimed. An explaining polynomial h for Ag gives roots of $A - (X-\beta)h$, a nonzero polynomial of degree at most K. Interpolation again gives both equalities. □

3.4 Boolean polynomials and witnesses

The Gold construction in Lemma 5.12 first produces polynomials taking only the values zero and one on the domain, with a controlled derivative. The following conversion turns their complementary root sets into witnesses for one fixed received pair, separating this step from counting the polynomials.

Definition 3.14 (Boolean functions, supports, and balance)**.** Let U be a finite binary vector space. A *Boolean function* on U is a map $\varphi : U \to \mathbb{F}_2$. Its *support* is $\operatorname{supp}(\varphi) = \{x \in U : \varphi(x) = 1\}$. It is *balanced* if $|\operatorname{supp}(\varphi)| = |U|/2$. When $\mathbb{F}$ has characteristic two and $U \subseteq \mathbb{F}$, a *Boolean polynomial* on U is a polynomial in $\mathbb{F}[X]$ whose values on U lie in $\mathbb{F}_2$.

The coefficients of a Boolean polynomial need not lie in $\mathbb{F}_2$. The condition concerns its values on the domain. For the Gold construction, we also use the degree of a Boolean function in binary coordinates, which is different from the degree of its univariate representative.

Definition 3.15 (Quadratic Boolean functions and polar forms)**.** A Boolean function $\psi : U \to \mathbb{F}_2$ is *quadratic* if, in binary linear coordinates $x_1, \dots, x_d$, it can be written as

$$\psi(x) = c + \sum_i b_i x_i + \sum_{i<j} a_{ij} x_i x_j, \qquad c, b_i, a_{ij} \in \mathbb{F}_2.$$

Its *polar form* is the bilinear form

$$B_\psi(x, y) = \psi(x + y) + \psi(x) + \psi(y) + \psi(0).$$

The *polar radical* is $\operatorname{rad}(B_\psi) = \{u \in U : B_\psi(x, u) = 0 \text{ for all } x \in U\}$. The *polar rank* is the rank of the matrix $(B_\psi(e_i, e_j))_{i,j}$ in any basis of U. An *alternating binary matrix* is a symmetric matrix over $\mathbb{F}_2$ with zero diagonal.

The polar matrix is alternating, so its rank is even. The rank and radical do not depend on the chosen basis. In coordinates the polar radical is the null space of the polar matrix, so it has $|U|/2^r$ elements when the polar rank is r. A vector u lies in it exactly when $\psi(x + u) + \psi(x)$ does not depend on x. In suitable coordinates, the polar radical is spanned by the coordinate directions that occur in no cross term of ψ. If ψ is moreover constant on the polar radical, then ψ is constant on each of its cosets, and every level set of ψ is a union of such cosets. Unless specified otherwise, the radical in our binary Gold construction means this polar radical; ψ need not vanish on it.

Lemma 3.16 (From Boolean polynomials to witnesses)**.** Let D be binary additive of size $N \geq 8$ in a finite field $\mathbb{B}$, put $K = N/4$ and $\lambda = L'_D$, and fix $\beta \in \mathbb{F} \setminus D$ in a finite extension. Suppose $H \in \mathbb{B}[X]$ has degree $N - T$, all its roots are distinct and lie in D, and

$$H^2 + H = (L_D/\lambda)H', \qquad 2 \leq T < N/2, \quad T \text{ even}.$$

Then

$$P = \sqrt{H'/\lambda}\,\frac{L_D}{H}, \qquad P^2 = L_D + \frac{L_D}{H}, \qquad R = \sqrt{L_D - \lambda X}$$

are polynomials, P has exactly T roots on D, and $\deg(P + R) = T/2$. For the fixed pair

$$f(x) = \frac{R(x) + \sqrt{\lambda\beta}}{x - \beta}, \qquad g(x) = \frac{1}{x - \beta},$$

the challenge $a = P(\beta) + \sqrt{L_D(\beta)}$ is nonzero and has a witness of degree at most $T/2 - 1$ with exactly T agreements. Moreover,

$$a^2 = \frac{L_D(\beta)}{H(\beta)}, \qquad \operatorname{agr}_K(f) \leq 3N/8 - 1, \qquad \operatorname{agr}_K(g) = \operatorname{CA}_K(f, g) = K.$$

In particular, distinct values $H(\beta)$ give distinct nonzero challenges for this same pair.

Proof. Since the roots of H are distinct and lie in D, $H \mid L_D$; the derivative H' is a square in characteristic two. The assumed identity $H^2 + H = (L_D/\lambda)H'$ gives the displayed formula for P^2, so $P^2 = L_D/H$ at every point of D. At a root of H, the polynomial L_D/H is nonzero because the roots of L_D are simple, so P is nonzero there. At every other point of D, the same identity reduces to $H^2 + H = 0$ and gives $H = 1$ and hence $P = 0$. Thus its root count is T. Also $(P + R)^2 = L_D/H - \lambda X$ has degree T, giving the correction degree. Write $S = R + \sqrt{\lambda\beta}$. Since $S(\beta)^2 = L_D(\beta)$,

$$h_a = \frac{S + a + P}{X - \beta}$$

is a polynomial of degree at most $T/2 - 1$, and $f(x) + a\, g(x) - h_a(x) = P(x)/(x - \beta)$ at every $x \in D$. Evaluating $P^2 = L_D + L_D/H$ at β gives $a^2 = L_D(\beta)/H(\beta)$; $H(\beta) \neq 0$ because all its roots lie in D. Finally, Lemma 3.13 gives the agreement bounds. □

The hypotheses on H describe the agreement set directly. Let $A \subseteq D$ be the set of T points where $H = 1$. Then $L_D/H = (\lambda/c)L_A$ for a nonzero constant c, and the identity $(P + R)^2 = L_D/H - \lambda X$ from the proof reads

$$L_A = \frac{c}{\lambda}(P + R)^2 + cX.$$

Thus the locator of A is a square plus a linear term; equivalently, its derivative is the nonzero constant c. Conversely, if $A \subseteq D$ has $2 \leq |A| < N/2$ and $L'_A = c$ is a nonzero constant, then $H = (c/\lambda)L_D/L_A$ satisfies the hypotheses. These are exactly the sets on which a polynomial agrees with R at twice its degree, the maximum under the bound stated before Lemma 3.13. Every affine subspace of D of positive dimension is such a set. The hyperplanes, of size exactly $N/2$, are treated in Theorem 4.7 for the same pair (f, g), and Section 5 constructs superpolynomially many such sets that are not subspaces.

3.5 Padding and collision averaging

The preceding tools give a received pair at a particular rate and one challenge for each polynomial. We finish with two operations used to obtain the final parameters: adding agreement points to raise the rate, and keeping many challenges distinct when evaluations collide.

Definition 3.17 (Locator padding)**.** Let $B \subseteq D$ have size w and locator L_B. The *padding* of inputs f, g and an explaining polynomial H_z by B is

$$\widetilde{f} = L_B f, \qquad \widetilde{g} = L_B g, \qquad \widetilde{H}_z = L_B H_z.$$

The same multiplier is used for the two inputs and every selected witness.

If $f + zg$ agrees with H_z exactly on A_z, the padded combination agrees with $\widetilde{H}_z$ exactly on $A_z \cup B$. A witness of degree less than K becomes one of degree less than $K + w$, so the new message length must be at least $K + w$. The challenge z is unchanged.

Padding adds only the points of B outside A_z. By the next lemma, one set B meets every old agreement set in at most the average wT/N plus a controlled error.

Lemma 3.18 (Balanced padding)**.** Let D have size N, and let $S_1, \ldots, S_M \subseteq D$ all have size T, with $M \geq 1$. For every integer $1 \leq w < N$, there is a subset $B \subseteq D$ of size exactly w such that, simultaneously for all i,

$$|B \cap S_i| \leq \frac{w}{N}|S_i| + \Delta, \qquad |B \cup S_i| \geq w + \left(1 - \frac{w}{N}\right)|S_i| - \Delta,$$

where $\Delta = \sqrt{(w/2)\ln(2M)}$.

Proof. The lower bound on the union size follows from the intersection bound via $|B \cup S_i| = w + T - |B \cap S_i|$.

Choose a uniformly random w-element subset of D. For a fixed set of size T, sample those w points without replacement and reveal one at a time whether the sampled point belongs to the fixed set. After j draws with r_j successes, the conditional expectation of the final intersection size is $Z_j = r_j + (w-j)(T-r_j)/(N-j)$. At each step, the two possible values of Z_j differ by at most one, and the conditional mean of $Z_j - Z_{j-1}$ is zero. A centered variable of range one has exponential moment at most $e^{t^2/8}$: its log moment generating function has second derivative at most $1/4$. Iterating this bound and optimizing Markov's inequality gives

$$\Pr\left[|B \cap S_i| - wT/N \geq u\right] \leq e^{-2u^2/w}.$$

At the stated Δ, the failure probability for each of the M sets is at most $1/(2M)$. Summing these probabilities shows that all intersection bounds hold simultaneously with probability at least $1/2$.

□

Distinct corrections can give the same challenge. The following averaging bound, also used by Ben-Sasson, Carmon, Haböck, Kopparty, and Saraf [6] and by Crites and Stewart [19], bounds that loss by choosing a good value of a parameter, such as the pole.

Lemma 3.19 (Collision averaging)**.** Suppose $M \geq 1$ indexed values are computed for each of $r > 0$ parameter choices. If the total number of unordered colliding index pairs, summed over all choices, is at most F, some choice gives at least

$$\max\left\{M - \lfloor F/r \rfloor, \left\lceil \frac{rM^2}{rM + 2F} \right\rceil\right\}$$

distinct values. At most one of them is zero.

Proof. Choose a parameter with at most F/r colliding pairs. Group indices that give the same value. If the nonempty groups have sizes $v_1, \ldots, v_u$, then $M - u = \sum_i (v_i - 1) \leq \sum_i \binom{v_i}{2} \leq \lfloor F/r \rfloor$. Also

$$M^2 \leq u \sum_i v_i^2 = u\left(M + 2\sum_i \binom{v_i}{2}\right) \leq u(M + 2F/r).$$

Both bounds hold at the same choice. □

4 Subspace-locator constructions

This section proves the subspace-locator results sketched in Section 2.3, which apply to every binary additive domain D of size N. Section 4.3 proves the hyperplane theorem whose received pair Section 5 reuses.

4.1 Quadratically many exceptional challenges on arbitrary additive domains

Let $N = 16K$, so that the rate is $1/16$. Section 2.3 constructs a pair with one exceptional challenge for each codimension-two subspace of the domain, when the domain lies in a proper subfield $\mathbb{B}$ of the challenge field. Theorem 4.1 proves in addition that these are all the exceptional challenges, and bounds the agreement of each input. Corollary 4.2 then treats challenge fields with no such subfield.

Theorem 4.1 (Quadratic count at rate $1/16$)**.** Let $D \subseteq \mathbb{B}$ be a binary additive domain of size $N = 16K$, where $K \geq 2$ is a power of two, and let $\mathbb{F} \supsetneq \mathbb{B}$ be a finite field. Put $M = (N-1)(N-2)/6$, the number of codimension-two subspaces of D. There is a pair f, g over $\mathbb{F}$ such that:

1. $\mathrm{agr}_K(f) \leq 2K$ and $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = 2K - 1$;

2. for every integer $2K+1 \le T \le 4K-1$, the set $\mathrm{Bad}_T(f,g)$ is the same set of M nonzero challenges, and each of them has maximum agreement exactly $4K-1 = N/4-1$;

3. $\mathrm{Bad}_{4K}(f,g)$ is empty.

If $[\mathbb{F}:\mathbb{B}] \ge 3$, the pair can be chosen with $\mathrm{agr}_K(f) = 2K-1$ as well.

The Johnson threshold $\sqrt{N(K-1)}$ lies strictly between $4K-3$ and $4K-2$, since $(4K-3)^2 < 16K(K-1) < (4K-2)^2$ for $K \ge 2$. The count M therefore holds at $T = 4K-3 = N/4-3$, the largest integer below Johnson, where the agreement exceeds the common agreement by $N/8-2$ positions. The proof uses an element $\theta \in \mathbb{F} \setminus \mathbb{B}$, which gives a second coordinate over $\mathbb{B}$ in which to record a locator coefficient. A third coordinate, available when $[\mathbb{F}:\mathbb{B}] \ge 3$, is used to lower the agreement of f.

Proof. Let W range over the codimension-two linear subspaces of D, and write

$$L_W = X^{4K} + a_W X^{2K} + b_W X^K + V_W, \qquad \deg V_W \le K/2.$$

The coefficients a_W, b_W lie in $\mathbb{B}$ and determine W (Lemma 3.9 with $s=2$). Choose $\theta \in \mathbb{F} \setminus \mathbb{B}$. We first work with the pair

$$f_0 = X^{8K-1} + \theta X^{4K-1}, \qquad g = X^{2K-1},$$

and obtain f from f_0 in Step 5.

Step 1: witnesses. As in Section 2.3, put $z_W = a_W^3 + b_W^2 + \theta a_W$. Then

$$\begin{aligned} P_W &= L_W^2 + (a_W^2+\theta)L_W = X^{8K} + \theta X^{4K} + z_W X^{2K} + C_W, \\ C_W &= (a_W^2+\theta)(b_W X^K + V_W) + V_W^2. \end{aligned} \tag{4.1}$$

Every term of C_W is divisible by X, and $\deg C_W \le K$, so $H_W = C_W/X$ is a polynomial of degree less than K. At a nonzero point of D, the difference $f_0 + z_W g - H_W$ equals $P_W/X = L_W(L_W + a_W^2 + \theta)/X$. The second factor does not vanish there: $L_W(x)$ and a_W^2 belong to $\mathbb{B}$, whereas θ does not. At zero, f_0 and g vanish, but $H_W(0) = (a_W^2+\theta)L_W'$ is nonzero, because the roots of L_W are simple. Hence $f_0 + z_W g$ agrees with H_W exactly on $W \setminus \{0\}$, a set of $4K-1$ points.

Step 2: the challenges are distinct. The elements $1, \theta$ are linearly independent over $\mathbb{B}$. If $z_W = z_{W'}$, comparing the coefficients of θ gives $a_W = a_{W'}$, and comparing the remaining coefficients then gives $b_W^2 = b_{W'}^2$, hence $b_W = b_{W'}$ and $W = W'$. So the M subspaces give M distinct challenges.

Step 3: every challenge with more than $2K$ agreements is some z_W. Suppose that $f_0 + zg$ agrees with a polynomial h, $\deg h < K$, on a set S of more than $2K$ points. We show that $z = z_W$ and $h = H_W$ for some W. To do so, we split the agreement into its coordinates over $\mathbb{B}$, eliminate between the coordinates of 1 and θ to show that the polynomial from the θ coordinate has the shape of a codimension-two locator, and then show that L_D is an additive polynomial in it.

Expand z and the coefficients of h in a $\mathbb{B}$-basis of $\mathbb{F}$ beginning with $1, \theta$. The coefficients of f_0 and g lie in $\mathbb{B} + \mathbb{B}\theta$, so in every other coordinate j, the polynomial $z_j X^{2K-1} - h_j$ vanishes on S. It has degree at most $2K-1$, so it is zero, and $z_j = h_j = 0$. We may thus write

$$z = z_0 + \theta a, \qquad h = h_0 + \theta h_1, \qquad z_0, a \in \mathbb{B}, \quad h_0, h_1 \in \mathbb{B}[X].$$

The coordinates of θ and of 1 say that $X^{4K-1} + aX^{2K-1} + h_1$ and $X^{8K-1} + z_0X^{2K-1} + h_0$ vanish on S. Multiplying by X, the polynomials

$$P_1 = X^{4K} + aX^{2K} + Xh_1, \qquad P_0 = X^{8K} + z_0X^{2K} + Xh_0$$

vanish on S. Their combination

$$P_1^2 + P_0 + a^2P_1 = (z_0 + a^3)X^{2K} + (Xh_1)^2 + a^2Xh_1 + Xh_0 \tag{4.2}$$

has degree at most $2K$ and vanishes on the more than $2K$ points of S, so it is zero. Since $\deg(Xh_i) \le K$, comparison of coefficients above degree K yields

$$Xh_1 = bX^K + V, \qquad \deg V \le K/2, \qquad V(0) = 0, \qquad b^2 = z_0 + a^3.$$

Thus $P_1 = X^{4K} + aX^{2K} + bX^K + V$. We now identify P_1 as a subspace locator. Write

$$L_D = X^{16K} + d_8X^{8K} + d_4X^{4K} + \text{terms of degree at most } 2K$$

and set $\eta = d_8 + a^4$ and $\xi = d_4 + b^4 + \eta a^2$. The polynomial $L_D + P_1^4 + \eta P_1^2 + \xi P_1$ has degree at most $2K$ and vanishes on S, so

$$L_D = P_1^4 + \eta P_1^2 + \xi P_1. \tag{4.3}$$

In particular, P_1 divides L_D, and differentiation gives $L_D' = \xi P_1' \neq 0$. Thus P_1 has $4K$ distinct roots, all in D. Equation (4.3) says that $L_D = A \circ P_1$ for the additive polynomial $A = X^4 + \eta X^2 + \xi X$, and $P_1(0) = 0$, so P_1 is additive by Lemma 3.10. Its roots therefore form a codimension-two subspace $W \le D$, and $P_1 = L_W$, so that $a = a_W$, $b = b_W$, and $V = V_W$. The relation $b^2 = z_0 + a^3$ now gives $z = z_W$, and (4.2) gives $Xh_0 = V^2 + a^2(bX^K + V)$, so $Xh = C_W$ and $h = H_W$.

Together with Step 1, this shows that for the pair f_0, g the challenges with more than $2K$ agreements are exactly the z_W, and that each has maximum agreement exactly $4K - 1$.

Step 4: common agreement. The word g differs from every polynomial of degree less than K by a nonzero polynomial of degree $2K - 1$. It therefore has at most $2K - 1$ agreements with any codeword, which also bounds the common agreement of any pair containing g. To attain $2K - 1$, choose a binary subspace $U \le D$ of size $2K$. The remainders r_1, r_2, r_3 of X^{2K}, X^{4K}, X^{8K} modulo L_U are additive of degree at most K, with zero constant term. Thus r_1/X and $(r_3 + \theta r_2)/X$ have degree less than K and match g and f_0 simultaneously on $U \setminus \{0\}$.

Step 5: individual agreement of the first input. For $\sigma \in \mathbb{F}$, the pair $f = f_0 + \sigma g$ and g has the same common agreement, and $f + zg = f_0 + (z + \sigma)g$, so its exceptional sets are those of f_0, g translated by σ. By Step 3, $\operatorname{agr}_K(f) \le 2K$ whenever σ is not one of the challenges z_W. We show that $\sigma = \sqrt{d_4} \in \mathbb{B}$ is such an element. If $\sigma = z_W$, the coefficient of θ would force $a_W = 0$, and the remaining coefficient would give $b_W^2 = \sigma$. Then $\xi = d_4 + b_W^4 = 0$ in (4.3), contradicting $L_D' = \xi L_W' \neq 0$. With this σ, the challenges $z_W + \sigma$ are distinct, and they are nonzero because their witnesses have $4K - 1 > 2K$ agreements. This proves the three parts of the theorem.

When $[\mathbb{F} : \mathbb{B}] \ge 3$, choose instead $\sigma \notin \mathbb{B} + \mathbb{B}\theta$, so that $1, \theta, \sigma$ are linearly independent over $\mathbb{B}$. Choose a $\mathbb{B}$-linear functional on $\mathbb{F}$ that vanishes at 1 and θ and takes the value 1 at σ. Applying it to the coefficients of an explaining polynomial for $f = X^{8K-1} + \theta X^{4K-1} + \sigma X^{2K-1}$ gives an explaining polynomial for $g = X^{2K-1}$ on the same set. Hence $\operatorname{agr}_K(f) \le \operatorname{agr}_K(g) \le 2K - 1$, and the remainders of Step 4 attain equality. In particular zero is not exceptional, and the three parts hold as before. □

For each counted challenge $z = z_W + \sigma$, the polynomial $H_W - zg$ has degree $2K - 1 < N/8$ and leading coefficient $-z$, and it agrees with f on $N/4 - 1$ positions. The theorem therefore also gives $(N-1)(N-2)/6$ codewords of the rate-$1/8$ code at agreement $N/4 - 1$, below that rate's Johnson threshold $\sqrt{N(N/8-1)} \approx 0.354N$.

Corollary 4.2 (Any finite field containing the evaluation domain)**.** Let $\mathbb{F}$ be a finite field of size q, let $D \subseteq \mathbb{F}$ be a binary additive domain of size $N = 16K$ with $K \geq 2$ a power of two, and put $M = (N-1)(N-2)/6$. There is a scalar $\theta \in \mathbb{F}$ such that the pair

$$f = X^{8K-1} + \theta X^{4K-1}, \qquad g = X^{2K-1}$$

has $\mathrm{CA}_K(f, g) = 2K - 1$ and at least

$$\max\left\{M - \left\lfloor \frac{\binom{M}{2}}{q} \right\rfloor, \left\lceil \frac{qM}{q+M-1} \right\rceil\right\}$$

distinct exceptional challenges, each with at least $4K - 1$ agreements. In particular, $q \geq M$ gives more than $M/2$ distinct challenges, and $q > \binom{M}{2}$ makes all M distinct. If $D = \mathbb{F}$, at least $N - 5$ of the N challenges are exceptional.

Proof. Use the locator coefficients and the polynomials H_W of Step 1 in the proof of Theorem 4.1. For every $\theta \in \mathbb{F}$, the difference $f + z_W g - H_W$ vanishes on $W \setminus \{0\}$, giving at least $4K - 1$ agreements. Step 4 of that proof gives common agreement exactly $2K - 1$.

The coefficient pair (a_W, b_W) determines W (Lemma 3.9). For two distinct subspaces, the affine functions

$$\theta \longmapsto a_W^3 + b_W^2 + \theta a_W$$

coincide for at most one θ if their a_W coefficients differ. If those coefficients agree, their b_W coefficients differ, so the functions never coincide. Thus the total number of collisions over all q choices of θ is at most $\binom{M}{2}$. Lemma 3.19, with $r = q$ and $F = \binom{M}{2}$, gives both bounds at one value of θ. When $D = \mathbb{F}$, so that $q = N$, the second bound is the ceiling of

$$\frac{NM}{N+M-1} = N - 6 + \frac{24}{N+4},$$

which is $N - 5$ since $N \geq 32$. □

4.2 Every challenge exceptional at every fixed rate

This subsection proves Theorem 4.5, sketched at the end of Section 2.3. Lemma 4.3 extends the construction of Section 4.1 from codimension two to codimension s, at rate 2^{-s-2}, and the proof of the theorem pads it from a small subspace to rate ρ.

Lemma 4.3 (Unpadded locator construction)**.** Let $D \subseteq \mathbb{B} \subseteq \mathbb{F}$ be a binary additive domain of size $N = 2^d$ in a finite field $\mathbb{F}$ of size q, and let $s \geq 2$ with $d \geq 2s$. Put

$$K = N/2^{s+2}, \qquad M = \begin{bmatrix} d \\ s \end{bmatrix}_2.$$

There is a pair over $\mathbb{F}$ with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = 2K - 1$ and at least $\lceil qM/(q+M-1) \rceil$ distinct exceptional challenges at agreement $4K - 1$. One of these challenges may be zero. If $[\mathbb{F} : \mathbb{B}] \geq s + 1$, a pair can instead be chosen with

$$\mathrm{agr}_K(f) = \mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = 2K - 1, \qquad |\mathrm{Bad}_{4K-1}(f, g) \setminus \{0\}| \geq M.$$

The guaranteed agreement sets are the M codimension-s subspaces of D, of size $N/2^s = 4K$, with the point zero removed. The hypothesis $d \geq 2s$ ensures that the first s nonleading locator coefficients determine the subspace (Lemma 3.9).

Proof. Let W range over the codimension-s subspaces of D, and write

$$L_W = \sum_{i=0}^{d-s} a_i X^{4K/2^i}, \qquad a_0 = 1.$$

Step 1: witnesses. For $0 \leq j < s$, the power $L_W^{2^{s-1-j}}$ is linearized with leading term $X^{N/2^{j+1}}$. We combine these powers with coefficients b_j chosen so that, for $1 \leq j < s$, the coefficient of $X^{N/2^{j+1}}$ in the combination is a prescribed parameter $\theta_j \in \mathbb{F}$, the same for every W. Explicitly, set

$$b_0 = 1, \qquad b_j = \theta_j + \sum_{i<j} b_i a_{j-i}^{2^{s-1-i}} \quad (1 \leq j < s).$$

Then

$$P_W = \sum_{j=0}^{s-1} b_j L_W^{2^{s-1-j}} = X^{N/2} + \sum_{j=1}^{s-1} \theta_j X^{N/2^{j+1}} + z_W X^{2K} + C_W, \qquad \deg C_W \leq K, \quad C_W(0) = 0,$$

where

$$z_W = \sum_{j=0}^{s-1} b_j a_{s-j}^{2^{s-1-j}}. \tag{4.4}$$

The terms before $z_W X^{2K}$ do not depend on W. Divide their sum by X to define the first input f, and take $g = X^{2K-1}$ as the second input. Since P_W vanishes on W, the polynomial C_W/X, of degree less than K, agrees with $f + z_W g$ on the $4K - 1$ points of $W \setminus \{0\}$.

Step 2: collisions. We show that different subspaces give different affine functions of the parameters. Each b_j is an affine function of $\theta_1, \ldots, \theta_j$ whose coefficients are polynomials in the locator coefficients, so by (4.4) z_W is affine in the parameters. Its coefficients are triangular in the locator coefficients: writing $[\theta_j] z_W$ for the coefficient of θ_j,

$$[\theta_{s-k}] z_W = a_k^{2^{k-1}} + F_k(a_1, \ldots, a_{k-1}) \qquad (1 \leq k < s),$$

and the constant term is $a_s^{2^{s-1}} + F_s(a_1, \ldots, a_{s-1})$, for polynomials F_k that do not depend on W. For example,

$$[\theta_{s-1}] z_W = a_1, \qquad [\theta_{s-2}] z_W = a_2^2 + a_1^3,$$

where for $s = 2$ the second expression is the constant term. To see this, use induction on j in the recurrence for b_j. The coefficient of θ_t in b_j is 1 for $j = t$ and a polynomial in $a_1, \ldots, a_{j-t}$ for $j > t$, and the part of b_j free of the parameters is a polynomial in $a_1, \ldots, a_j$. In (4.4), the summand $j = s - k$ therefore contributes $a_k^{2^{k-1}}$ to $[\theta_{s-k}] z_W$, and each later summand contributes a polynomial in $a_1, \ldots, a_{k-1}$. The summand $j = 0$ contributes $a_s^{2^{s-1}}$ to the constant term, and each later summand contributes a polynomial in $a_1, \ldots, a_{s-1}$. Since raising to a power of two is a bijection of $\mathbb{F}$, these expressions recover $a_1, \ldots, a_s$ one after another, and $a_1, \ldots, a_s$ determine W (Lemma 3.9). Two distinct subspaces therefore give distinct affine functions of the parameters, and two distinct affine functions agree on at most a $1/q$ fraction of $\mathbb{F}^{s-1}$. The total number of colliding pairs over all q^{s-1} parameter choices is thus at most $q^{s-2}\binom{M}{2}$, and Lemma 3.19 gives a parameter choice with at least $\lceil qM/(q + M - 1) \rceil$ distinct challenges.

Step 3: common agreement. Choose a subspace $U \le D$ of size $2K$. Step 4 of the proof of Theorem 4.1 applies, with every power X^{2^i} in the numerators of the two inputs reduced modulo L_U, and gives $\mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = 2K-1$.

Step 4: the second pair. When $[\mathbb{F}:\mathbb{B}] \ge s+1$, choose $1, \theta_1, \dots, \theta_{s-1}, \tau$ linearly independent over $\mathbb{B}$, and add τg to the first input. The locator coefficients lie in $\mathbb{B}$, so each z_W lies in the span of $1, \theta_1, \dots, \theta_{s-1}$ over $\mathbb{B}$, and its coordinates there are the coefficients computed in Step 2. Hence the z_W are distinct. The challenges of the new pair are the $z_W + \tau$. They are distinct, and their τ coordinate is one, so none is zero. Projection onto the τ coordinate bounds the agreement of the new first input by $\mathrm{agr}_K(g) \le 2K-1$, and Step 3 applies to the new pair as well. □

Taking $s = 3$ in Lemma 4.3 gives an explicit cubic count on every prescribed binary additive domain.

Corollary 4.4 (Cubic count at rate 1/32)**.** Let $D \subseteq \mathbb{B}$ be binary additive of size $N = 2^d$, with $d \ge 6$, and let $[\mathbb{F}:\mathbb{B}] \ge 4$. At $K = N/32$, there is one pair satisfying

$$\mathrm{agr}_K(f) = \mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = N/16 - 1$$

and having at least

$$\frac{(N-1)(N-2)(N-4)}{168}$$

distinct nonzero exceptional challenges at agreement $N/8 - 1$.

Proof. Apply Lemma 4.3 with $s = 3$ and expand $\begin{bmatrix} d \\ 3 \end{bmatrix}_2$. □

Theorem 4.5 (Every fixed rate on every additive domain)**.** Fix $0 < \rho < 1$ and an integer $s \ge 2$. There are constants α and $c > 0$, depending only on ρ and s, with $\rho < \alpha < \sqrt{\rho}$, such that the following hold for every sufficiently large binary additive domain D of size N in a finite field $\mathbb{F}$ of size q, with

$$K = \lfloor \rho N \rfloor, \qquad T = \lceil \alpha N \rceil.$$

1. There is a pair with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = K$ and

$$\frac{|\,\mathrm{Bad}_T(f,g) \setminus \{0\}|}{q} \ge \frac{1}{1 + q/(cN^s)} - \frac{1}{q}. \tag{4.5}$$

   Equivalently, there are at least $q/(1+q/(cN^s)) - 1 \ge \frac{1}{2}\min\{q, cN^s\} - 1$ distinct nonzero exceptional challenges; in particular, $q \ge N^s$ gives $\Omega_{\rho,s}(N^s)$ of them.

2. If $q \le N^a$ for a fixed $a \ge 1$ with $s > 2a$, there is a pair with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = K$ and

$$\mathrm{Bad}_T(f,g) = \mathbb{F}.$$

   Here zero is exceptional as well.

3. If $D \subseteq \mathbb{B} \subsetneq \mathbb{F}$, there is a pair with

$$\mathrm{agr}_K(f) = \mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = K, \qquad |\,\mathrm{Bad}_T(f,g) \setminus \{0\}| \ge \frac{|\mathbb{B}|}{1 + |\mathbb{B}|/(cN^s)} - 1.$$

   If moreover $[\mathbb{F}:\mathbb{B}] \ge s+1$, there is a pair with these three agreements equal to K that satisfies (4.5).

For the pairs of the first two parts, the first input f also has at least as many codewords of the code of message length $K+1$ at agreement T as the pair has exceptional challenges (see the end of the proof). The proof takes $\alpha = \rho + 2^{-r-s-2}$ for an integer r depending only on ρ and s, so the agreement exceeds the common agreement by about $2^{-r-s-2}N$ positions.

Proof. Put $\kappa = 2^{-s-2}$, and choose $\mu = 2^{-r}$, for a sufficiently large integer r, such that

$$2\mu\kappa < \rho, \qquad \rho < 1 - \mu(1-2\kappa), \qquad \rho + \mu\kappa < \sqrt{\rho}.$$

Set $\alpha = \rho + \mu\kappa$. Let $D_0 \leq D$ be a subspace of size $n = \mu N$, and put

$$K_0 = \kappa n, \qquad w = K - 2K_0 + 1.$$

For sufficiently large N, the first inequality makes w positive, and the second gives $w \leq N - n$, so that a set of w points fits outside D_0. The third places α below $\sqrt{\rho}$.

The seed pair. Apply Lemma 4.3 on D_0, whose dimension is at least $2s$ for large N. It gives polynomial inputs f_0 and $g_0 = X^{2K_0-1}$, and at least $\lceil qM/(q+M-1) \rceil$ distinct challenges, where $M = \begin{bmatrix} \log_2 n \\ s \end{bmatrix}_2 \geq (n/2^s)^s = cN^s$ with $c = 2^{-(r+s)s}$, by the size bound for Gaussian binomial coefficients. Each challenge has a witness of degree less than K_0 that agrees with the combination on at least $4K_0 - 1$ points of D_0.

Padding. Evaluate the polynomial inputs and witnesses on all of D, and multiply them by the locator L_E of a set $E \subseteq D \setminus D_0$ of size w (Definition 3.17). The padded witnesses have degree at most $K_0 - 1 + w = K - K_0$, which is less than K. Every point of E is a new agreement, so each challenge now has at least

$$(4K_0 - 1) + w = K + 2K_0$$

agreements. Since $K + 2K_0 \geq (\rho + 2\mu\kappa)N - 1$ and $T \leq (\rho + \mu\kappa)N + 1$, this is at least T for large N. The padded second input $g = L_E g_0$ is monic of degree K, so it agrees with any polynomial of degree less than K on at most K points. Interpolating both inputs on any K points then gives $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$.

The first part. Discarding at most one zero challenge leaves at least

$$\frac{qM}{q+M-1} - 1 \geq \frac{q}{1+q/M} - 1 \geq \frac{q}{1+q/(cN^s)} - 1$$

nonzero exceptional challenges, which is (4.5).

The second part. If $M > (q-1)^2$, then $qM/(q+M-1) > q-1$, so the number of distinct challenges is q and every element of $\mathbb{F}$ is exceptional, including zero. For $q \leq N^a$ and $s > 2a$, the inequality $M \geq cN^s > (q-1)^2$ holds for every sufficiently large N.

The third part. First let $[\mathbb{F} : \mathbb{B}] \geq s+1$, and use the second pair of Lemma 4.3 on D_0 as the seed. Its M challenges are distinct and nonzero, and its first input contains the term τg_0 with τ independent of the other coefficients over $\mathbb{B}$. After padding, projection onto the τ coordinate bounds the agreement of the first input by that of the second, which is K, and interpolation attains K. All M challenges remain exceptional, and $M \geq q/(1+q/M)$ gives (4.5). For an arbitrary proper extension, apply the first part with $\mathbb{B}$ as the challenge field, and then apply Lemma 3.12 to pass to $\mathbb{F}$. The conversion preserves the counted nonzero challenges and makes both individual agreements equal to the common agreement K, with the same message length and agreement.

Decoding lists. If h_z has degree less than K and explains $f + zg$, then $h_z - zg$ agrees with f on the same positions and has degree at most K. Its coefficient of X^K is $-z$, so distinct challenges give distinct codewords of the code of message length $K + 1$. □

The pair of the first two parts controls only $\mathrm{agr}_K(g)$. When every challenge is exceptional, zero is too, so f itself agrees with a codeword on at least $T > K$ positions. This is why the third part, with both individual agreements equal to K, uses a separate pair.

A finite instance of the same padding, applied to the quadratic count of Corollary 4.2, bears on an early binary-field implementation.

Corollary 4.6 (Rate $1/8$ at finite length)**.** Let D be a binary additive domain of size $N = 2^d$, with $d \geq 6$, in a finite field $\mathbb{F}$ of size q, and put

$$K = \frac{N}{8}, \qquad M = \frac{(N/2 - 1)(N/2 - 2)}{6}.$$

There is a pair with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$ and at least $\lceil qM/(q + M - 1) \rceil$ distinct exceptional challenges at agreement $3N/16$. The same holds on every translate of D. For $N = 2^{20}$ and $q = 2^{64}$, this gives more than 4.58×10^{10} exceptional challenges, so the exceptional probability is greater than $2^{-28.585}$.

Proof. Choose a subspace $D_0 \leq D$ of size $n = N/2$ and put $K_0 = n/16 = N/32$. Apply the padding step of the proof of Theorem 4.5, with the pair of Corollary 4.2 on D_0 as the seed and $w = K - 2K_0 + 1 = N/16 + 1$. The padded pair has $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$ and the same $\lceil qM/(q + M - 1) \rceil$ distinct challenges, each with at least $(4K_0 - 1) + w = 3N/16$ agreements. For a translate $D + c$, substitute $X - c$ for X in the inputs and witnesses; degrees and agreement sets are preserved. With $N = 2^{20}$ and $q = 2^{64}$, direct computation gives $\lceil qM/(q + M - 1) \rceil = 45{,}812{,}722{,}234 > 2^{64-28.585}$. □

The 2018 implementation of Ben-Sasson, Bentov, Horesh, and Riabzev [5, Appendix B.8] targeted 60 bits of security over a 64-bit binary field, with the commitment phase of its proximity test run twice independently and 22 query repetitions at rate $1/8$, each query selecting one of the two sets of committed oracles. A Johnson-based analysis gives a query-error term of about $(\sqrt{1/8})^{22} = 2^{-33}$ [7, Theorem 8.3]; the target would need a proximity gap down to agreement about 15.1%. But on their affine binary domains at $N = 2^{20}$, the pair above has common agreement 12.5% and reaches 18.75% with probability above $2^{-28.585}$, hence $2^{-57.17}$ for both challenges. An analysis that counts every exceptional challenge as a failure therefore cannot certify the target.

4.3 Exceptional probability approaching one at half agreement

This subsection proves the hyperplane example of Section 2.1, at rate $1/4$, where half agreement is the asymptotic Johnson threshold. Section 5 keeps its received pair and replaces hyperplanes by more general agreement sets.

Theorem 4.7 (Hyperplanes at half agreement)**.** Let $\mathbb{F}$ be a finite field of characteristic two, and let $D \subsetneq \mathbb{F}$ be an affine flat of size $N = 2^d$, $d \geq 3$. Put $K = N/4$. There is a pair with inputs and challenges in $\mathbb{F}$ satisfying

$$\mathrm{CA}_K(f, g) = K, \qquad \mathrm{agr}_K(f) \leq 3N/8 - 1, \qquad \mathrm{agr}_K(g) = K,$$

and

$$|\operatorname{Bad}_{N/2}(f, g)| = 2N - 2.$$

All these exceptional challenges are nonzero. If $|\mathbb{F}| = 2N$, then $\operatorname{Bad}_{N/2}(f, g) = \mathbb{F} \setminus \{0, s\}$ for some $s \neq 0$, giving exceptional probability exactly $1 - 1/N$.

Proof. Choose $\beta \in \mathbb{F} \setminus D$, put $\lambda = L'_D$ and

$$R = \sqrt{L_D - \lambda X}, \qquad S = R + \sqrt{\lambda\beta}, \qquad f(x) = \frac{S(x)}{x-\beta}, \quad g(x) = \frac{1}{x-\beta}.$$

Lemma 3.13 gives the individual and common-agreement bounds. For every affine hyperplane H of D, its locator L_H has degree $N/2$, with all lower terms of degree at most K. The same holds for S, so this is the pole reduction of Lemma 3.11 with shared part S and corrections $L_H - S$. Set $z_H = L_H(\beta) - S(\beta)$. Then

$$h_H = \frac{S + z_H - L_H}{X - \beta}$$

is a polynomial of degree at most $K - 1$: its numerator has degree at most K and vanishes at β. At every $x \in D$ we have $f(x) + z_H g(x) - h_H(x) = L_H(x)/(x-\beta)$, so h_H agrees with $f + z_H g$ exactly on H.

All $2N - 2$ challenges z_H are distinct. The locators of parallel hyperplanes differ by a nonzero constant. Nonparallel hyperplanes intersect in K points, so their nonzero locator difference, of degree at most K, cannot also vanish at β. The bound on $\mathrm{agr}_K(f)$ shows that zero is not among them.

To prove that these are all the exceptional challenges, suppose a polynomial h of degree less than K agrees with $f + zg$ at $N/2$ points. The numerator of $f + zg - h$ is $F = S + z - (X - \beta)h$, monic of degree $N/2$, splitting into distinct roots in D. Hence $F \mid L_D$. Since

$$F^2 - L_D = -\lambda(X - \beta) + z^2 - (X - \beta)^2 h^2$$

has degree at most $2K = N/2$ and is divisible by F, it equals cF. Its derivative is $-\lambda \neq 0$, so $c \neq 0$. Thus $L_D = A \circ F$ for the additive polynomial $A = X^2 - cX$. After subtracting constant terms, Lemma 3.10 shows that F is a constant plus an additive polynomial. Its root set is therefore an affine hyperplane of D. This proves the exact count in every containing field. Put $s = S(\beta) = \sqrt{L_D(\beta)} \neq 0$. No z_H equals s, since that would give $L_H(\beta) = 0$. When $|\mathbb{F}| = 2N$, the exceptional challenges are consequently exactly $\mathbb{F} \setminus \{0, s\}$. □

5 Gold constructions: superpolynomially many exceptions near Johnson

This section proves the Gold results sketched in Section 2.2. We keep the received pair of Theorem 4.7 and replace its hyperplanes by level sets of quadratic Boolean functions, which give many more exceptional challenges slightly below half agreement.

5.1 The counting bound and its consequences

In the theorem below, L is the guaranteed number of polynomials, T is their root count on D, and δ bounds the number of exterior points where two distinct members can coincide. Here $2t$ is the rank of the quadratic functions, and $\Delta \geq 1$ is a density requirement.

Theorem 5.1 (The Gold counting bound)**.** Let $\mathbb{B} = \mathbb{F}_{2^m}$ and let $D \subseteq \mathbb{B}$ be binary additive of dimension d, with $N = 2^d$. Choose $2 \leq t \leq \lfloor d/2 \rfloor$, put $\iota = 1$ for even d and $\iota = 0$ for odd d, and suppose

$$\Delta = m - t(m - d + \iota) \geq 1.$$

Set

$$L = 2^{2t}(2^\Delta - 1)\begin{bmatrix} \lfloor d/2 \rfloor \\ t \end{bmatrix}_4, \qquad T = \frac{N}{2} - \frac{N}{2^{t+1}}, \qquad \delta = \frac{N}{2^{2t}}.$$

Here $\begin{bmatrix} \lfloor d/2 \rfloor \\ t \end{bmatrix}_4$ is a Gaussian binomial coefficient (Section 3.1); it lies between $4^{t(\lfloor d/2 \rfloor - t)}$ and four times that value.

1. *Decoding list.* Some received word over $\mathbb{B}$ has at least L codewords of message length $N/4$ at agreement T.

2. *Exceptional challenges.* For every finite extension $\mathbb{F} \supseteq \mathbb{B}$ with $q = |\mathbb{F}| > N$, there is one received pair over $\mathbb{F}$ with $\mathrm{agr}_{N/4}(g) = \mathrm{CA}_{N/4}(f, g) = N/4$ and at least

$$Z = \max\left\{L - \left\lfloor \frac{\delta\binom{L}{2}}{q-N} \right\rfloor, \left\lceil \frac{L(q-N)}{q-N+\delta(L-1)} \right\rceil\right\} \geq \frac{1}{2}\min\left\{L, \frac{q-N}{\delta}\right\} \tag{5.1}$$

distinct nonzero exceptional challenges at agreement T, and at least Z of them admit explaining polynomials of degree at most $T/2 - 1$. The pair can also be chosen with $\mathrm{agr}_{N/4}(f) \leq 3N/8 - 1$.

The same conclusions hold on every affine translate of D.

The containing field. A larger t raises T toward $N/2$ and lowers δ, but each of the $t - 1$ equations of Section 5.3 costs up to m binary degrees of freedom. For $m = d + c$ the condition $\Delta \geq 1$ holds for t proportional to d; for $m \geq 2d$ it fails for every $t \geq 2$. To apply Theorem 5.1, choose for $\mathbb{B}$ the smallest subfield of the challenge field containing D. It depends on which elements D contains, not only on its dimension.

LeanVM works over $\mathbb{F}_{2^{64}} = \mathbb{F}_2[u]/(u^{64} + u^4 + u^3 + u + 1)$ and evaluates on the domains $\mathrm{span}_{\mathbb{F}_2}\{1, u, \ldots, u^{d-1}\}$ [42]. For $D = \mathrm{span}_{\mathbb{F}_2}\{1, u, \ldots, u^{21}\}$, a field containing D contains $\mathbb{F}_2(u) = \mathbb{F}_{2^{64}}$, so the smallest choice is $m = 64$. With $d = 22$ and $\iota = 1$, this gives $\Delta = 64 - 43t < 1$ for every $t \geq 2$, placing this domain outside the parameter range of Theorem 5.1. Flock's domains are the spans of $1, u, \ldots, u^{d-1}$ for a generator u of $\mathbb{F}_{2^{128}}$ over $\mathbb{F}_2$, with $d \leq 24$ [25]. There $m = 128$, and these domains are outside the range for the same reason. Section 6.4 gives explicit finite bounds on such domains, at agreement thresholds farther below Johnson.

5.2 Exceptional counts and probabilities near Johnson

Letting t grow with N gives superpolynomial counts near Johnson over a challenge field of *quasipolynomial* size $N^{O(\log N)}$. With a fixed extension degree instead, the agreement still approaches Johnson and the exceptional probability stays constant.

Corollary 5.2 (Dense additive domains)**.** Fix an integer $c \geq 0$, and put $\theta_c = \min\{1/4, 1/(c+1)\}$ and $e_c = \theta_c(1 - 2\theta_c)$. For every sufficiently large d and every additive d-space $D \subseteq \mathbb{B} = \mathbb{F}_{2^{d+c}}$, with $N = 2^d$, there is an agreement T with $T/N = 1/2 - \Theta_c(N^{-\theta_c})$ such that the following hold for the code of message length $N/4$ on D.

1. *Lists.* Some word over $\mathbb{B}$ has at least $2^{e_c(\log_2 N)^2 - O_c(\log N)}$ codewords at agreement T.

2. *Exceptional challenges.* Over some extension $\mathbb{F} \supseteq \mathbb{B}$ with $\log_2 |\mathbb{F}| = e_c(\log_2 N)^2 + O_c(\log N)$, some pair with $\mathrm{CA}_{N/4}(f, g) = N/4$ has at least $2^{e_c(\log_2 N)^2 - O_c(\log N)}$ distinct nonzero exceptional challenges at agreement T, a fraction $\Omega_c(N^{-1+2\theta_c})$ of $\mathbb{F}$.

In particular, for $c \leq 3$ the list size and the exceptional count are at least $N^{(1/8 - o(1))\log_2 N}$, the Johnson deficit is $\Theta(N^{-1/4})$, and the exceptional probability is $\Omega(N^{-1/2})$. The decoding list is over an alphabet of size $2^c N$.

Proof. Apply Theorem 5.1 with

$$t = \min\left\{\lfloor d/4 \rfloor, \left\lfloor \frac{d + c - 1}{c + 1} \right\rfloor\right\}.$$

This t is at least two for large d, and

$$\Delta = d + c - t(c + \iota) \geq d + c - t(c + 1) \geq 1.$$

Also $t = \theta_c d + O_c(1)$. The Gaussian product formula gives

$$\log_2 \begin{bmatrix} n \\ t \end{bmatrix}_4 = 2t(n - t) + O(1), \qquad n = \lfloor d/2 \rfloor.$$

Consequently the polynomial count in Theorem 5.1 satisfies $\log_2 L = \theta_c(1 - 2\theta_c)d^2 + O_c(d)$.

Write $\delta = N/2^{2t}$ and $q_0 = N + \delta(L - 1)$. Choose q to be the largest power of $|\mathbb{B}|$ with $q \leq q_0$. For large d, $q_0 \geq 2|\mathbb{B}|N$. Thus $q > q_0/|\mathbb{B}|$, $q \geq 2N$, and $\delta(L - 1)/(2|\mathbb{B}|) < q - N \leq \delta(L - 1)$. The nonzero count in (5.1) therefore obeys

$$Z \geq \frac{q - N}{2\delta} - 1 > \frac{L - 1}{4|\mathbb{B}|} - 1, \qquad \frac{Z}{q} \geq \frac{1 - N/q}{2\delta} - \frac{1}{q} \geq \frac{1}{8\delta}$$

for sufficiently large d. These inequalities give the stated count and probability bounds, and $\log_2 q = \log_2 L + O_c(d)$ gives the field size. □

Corollary 5.3 (Fixed extension degree)**.** Fix an integer $e \geq 2$. For all sufficiently large n, put $N = 2^{2n-1}$, $\mathbb{B} = \mathbb{F}_{2N}$ and $\mathbb{F} = \mathbb{F}_{(2N)^e}$. On every binary hyperplane $D \subset \mathbb{B}$, there is one pair with

$$\mathrm{CA}_{N/4}(f, g) = \mathrm{agr}_{N/4}(g) = N/4, \qquad \mathrm{agr}_{N/4}(f) \leq 3N/8 - 1,$$

and, at $T = N/2 - 2^{e-3/2}\sqrt{N}$,

$$|\operatorname{Bad}_T(f, g) \setminus \{0\}| \geq (2^{1-2e} - o(1))|\mathbb{F}|.$$

On the full field $D = \mathbb{B} = \mathbb{F}_N$, with $N = 2^{2n}$ and $\mathbb{F} = \mathbb{F}_{N^e}$, the same individual and common-agreement bounds hold, and at $T = N/2 - 2^{e-2}\sqrt{N}$ we have

$$|\operatorname{Bad}_T(f, g) \setminus \{0\}| \geq (4^{1-e} - o(1))|\mathbb{F}|.$$

In particular, $q = N^2$ permits agreement $N/2 - \sqrt{N}$ with exceptional probability at least $1/4 - o(1)$.

Proof. In Theorem 5.1, take $d = 2n - 1$, $m = 2n$ and $t = n - e$. For $n \geq e + 2$ these parameters are admissible, and

$$\Delta = n + e, \qquad \delta = 2^{2e-1}, \qquad L = 2^{2n-2e}(2^{n+e} - 1)\begin{bmatrix} n - 1 \\ e - 1 \end{bmatrix}_4.$$

For $q = (2N)^e$, the Gaussian product gives $L/q \to \infty$. Dividing (5.1) by q therefore gives a lower bound tending to $1/\delta$; the agreement bounds follow from the same theorem.

For the full-field case, take $d = m = 2n$ and $t = n - e + 1$. Then

$$\Delta = n + e - 1, \qquad \delta = 4^{e-1}, \qquad L = 2^{2n-2e+2}(2^{n+e-1} - 1)\begin{bmatrix} n \\ e - 1 \end{bmatrix}_4.$$

For fixed e, the product formula gives $\log_2(L/N^e) = n - 2e^2 + 3e - 1 + O_e(1)$, so again $L/q \to \infty$. Dividing (5.1) by q again gives a lower bound tending to $1/\delta$. □

Theorem 5.4 (No fixed polynomial exceptional bound below Johnson)**.** Fix an agreement fraction $1/4 < a < 1/2$ and a proposed polynomial bound $C_0 N^b$, where $C_0, b > 0$. For arbitrarily large code lengths N, there is a rate-$1/4$ Reed–Solomon code over a binary field $\mathbb{F}$ and two received words f, g with the following properties:

1. The two words have common agreement exactly $N/4$. That is, the largest number of positions on which f and g simultaneously match a pair of codewords is $N/4$.

2. For more than $C_0 N^b$ distinct challenges $z \in \mathbb{F}$, the combination $f + zg$ agrees with a codeword on at least aN positions.

The field size is polynomial in N, with an exponent that depends only on b.

Proof. Take $e = \max\{2, \lfloor b \rfloor + 1\}$, so $e > b$. We construct examples for arbitrarily large powers of two N. The evaluation domain D is an $\mathbb{F}_2$-hyperplane in a field $\mathbb{B}$ of size $2N$, and the received words and challenges take values in an extension $\mathbb{F}$ of size $(2N)^e$. The code consists of evaluations on D of polynomials in $\mathbb{F}[X]$ of degree less than $N/4$, so its rate is $1/4$.

Apply Corollary 5.3. Its agreement fraction tends to $1/2$, so eventually $T \geq \lceil aN \rceil$, and its count is $\Omega_e(N^e) > C_0 N^b$. □

5.3 From quadratic functions to polynomials with many roots

Throughout this subsection, $D \subseteq \mathbb{B}$ is binary additive of dimension d, with $N = 2^d$ and monic locator

$$L_D = \sum_{i=0}^{d} \lambda_i X^{2^i}, \qquad \lambda_d = 1, \quad \lambda_0 \neq 0.$$

We normalize the locator so that its derivative is one:

$$\Lambda = \frac{L_D}{\lambda_0} = \sum_{i=0}^{d} \mu_i X^{2^i}, \qquad \eta = \lambda_0^{-1/2},$$

so that $\mu_0 = 1$ and $\mu_d = \eta^2$.

We keep the polynomial $R = \sqrt{L_D - \lambda_0 X}$ of Theorem 4.7, which depends only on D, and look for sets $E \subseteq D$ with polynomials $P = R + C$ that vanish on E and have $\deg C = |E|/2$. By the discussion after Lemma 3.16, these are the sets whose locators have constant derivative, such as affine subspaces. Here E is the set of ones of a *quadratic* Boolean function $\psi + \kappa$. Such sets of size close to $N/2$ are far more numerous than subspaces. Under the Gold moment equations, the polynomial H of $\psi + \kappa$ has degree equal to its number of zeros, and L_D/H is then a scalar multiple of L_E (Remark 5.11).

The argument passes between functions $D \to \mathbb{F}_2$ and polynomials over $\mathbb{B}$. Since $\mathbb{F}_2 \subseteq \mathbb{B}$, every function $D \to \mathbb{F}_2$ is the restriction of exactly one polynomial of degree less than N (Definition 3.6). We write φ and ψ for functions on D, and ℓ, Q, and H for the polynomials representing them. Table 3 summarizes the correspondences proved below.

Linear functions. Quadratic Boolean functions on D are built from linear functions $D \to \mathbb{F}_2$, so we first represent these by polynomials.

Lemma 5.5 (Labels of linear functions)**.** Every $\mathbb{F}_2$-linear function $\varphi : D \to \mathbb{F}_2$ agrees on D with exactly one polynomial $\ell \in \mathbb{B}[X]$ that is a combination of $X, X^2, X^4, \ldots, X^{N/2}$. The coefficient of X in ℓ has a square root $\omega \in \mathbb{B}$. We call ω the *label* of φ and write ℓ_ω for ℓ.

1. The polynomial ℓ_ω satisfies $\ell_\omega^2 + \ell_\omega = \omega^2 \Lambda$.

2. The labels form a binary d-space $\widehat{D} \subseteq \mathbb{B}$, the *label space* of D. The map $\omega \mapsto \ell_\omega|_D$ is an $\mathbb{F}_2$-linear bijection from $\widehat{D}$ onto the space of linear functions $D \to \mathbb{F}_2$.

Function on D	Polynomial in $\mathbb{B}[X]$
linear function with label ω	ℓ_ω, with $\ell_\omega^2 + \ell_\omega = \omega^2\Lambda$ (Lemma 5.5)
coordinate x_i	$\ell_i = \ell_{\omega_i}$
product $x_i x_j$	$\ell_i\ell_j + \omega_i\omega_j\Lambda$
quadratic function ψ with matrix A and label ω	Q, with $Q^2 + Q = \Lambda Q'$ (Lemma 5.6)
polar radical of ψ	roots in D of $J = Q' - Q'(0)$
zeros of $\psi + \kappa$	roots of $H = Q + \kappa$, when $\deg H$ equals their number
ones of $\psi + \kappa$	roots on D of $P = R + C$ (Lemma 5.12)

Table 3: Functions on D and the polynomials that represent them in Section 5.3.

3. For $\omega \neq 0$, the polynomial ℓ_ω has degree $N/2$ and leading coefficient $\eta\omega$.

For example, if $D = \mathbb{B} = \mathbb{F}_{2^m}$, then $\ell_\omega = \sum_{i=0}^{m-1} \omega^{2^{i+1}} X^{2^i}$ restricts to $x \mapsto \mathrm{Tr}(\omega^2 x)$, and $\widehat{D} = \mathbb{B}$. In general $\widehat{D}$ differs from D.

Proof. Evaluating the polynomials $\sum_{i=0}^{d-1} c_i X^{2^i}$ on a binary basis of D is a $\mathbb{B}$-linear map between two d-dimensional spaces. A polynomial in its kernel vanishes on all of D by additivity, and a nonzero one has fewer than N roots, so the kernel is zero. So exactly one such ℓ matches φ on the basis, and then on all of D because both are additive.

The polynomial $\ell^2 + \ell$ is linearized of degree at most N and vanishes on D, so it is a constant multiple of L_D. Comparing coefficients of X gives $\ell^2 + \ell = \omega^2 L_D/\lambda_0 = \omega^2\Lambda$, and comparing coefficients of X^N gives the third part. For the second part, $\varphi \mapsto \ell$ and $\ell \mapsto \omega$ are additive, and $\omega = 0$ forces $\ell^2 = \ell$, so ℓ is constant and hence zero. □

Quadratic functions. Fix a basis $\omega_1, \ldots, \omega_d$ of the label space $\widehat{D}$ and write $\ell_i = \ell_{\omega_i}$. By Lemma 5.5, the functions $x \mapsto x_i = \ell_i(x)$ are binary linear coordinates on D, namely those of the basis of D dual to $\ell_1, \ldots, \ell_d$. For an alternating binary $d \times d$ matrix A and a label $\omega \in \widehat{D}$, define a function $\psi : D \to \mathbb{F}_2$ and a polynomial $Q \in \mathbb{B}[X]$ by

$$\psi(x) = \sum_{i<j} A_{ij} x_i x_j + \ell_\omega(x), \qquad Q = \sum_{i<j} A_{ij}\big(\ell_i\ell_j + \omega_i\omega_j\Lambda\big) + \ell_\omega. \tag{5.2}$$

Every quadratic Boolean function on D that vanishes at zero is of this form for exactly one pair (A, ω), and A is its polar matrix. The entries of A and the label ω are the free parameters of the construction. We write ψ_A for the function with $\omega = 0$, and

$$J = \sum_{i<j} A_{ij}\big(\omega_i^2\ell_j + \omega_j^2\ell_i\big), \qquad \varepsilon_A = \sum_{i<j} A_{ij}\omega_i\omega_j,$$

which depend only on A. The polynomial J is linearized of degree at most $N/2$. Recall from Definition 3.15 that the polar radical of ψ is the null space of A in the coordinates x_i: it consists of the $u \in D$ for which $\psi(x + u) + \psi(x)$ does not depend on x, and it has $N/2^{\mathrm{rank}\,A}$ elements.

Lemma 5.6 (The polynomial of a quadratic function)**.** Let ψ, Q, J, and ε_A be as above.

1. The polynomial Q has degree less than N, satisfies $Q(0) = 0$, and agrees with ψ on D.

2. Its derivative is $Q' = J + \varepsilon_A + \omega^2$, and

$$Q^2 + Q = \Lambda Q'. \tag{5.3}$$

3. The polar radical of ψ is $\{y \in D : J(y) = 0\}$.

Proof. Since Λ vanishes on D, the polynomial Q agrees with ψ there. By the third part of Lemma 5.5, $\ell_i\ell_j$ and $\omega_i\omega_j\Lambda$ have the same leading term $\eta^2\omega_i\omega_j X^N$, so $\deg Q < N$; also $Q(0) = 0$. The formula for Q' follows from $\ell_i' = \omega_i^2$ and $\Lambda' = 1$. Both sides of (5.3) are additive in Q, so it suffices to check the identity on each summand of Q. For ℓ_ω it is the first part of Lemma 5.5. For $p = \ell_i\ell_j + \omega_i\omega_j\Lambda$, substituting $\ell_i^2 = \ell_i + \omega_i^2\Lambda$ and $\ell_j^2 = \ell_j + \omega_j^2\Lambda$ gives

$$p^2 + p = \Lambda\big(\omega_i^2\ell_j + \omega_j^2\ell_i + \omega_i\omega_j\big) = \Lambda p',$$

because the terms $\omega_i^2\omega_j^2\Lambda^2$ cancel.

For the third part, fix $y \in D$ with coordinates $y_i = \ell_i(y) \in \mathbb{F}_2$. The polynomials ℓ_i, ℓ_ω, and Λ are additive, so

$$Q(X + y) + Q(X) + Q(y) = \sum_{i<j} A_{ij}\big(y_j\ell_i + y_i\ell_j\big) = \ell_{\omega'}, \qquad \omega' = \sum_{i<j} A_{ij}\big(y_j\omega_i + y_i\omega_j\big).$$

On D this polynomial takes the values of the polar form $B_\psi(\cdot, y)$. By the second part of Lemma 5.5, it vanishes on D exactly when $\omega' = 0$. Since the y_i lie in $\mathbb{F}_2$, we have $\omega'^2 = J(y)$, so y lies in the polar radical exactly when $J(y) = 0$. □

The moment equations. If the degree of $H = Q + \kappa$ equals the number of zeros of $\psi + \kappa$, then H is a scalar multiple of the locator of that zero set. The following equations on A lower $\deg Q$ to that number when A has rank $2t$.

Definition 5.7 (Gold moments)**.** Let $\mathbb{B}$ be a finite field of characteristic two, and let $\omega_1, \dots, \omega_d \in \mathbb{B}$ be linearly independent over $\mathbb{F}_2$. For an alternating binary $d \times d$ matrix A and an integer $k \geq 1$, the k-th *Gold moment* of A is

$$M_k(A) = \sum_{i<j} A_{ij}\big(\omega_i\omega_j^{2^k} + \omega_j\omega_i^{2^k}\big) \in \mathbb{B}.$$

Each summand is the polarization of $x \mapsto x^{2^k+1}$, the power function studied by Gold [30], and each moment is $\mathbb{F}_2$-linear in the entries of A. For matrices of rank $2t$ on a full field, the equations $M_k(A) = 0$ for $1 \leq k < t$ correspond to those by which Berman, Shany, and Tamo [11, Theorem IV.1] characterize the quadratic functions whose supports are minimum-weight codewords of extended BCH codes; theirs are the squares of ours, after a change of basis.

Lemma 5.8 (Moment equations and the coefficients of J)**.** Write $J = \sum_{i=0}^{d-1} J_i X^{2^i}$. Then $J_0 = 0$, and for $2 \leq t \leq d/2$ the following are equivalent:

1. $M_1(A) = \cdots = M_{t-1}(A) = 0$;
2. $J_1 = \cdots = J_{t-1} = 0$;
3. $J_{d-t+1} = \cdots = J_{d-1} = 0$, that is, $\deg J \leq N/2^t$.

When they hold,

$$J = \sum_{i=t}^{d-t} J_i X^{2^i} = \widehat{J}^{2^t}, \qquad \widehat{J} = \sum_{i=t}^{d-t} J_i^{2^{-t}} X^{2^{i-t}}, \qquad \deg \widehat{J} \leq \frac{N}{2^{2t}}, \tag{5.4}$$

where $a^{2^{-r}}$ denotes the 2^r-th root of a in $\mathbb{B}$ (Figure 4).

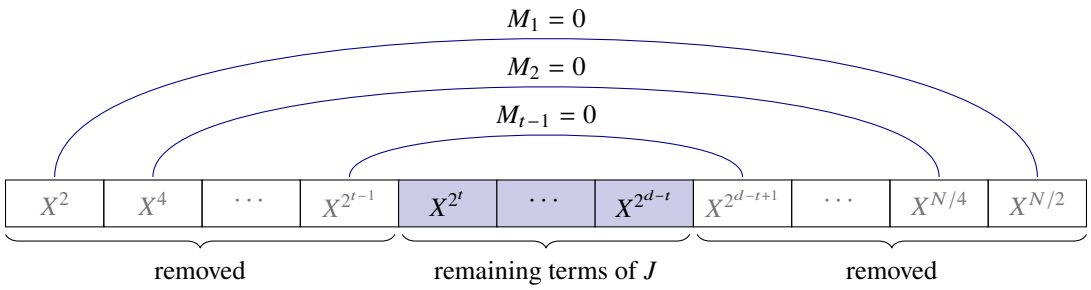


Figure 4: How the Gold moment equations control $\deg Q'$ (Lemma 5.8). The nonconstant part J of Q' is additive, and its possible terms are $X^2, X^4, \dots, X^{N/2}$. Once $M_1 = \cdots = M_{k-1} = 0$, the equation $M_k = 0$ removes the terms X^{2^k} and $X^{2^{d-k}}$, one at each end. The $t-1$ equations leave only $X^{2^t}, \dots, X^{2^{d-t}}$. The picture is drawn for $t \geq 4$; for $t = 2$ only $M_1 = 0$ is imposed and only X^2 and $X^{N/2}$ are removed. Removing the high terms bounds $\deg Q'$ by $N/2^t$, and removing the low terms makes J a 2^t-th power.

Proof. For a label $\omega \in \widehat{D}$, let $\omega^{(i)}$ be the coefficient of X^{2^i} in ℓ_ω, and write $\omega_k^{(i)}$ for $\omega = \omega_k$, so that $J_i = \sum_{j<k} A_{jk}\big(\omega_j^2 \omega_k^{(i)} + \omega_k^2 \omega_j^{(i)}\big)$. Comparing coefficients in $\ell_\omega^2 + \ell_\omega = \omega^2 \Lambda$ gives

$$\omega^{(0)} = \omega^2, \qquad \omega^{(i)} = \big(\omega^{(i-1)}\big)^2 + \mu_i \omega^2 \quad (1 \leq i \leq d-1), \qquad \omega^{(d-1)} = \eta\omega.$$

Solving upward gives $\omega^{(i)} = \sum_{s=0}^{i} \mu_{i-s}^{2^s} \omega^{2^{s+1}}$. In J_i the terms with $s = 0$ cancel, and $\omega_j^2 \omega_k^{2^{s+1}} + \omega_k^2 \omega_j^{2^{s+1}} = \big(\omega_j \omega_k^{2^s} + \omega_k \omega_j^{2^s}\big)^2$, so

$$J_i = \sum_{s=1}^{i} \mu_{i-s}^{2^s} M_s(A)^2.$$

Thus $J_0 = 0$. Since $\mu_0 = 1$, the moment $M_i(A)^2$ occurs in J_i with coefficient one, and induction on i shows that the first two conditions are equivalent. Solving downward instead, with $\omega^{(i-1)} = \sqrt{\omega^{(i)}} + \sqrt{\mu_i}\,\omega$, induction on s gives constants $\nu_{s,r} \in \mathbb{B}$ with $\omega^{(d-1-s)} = \sum_{r=0}^{s} \nu_{s,r}\, \omega^{2^{-r}}$: start with $\nu_{0,0} = \eta$, and step with $\nu_{s+1,0} = \sqrt{\mu_{d-1-s}}$ and $\nu_{s+1,r+1} = \sqrt{\nu_{s,r}}$. Since $\omega_j^2 \omega_k^{2^{-r}} + \omega_k^2 \omega_j^{2^{-r}} = \big(\omega_j \omega_k^{2^{r+1}} + \omega_k \omega_j^{2^{r+1}}\big)^{2^{-r}}$,

$$J_{d-1-s} = \sum_{r=0}^{s} \nu_{s,r}\, M_{r+1}(A)^{2^{-r}}.$$

Here $\nu_{s,s} = \eta^{2^{-s}} \neq 0$, so induction on s shows that the first and third conditions are equivalent. Under these conditions only the coefficients $J_t, \dots, J_{d-t}$ remain, and every remaining exponent is divisible by 2^t. □

Lemma 5.9 (Rank under the moment equations)**.** Let $2 \leq t \leq d/2$, and let $A \neq 0$ satisfy $M_1(A) = \cdots = M_{t-1}(A) = 0$. Then A has rank at least $2t$. If its rank is exactly $2t$, and V is the polar radical, of size $N/2^{2t}$, then

$$J = J_{d-t}\, L_V^{2^t}, \qquad J_{d-t} \neq 0, \qquad \deg J = \frac{N}{2^t}.$$

Proof. By Lemma 5.6 and (5.4), the polar radical V is the set of roots of $\widehat{J}$ in D. Since $A \neq 0$, we have $V \neq D$, so $\widehat{J} \neq 0$, and $|V| = N/2^{\operatorname{rank} A}$ is at most $\deg \widehat{J} \leq N/2^{2t}$. If the rank is $2t$, the polynomial $\widehat{J}$ vanishes on all $N/2^{2t}$ points of V, so it is a constant multiple of L_V. □

Level sets. The next lemma concerns only the functions on D and does not use the moment equations.

Lemma 5.10 (Level sets of a quadratic function)**.** Let A have rank $2t$ with $1 \le t \le d/2$, let V be its polar radical, and put $T = N/2 - N/2^{t+1}$. Exactly 2^{2t} labels $\omega \in \widehat{D}$ make ψ vanish on V. For each of them, ψ is constant on every coset of V, and exactly one $\kappa \in \mathbb{F}_2$ makes $\psi + \kappa$ take the value one at T points of D and the value zero at the other $N - T$.

Proof. For $v \in V$ and $x \in D$, we have $\psi_A(x + v) = \psi_A(x) + \psi_A(v)$, so ψ_A is linear on V. The function ψ vanishes on V exactly when ℓ_ω agrees with ψ_A on V. By Lemma 5.5, exactly 2^{2t} labels ω have this property, one for each extension to D of the linear function $\psi_A|_V$. Fix one. Then $\psi(x + v) = \psi(x)$ for $v \in V$, and the signed sum $\sigma = \sum_{x \in D} (-1)^{\psi(x)}$ satisfies

$$\sigma^2 = \sum_{u \in D} (-1)^{\psi(u)} \sum_{x \in D} (-1)^{B_\psi(x,u)} = N|V| = \frac{N^2}{2^{2t}},$$

because the inner sum is N for $u \in V$, where $\psi(u) = 0$, and zero otherwise. So $\sigma = \pm N/2^t$. The function $\psi + \kappa$ takes the value one at $(N - (-1)^\kappa \sigma)/2$ points, which equals T exactly when $(-1)^\kappa \sigma > 0$. □

Matching the degree to the number of zeros. The rank of A and the moment equations bound the same degree from opposite sides.

Remark 5.11 (Rank, moments, and degree). Let A have rank $2r > 0$, choose ω and κ as in Lemma 5.10, and let $H = Q + \kappa$ be the polynomial of $\psi + \kappa$. By (5.3), $H^2 + H = \Lambda H'$ with $H' = J + \varepsilon_A + \omega^2$, and $J \neq 0$, so $\deg H = (N + \deg J)/2$. The polynomial H is nonzero and vanishes at the zeros of $\psi + \kappa$, so

$$\deg H \ge \frac{N}{2} + \frac{N}{2^{r+1}}, \qquad \text{that is,} \qquad \deg J \ge \frac{N}{2^r}.$$

By Lemma 5.8, the equations $M_1(A) = \cdots = M_{t-1}(A) = 0$ hold exactly when $\deg J \le N/2^t$. Together these give $r \ge t$ again, and for $r = t$ the degree of H equals the number of zeros of $\psi + \kappa$. Then every root of H lies in D. The next lemma uses this case.

Lemma 5.12 (Gold moments give polynomials with many roots)**.** Fix a basis $\omega_1, \dots, \omega_d$ of the label space $\widehat{D}$, let $2 \le t \le d/2$, and put

$$T = \frac{N}{2} - \frac{N}{2^{t+1}}, \qquad R = \sqrt{L_D - \lambda_0 X} = \sum_{i=1}^{d} \sqrt{\lambda_i}\, X^{2^{i-1}}.$$

Each alternating binary $d \times d$ matrix A of rank $2t$ with $M_1(A) = \cdots = M_{t-1}(A) = 0$ gives 2^{2t} distinct monic polynomials

$$P = R + C \in \mathbb{B}[X], \qquad \deg C = \frac{T}{2} = \frac{N}{4} - \frac{N}{2^{t+2}},$$

one for each label ω of Lemma 5.10. The roots of P on D are the T points where $\psi + \kappa$ takes the value one. The polynomials from different matrices are also distinct. Every polynomial P of this family has the following properties.

1. It satisfies
$$P'(P^2 + L_D) = \lambda_0 P. \tag{5.5}$$
2. Its set of roots on D is a union of cosets of a subspace of D of dimension $d - 2t$.
3. It takes the same value as any other polynomial of the family at at most $N/2^{2t}$ points outside D, in any field containing $\mathbb{B}$.

Proof. Fix such a matrix A, with polar radical V, and one of the 2^{2t} labels ω of Lemma 5.10, with its κ. Let $H = Q + \kappa$ be the polynomial of $\psi + \kappa$. By Lemma 5.6, $H^2 + H = \Lambda H'$ with $H' = Q'$.

The polynomial P. By Lemmas 5.8 and 5.9, $H' = J + \varepsilon_A + \omega^2 = U^2$ with $U = \widehat{J}^{2^{t-1}} + \sqrt{\varepsilon_A + \omega^2}$ of degree $N/2^{t+1}$. Since $t \geq 2$, every exponent in U is even and $U' = 0$. Leading terms in $H^2 + H = \Lambda U^2$ give $\deg H = N/2 + N/2^{t+1} = N - T$ and $\mathrm{lc}(H) = \eta\,\mathrm{lc}(U)$. So H has as many zeros in D as its degree: its roots are simple and lie in D. Since $N \geq 2^{2t} \geq 16$, the number T is even with $2 \leq T < N/2$, and Lemma 3.16 applies with $\lambda = \lambda_0$. It gives the polynomial

$$P = \eta U \frac{L_D}{H}, \qquad P^2 = L_D + \frac{L_D}{H}, \qquad \deg(P + R) = \frac{T}{2},$$

whose roots on D are the T points where $\psi + \kappa = 1$. If E is this set, then $L_D/H = L_E/\mathrm{lc}(H)$, so $L_E = \mathrm{lc}(H)\,(C^2 + \lambda_0 X)$ with $C = P + R$, the form announced at the start of this subsection. By Lemma 5.10 they form a union of cosets of V, which is the second property, and P is monic because $\mathrm{lc}(H) = \eta\,\mathrm{lc}(U)$. Dividing $H^2 + H = \eta^2 L_D U^2$ by $\eta^2 U^2 H$ gives $P = (H + 1)/(\eta U)$. Differentiating $\eta U P = H + 1$ gives $P' = U/\eta$, and then $P'(P^2 + L_D) = (U/\eta)(L_D/H) = P/\eta^2 = \lambda_0 P$, which is the first property.

Distinctness. The derivative $P' = U/\eta$ determines $Q' = U^2$. Two polynomials satisfying (5.3) with the same derivative differ by a polynomial Y with $Y^2 = Y$, a constant, and $Q(0) = 0$; so Q' determines Q. In turn Q determines ψ, hence the pair (A, ω). So distinct pairs (A, ω) give distinct polynomials P.

Collisions outside D. Let $P_1 \neq P_2$ belong to the family, and let $\beta \notin D$, in a field containing $\mathbb{B}$, satisfy $P_1(\beta) = P_2(\beta)$. Since $P(\beta)^2 + L_D(\beta) = L_D(\beta)/H(\beta) \neq 0$, (5.5) gives $P_1'(\beta) = P_2'(\beta)$, that is, $U_1(\beta) = U_2(\beta)$. By the formula for U,

$$U_1 + U_2 = G^{2^{t-1}}, \qquad G = \widehat{J_1} + \widehat{J_2} + \varepsilon_0, \qquad \deg G \leq \frac{N}{2^{2t}},$$

for a constant ε_0. By the previous paragraph, $U_1 \neq U_2$, so $G \neq 0$, and β is one of its at most $N/2^{2t}$ roots. □

Rank two. For $d \geq 3$, Lemma 3.16 also applies at polar rank two, where there is no moment equation. For a subspace $W \leq D$ of codimension two with locator $L_W = X^{N/4} + a_W X^{N/8} + \cdots$, it gives the polynomial $L_W^2 + (a_W^2 + \theta)L_W$ from the proof of Theorem 4.1, with $\theta = \sqrt{\lambda_{d-1}}$.

5.4 Counting matrices of rank $2t$

Lemma 5.13 (Rank-$2t$ solutions of the moment equations)**.** Let $D \subseteq \mathbb{F}_{2^m}$ be binary additive of dimension d, let $\omega_1, \ldots, \omega_d$ be a basis of its label space, and let $2 \leq t \leq n = \lfloor d/2 \rfloor$, with ι and $\Delta \geq 1$ as in Theorem 5.1. Let C be the space of alternating binary $d \times d$ matrices A with $M_1(A) = \cdots = M_{t-1}(A) = 0$, and let C_{2r} be the set of its matrices of rank $2r$. Then

$$|C_{2t}| \geq \begin{bmatrix} n \\ t \end{bmatrix}_4 (2^\Delta - 1). \tag{5.6}$$

Proof. An alternating matrix has $\binom{d}{2}$ free binary entries, and each of the $t - 1$ moment equations imposes at most m binary linear constraints, so $|C| \geq 2^{\binom{d}{2} - m(t-1)}$. By Lemma 5.9, C_{2r} is empty for $0 < r < t$. It remains to count the matrices of rank exactly $2t$.

For alternating matrices A and B, put

$$\langle A, B \rangle = \sum_{i<j} A_{ij} B_{ij} \in \mathbb{F}_2, \qquad \chi_B(A) = (-1)^{\langle A, B \rangle}.$$

For $0 \le j \le n$ and a matrix A of rank $2r$, the sum $\pi_j(r) = \sum_{\operatorname{rank} B = 2j} \chi_B(A)$ depends only on r; these are the numbers $F_j^{(d)}(r)$ of Schmidt [44, Proposition 3.3], whose pairing of the quadratic function with polar matrix A and the alternating matrix B is $\langle A, B\rangle$. The moment identity of Delsarte and Goethals [22, Eq. (29)], also stated in [44, Eq. (13)], gives for $0 \le s, r \le n$

$$\sum_{j=0}^{s} \begin{bmatrix} n-j \\ n-s \end{bmatrix}_4 \pi_j(r) = 2^{(d-\iota)s} \begin{bmatrix} n-r \\ s \end{bmatrix}_4 . \tag{5.7}$$

Let $C_{2j}^{\perp}$ be the set of rank-$2j$ matrices B with $\langle A, B\rangle = 0$ for every $A \in C$. The sum of χ_B over C is $|C|$ for such B and zero for other B. Summing over all B of rank $2j$ and grouping the A by rank,

$$\sum_{r=0}^{n} |C_{2r}|\, \pi_j(r) = |C|\, |C_{2j}^{\perp}|.$$

Multiply by $\begin{bmatrix} n-j \\ n-s \end{bmatrix}_4$, sum over $0 \le j \le s$, apply (5.7), and take $s = n - t$. On the left, only $r = 0$ and $r = t$ remain: the Gaussian binomial vanishes for $r > t$, and C_{2r} is empty for $0 < r < t$. On the right, keep the term $j = 0$. This gives

$$2^{(d-\iota)(n-t)} \left(\begin{bmatrix} n \\ t \end{bmatrix}_4 + |C_{2t}| \right) \ge |C| \begin{bmatrix} n \\ t \end{bmatrix}_4 , \qquad \text{so} \qquad |C_{2t}| \ge \begin{bmatrix} n \\ t \end{bmatrix}_4 \left(\frac{|C|}{2^{(d-\iota)(n-t)}} - 1 \right).$$

Inserting the bound on $|C|$ and the identity $\binom{d}{2} - m(t-1) - (d-\iota)(n-t) = \Delta$, checked separately for even and odd d, proves (5.6). □

5.5 Proof of the counting bound

Proof of Theorem 5.1. By Lemmas 5.13 and 5.12, applied to a basis of the label space, there are L distinct polynomials $P_i = R + C_i$ $(1 \le i \le L)$ as in Lemma 5.12, with $\deg C_i = T/2 < N/4$. On the roots of P_i, the word $R|_D$ agrees with the codeword $C_i|_D$. The C_i are distinct of degree less than N, so this is the decoding list.

For the pair, let $\beta \in \mathbb{F} \setminus D$ and apply Lemma 3.11 with message length $N/4$ to $f_0(x) = R(x)/(x-\beta)$ and $g(x) = 1/(x-\beta)$. This gives $\operatorname{agr}_{N/4}(g) = \operatorname{CA}_{N/4}(f_0, g) = N/4$, and each $z_i = C_i(\beta)$ is exceptional at agreement T with a witness of degree $T/2 - 1$. Since $z_i = z_j$ exactly when $P_i(\beta) = P_j(\beta)$, the colliding pairs, summed over the $q - N$ poles, number at most $\delta\binom{L}{2}$, and Lemma 3.19 gives a pole with at least Z distinct values z_i. Finally, by Lemma 3.13 for $b = 2$, replacing f_0 by $f(x) = \sqrt{\lambda_0/(x-\beta)}$ translates the challenges by a constant and gives $\operatorname{agr}_{N/4}(f) \le 3N/8 - 1 < T$. So zero is not exceptional, and all Z challenges are nonzero. The second term of Z is at least $L/2$ when $\delta(L-1) \le q-N$, and at least $L(q-N)/(2\delta(L-1)) \ge (q-N)/(2\delta)$ otherwise, which gives the lower bound in (5.1). For an affine translate $D + a$, substitute $X - a$ for X and $\beta + a$ for β. □

5.6 Increasing agreement and rate by padding

The unused degree in Theorem 5.1 lets us add agreement points by multiplying the inputs and witnesses by a subspace locator. We choose the subspace to control its overlap with the old agreement sets.

Lemma 5.14 (Adding an additive set of common roots)**.** Let D be a binary additive space of dimension d, with $N = 2^d$, and let $\beta \notin D$. Suppose the received pair $f(x) = R(x)/(x-\beta)$, $g(x) = 1/(x-\beta)$ has L distinct

selected nonzero challenges with witnesses of degree less than K_0. Suppose each agreement set has size T and is invariant under translation by a subspace of dimension $d - 2t$. Fix $2t \le s < d$, and put

$$w = 2^s, \qquad K = K_0 + w < N, \qquad p_{d,s,r} = \frac{2^{r(d-s)} \begin{bmatrix} d-r \\ s-r \end{bmatrix}_2}{\begin{bmatrix} d \\ s \end{bmatrix}_2}.$$

There is a received pair with common agreement exactly K and at least $\lceil p_{d,s,2t} L \rceil$ selected nonzero challenges at agreement

$$T + w\left(1 - \frac{T}{N}\right).$$

Proof. Put $r = 2t$ and choose an s-dimensional subspace B of D uniformly at random. For a fixed codimension-r subspace V, the condition $B + V = D$ forces $\dim(B \cap V) = s - r$. Choose this intersection first. In the quotient by it, $B/(B \cap V)$ must complement $V/(B \cap V)$; relative to one complement, all choices are graphs of linear maps. Hence there are

$$\begin{bmatrix} d-r \\ s-r \end{bmatrix}_2 2^{r(d-s)}$$

successful subspaces, giving probability exactly $p_{d,s,r}$. The Gaussian product formula also gives

$$p_{d,s,r} = \prod_{j=0}^{r-1} \frac{1 - 2^{j-s}}{1 - 2^{j-d}}.$$

If an agreement set S is invariant under translation by V and $B + V = D$, every coset of V meets B in exactly 2^{s-2t} points. Consequently $|B \cap S| = wT/N$. Averaging over B shows that one choice has this property for at least $\lceil p_{d,s,2t} L \rceil$ selected challenges. Pad by this B (Definition 3.17). Each padded witness has degree less than K, and its agreement set is exactly $S_z \cup B$, of size $T + w - wT/N$, proving the claimed threshold.

The second input is $L_B(x)/(x - \beta)$, with $L_B(\beta) \neq 0$ and $\deg L_B \le K$. Lemma 3.11 gives exact common agreement K. □

Corollary 5.15 (Gold families at rate $1/2$)**.** Under the hypotheses of Theorem 5.1, suppose $2t \le d - 2$, and let Z be its bound (5.1). On the same domain and over the same challenge field, there is a pair with

$$\mathrm{CA}_{N/2}(f, g) = N/2, \qquad |\operatorname{Bad}_{T_{1/2}}(f, g) \setminus \{0\}| \ge \lceil p_{d,d-2,2t} Z \rceil, \qquad T_{1/2} = \frac{5N}{8} - \frac{3N}{2^{t+3}}.$$

Consequently the dense-domain quasipolynomial counts also hold at rate $1/2$ and agreement tending to $5/8$, with common-agreement gap tending to $1/8$.

Proof. For each distinct nonzero challenge, choose one witness from Theorem 5.1. Its agreement set is the root set of the corresponding polynomial P_i, which by the second property in Lemma 5.12 is invariant under translation by a subspace of dimension $d - 2t$. Its degree is below $N/4$. Apply Lemma 5.14 with $K_0 = N/4$ and $s = d - 2$. The new message length is $N/2$, the selected proportion is $p_{d,d-2,2t}$, and the agreement is $T + (N/4)(1 - T/N) = T_{1/2}$. The product formula gives $p_{d,d-2,2t} \ge 1 - 2^{2t+2-d}$, since its numerator is at least $1 - \sum_{j<2t} 2^{j-d+2}$ and each factor of its denominator is less than one. For the choices of t in Corollary 5.2 we have $t \le d/4$, so $p_{d,d-2,2t} = 1 - o(1)$. □

The agreement tends to $5/8$, below the rate-$1/2$ Johnson threshold $1/\sqrt{2}$. Section 6 gives a different construction that also applies to sparse domains.

Multiplying every polynomial by one common locator moves these lists to every fixed rate $\rho \ge 5/8$. This costs a fixed fraction of the agreement gap, but the agreement stays a constant above the rate.

Corollary 5.16 (Higher rates on every dense binary domain)**.** Fix integers $c \geq 0$ and $r \geq 1$ and a rate ρ with

$$1 - 3 \cdot 2^{-r-2} \leq \rho < 1 - 2^{-r-2}.$$

For every sufficiently large d and every additive d-space $D \subseteq \mathbb{B} = \mathbb{F}_{2^{d+c}}$, put $N = 2^d$ and $K = \lfloor \rho N \rfloor$. There is an integer T with

$$\frac{T}{N} = \frac{1+\rho}{2} - 2^{-r-3} - o(1)$$

such that the following hold.

1. Some word in $\mathbb{B}^D$ agrees with at least $N^{\Omega_{c,r}(\log N)}$ polynomials of degree less than K over $\mathbb{B}$ on at least T points each.
2. Over an extension $\mathbb{F}$ of $\mathbb{B}$ with $|\mathbb{F}| = N^{O_{c,r}(\log N)}$, there is a pair with

$$\operatorname{agr}_K(g) = \operatorname{CA}_K(f,g) = K, \qquad |\operatorname{Bad}_T(f,g) \setminus \{0\}| \geq N^{\Omega_{c,r}(\log N)}.$$

The limiting agreement fraction exceeds ρ by $(1-\rho)/2 - 2^{-r-3} > 0$ and is below $\sqrt{\rho}$. The windows for $r \geq 1$ cover every rate in $[5/8, 1)$.

For instance, $r = 1$ and $\rho = 5/8$ give agreement tending to $3/4$. The proof is in Appendix A.1.

Placing all padding roots outside the subspace reaches every fixed rate, at a limiting agreement fraction that exceeds the rate by 2^{-r-2}.

Corollary 5.17 (Every fixed rate on every dense binary domain)**.** Fix an integer $c \geq 0$, a rate $0 < \rho < 1$, and an integer $r \geq 1$ with $2^{-r-2} < \min\{\rho, (1-\rho)/3, \sqrt{\rho} - \rho\}$. For every sufficiently large d and every additive d-space $D \subseteq \mathbb{B} = \mathbb{F}_{2^{d+c}}$, with $N = 2^d$ and $K = \lfloor \rho N \rfloor$, the two conclusions of Corollary 5.16 hold for an integer T with $T/N = \rho + 2^{-r-2} - o(1)$. The limiting agreement fraction lies strictly between ρ and $\sqrt{\rho}$. The same holds on every translate $D + a$ with $a \in \mathbb{B}$.

Proof. Choose a subspace $D_0 \subseteq D$ of codimension r, and put $N_0 = |D_0| = 2^{-r}N$. Then $|\mathbb{B}| = 2^{c+r}N_0$, so Corollary 5.2 applies to D_0 with $c + r$ in place of c. As in the proof of Theorem 5.1, it gives polynomials $R + C_i$ over $\mathbb{B}$, for $1 \leq i \leq L$, with distinct C_i of degree less than $N_0/4$, each with exactly T_0 roots in D_0, where

$$T_0 = \frac{N_0}{2} - o(N_0), \qquad \log_2 L = \Theta_{c,r}\big((\log N)^2\big).$$

Let $S_i \subseteq D_0$ be the root set of $R + C_i$.

Padding outside the subspace. Put $w = K - N_0/4$. For large d, the number $N_0/4 = 2^{-r-2}N$ is an integer, and the hypotheses $2^{-r-2} < \rho$ and $3 \cdot 2^{-r-2} < 1 - \rho$ give

$$\frac{N_0}{4} \leq \lfloor \rho N \rfloor = K \leq \rho N < N - \frac{3N_0}{4}, \qquad \text{hence} \qquad 0 \leq w < N - N_0.$$

Choose any set $E \subseteq D \setminus D_0$ of size w, and put $\Pi = L_E$, of degree w. Each polynomial $\Pi(R + C_i) = \Pi R + \Pi C_i$ vanishes on $E \cup S_i$. The two sets are disjoint, since E lies outside D_0. Their union has

$$T = w + T_0 = K + \frac{N_0}{4} - o(N)$$

points, and $T/N = \rho + 2^{-r-2} - o(1)$. This limit exceeds ρ, and it is below $\sqrt{\rho}$ because $2^{-r-2} < \sqrt{\rho} - \rho$.

The polynomials ΠC_i have coefficients in $\mathbb{B}$ and degree less than $w + N_0/4 = K$, and they are distinct because the C_i are. At every root of $\Pi R + \Pi C_i$, the word ΠR equals ΠC_i. So the word $(\Pi R)|_D$ agrees with each ΠC_i on at least T points. Since $L = N^{\Omega_{c,r}(\log N)}$, this proves the first conclusion.

Distinct challenges. Let $\mathbb{F}$ be the smallest extension of $\mathbb{B}$ with $|\mathbb{F}| \geq NL$. Its size is at most $|\mathbb{B}|NL = N^{O_{c,r}(\log N)}$, and for large d at least $|\mathbb{F}|/2$ of its elements lie outside $\mathbb{B}$. For such a pole β, we have $\Pi(\beta) \neq 0$, since the roots of Π lie in D. Hence the values $(\Pi C_i)(\beta)$ and $(\Pi C_j)(\beta)$ collide only if β is a root of $C_i - C_j$, which happens for fewer than $N_0/4$ poles. Summed over all poles outside $\mathbb{B}$, there are at most $(N_0/4)\binom{L}{2}$ colliding pairs. Lemma 3.19 gives a pole $\beta \notin \mathbb{B}$ with at least

$$L - \frac{(N_0/4)\binom{L}{2}}{|\mathbb{F}|/2} \;\geq\; L - \frac{N_0 L}{4N} \;\geq\; \frac{3L}{4}$$

distinct values $z_i = (\Pi C_i)(\beta)$, at most one of them zero.

Apply Lemma 3.11 at this pole, with message length K, to the polynomials $\Pi R + \Pi C_i$. It gives the pair

$$f(x) = \frac{\Pi(x)R(x)}{x - \beta}, \qquad g(x) = \frac{1}{x - \beta} \qquad (x \in D),$$

with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$, and each z_i lies in $\mathrm{Bad}_T(f, g)$. At least $3L/4 - 1 = N^{\Omega_{c,r}(\log N)}$ of them are distinct and nonzero, which proves the second conclusion.

Translates. For $D + a$ with $a \in \mathbb{B}$, substitute $X - a$ for X in every polynomial above. Degrees are unchanged and root sets move by a. Evaluating the new polynomials at a pole β evaluates the old ones at $\beta - a$, which also lies outside $\mathbb{B}$. Both conclusions therefore carry over. □

5.7 A concrete bound for Binius64

Binius64 evaluates on domains that lie in a small subfield of its field, which places them in the range of Theorem 5.1; Corollary 5.18 gives the resulting bound. Binius64 uses the field $\mathbb{F}_{2^{128}} = \mathbb{F}_2[X]/(X^{128} + X^7 + X^2 + X + 1)$ for its codewords and its challenges [13]. It fixes a basis $\beta_0, \ldots, \beta_{127}$ of this field over $\mathbb{F}_2$ with

$$\beta_0 = 1, \qquad \beta_{i-1} = \beta_i^2 + \beta_i \quad (1 \leq i \leq 127),$$

and encodes a message of length 2^k at rate 2^{-r} on the domain $V_d = \mathrm{span}_{\mathbb{F}_2}\{\beta_0, \ldots, \beta_{d-1}\}$ of dimension $d = k + r$.

To see that $V_d \subseteq \mathbb{F}_{2^{32}}$ for $d \leq 32$, put $A(X) = X^2 + X$. The recurrence says $A(\beta_i) = \beta_{i-1}$ and $A(\beta_0) = 0$, so 32 successive applications of A send each of $\beta_0, \ldots, \beta_{31}$ to zero. Two applications of A give $X^4 + X$, four give $X^{16} + X$, and 32 give $X^{2^{32}} + X$, whose roots are the elements of $\mathbb{F}_{2^{32}}$. Hence $V_{32} = \mathbb{F}_{2^{32}}$, and $V_d \subseteq \mathbb{F}_{2^{32}}$ for every $d \leq 32$.

As an example we take $d = 27$, the domain for messages of length 2^{25} at rate $1/4$ and of length 2^{26} at rate $1/2$.

Corollary 5.18 (A 128-bit-field example)**.** Let D be any binary 27-space in $\mathbb{F}_{2^{32}}$, or any affine translate. Put $N = 2^{27}$, $K = 2^{25}$, and $\mathbb{F} = \mathbb{F}_{2^{128}}$. There is a fixed pair over $\mathbb{F}$ with $\mathrm{CA}_K(f, g) = K$ and more than 3.4248×10^{29} distinct nonzero exceptional challenges at agreement

$$\frac{T}{N} = \frac{16193}{32768} \approx 0.49417.$$

For a uniformly sampled challenge in $\mathbb{F}$, the exceptional probability is greater than $2^{-29.889}$. The pair can be chosen so that both inputs are individually far, with

$$\mathrm{agr}_K(f) \leq \frac{193N}{512} - 1, \qquad \mathrm{agr}_K(g) = \frac{N}{4}.$$

Proof. We first apply Theorem 5.1, then use the remaining degree allowance to increase agreement by locator padding. It suffices to prove the linear-domain case; translation gives the affine cases. With $d = 27$ and $m = 32$, the hypothesis of Theorem 5.1 is $\Delta = 32 - 5t \geq 1$, so $t = 6$ is the largest admissible choice. It gives $\Delta = 2$, $\delta = 2^{15}$, and

$$L = 2^{12} \cdot 3 \begin{bmatrix} 13 \\ 6 \end{bmatrix}_4 \approx 3.45167 \times 10^{29}.$$

Some members of this family may give the same challenge. With $q = 2^{128}$, the first term in (5.1) is the larger, and it counts

$$Z = L - \left\lfloor \frac{\delta \binom{L}{2}}{q - N} \right\rfloor \approx 3.45161 \times 10^{29}$$

distinct nonzero challenges at agreement $T_0 = 63N/128$. The witnesses have degree less than $K_0 = N/4 - N/256$.

The degree bound leaves room to multiply both inputs and their witnesses by a locator of degree $w = N/256$. This adds agreement wherever that locator vanishes. Apply Lemma 5.14 with $s = 19$ and $w = 2^{19} = N/256$. By the second property in Lemma 5.12, each agreement set is a union of cosets of the radical of its quadratic polar form. That radical has dimension $d - 2t = 15$, which gives the translation invariance required by the padding lemma. Here

$$p_{27,19,12} = \prod_{j=0}^{11} \frac{1 - 2^{j-19}}{1 - 2^{j-27}} \approx 0.9922399879.$$

The final message length is $K_0 + w = K$, the nonzero count after padding is $Z' = \lceil p_{27,19,12} Z \rceil \approx 3.424826 \times 10^{29}$, and the agreement is $T_0 + w(1 - T_0/N) = 16193N/32768$. Finally $128 - \log_2 Z' = 29.888054438\ldots$.

To obtain the additional bounds on each input individually, use the first input of Lemma 3.13 before padding. Its numerator differs from the fixed polynomial used in Theorem 5.1 by a polynomial of degree at most $N/8$. For the received word this adds a fixed polynomial of degree at most $N/8 - 1 < K_0$ and a scalar multiple of g, so the witness degrees remain strictly below K and the agreement sets are unchanged. This first input has agreement below T_0, so all selected challenges are nonzero. The padding locator has degree $w = N/256$, and the padded bound in that lemma gives $3N/8 + w/2 - 1 = 193N/512 - 1$. The agreement of the padded second input, and the common agreement of the pair, remain exactly K. □

The combination agreement is about 0.58 percentage points below Johnson and 24.42 percentage points above the inputs' common agreement. Thus the counterexample also rules out any permitted proximity loss smaller than this common-agreement gap (Section 3.1). Before padding, the same construction gives a single received word with L nearby codewords over the smaller field $\mathbb{F}_{2^{32}}$ at agreement $63/128$.

At rate $1/2$ on the same domain, Corollary 5.15 gives agreement $317/512$ from common agreement $1/2$, with at least $\lceil p_{27,25,12} Z \rceil > 3.45123 \times 10^{29}$ nonzero exceptional challenges, or exceptional probability greater than $2^{-29.877}$.

5.8 A concrete bound for Google's Longfellow

Longfellow's evaluation domains are not additive. Each of the four domains we analyze contains an affine subspace of 2048 points, and the Gold construction on that subspace, padded on the remaining points, gives a counterexample on the whole domain (Corollary 5.19). We first describe the domains, following the specification [29] and version 7 of the implementation [28].

Attributes	e	N	Common agreement K	Combination agreement T	T/N
1	4151	3230	461	845	26.16%
2	4265	3318	474	858	25.86%
3	4307	3352	478	862	25.72%
4	4415	3436	490	874	25.44%

Table 4: Longfellow's version-7 binary code parameters and the agreement $T = K + 384$ of Corollary 5.19.

The domains. The challenge field is $\mathbb{F}_{2^{128}}$. Longfellow fixes an element g such that $1, g, \ldots, g^{15}$ is a basis of the subfield $\mathbb{F}_{2^{16}}$ over $\mathbb{F}_2$ [29, Section 2.2.2]. For an integer $0 \le j < 2^{16}$ with bits $j_0, \ldots, j_{15}$, put $\mathrm{inj}(j) = \sum_i j_i g^i$. This map is $\mathbb{F}_2$-linear in the bits, so it sends the integers $c2^k, \ldots, (c+1)2^k - 1$ to an affine subspace of dimension k.

A row of the prover's witness has e entries, where $e < 2^{16}$ is fixed for each circuit. It holds the values at $\mathrm{inj}(0), \ldots, \mathrm{inj}(e-1)$ of a polynomial of degree less than $K = \lfloor (e+1)/9 \rfloor$. The first $2K - 1$ positions hold the message and the further evaluations that determine a product of two rows. The prover reveals combinations of rows through their values at these positions, and for zero knowledge it commits only to the remaining positions, which are the ones the verifier queries. The tests therefore concern the Reed–Solomon code of message length K on

$$S = \{\mathrm{inj}(j) : 2K - 1 \le j < e\}, \qquad N = |S| = e - 2K + 1.$$

Writing $e + 1 = 9K + r$ with $0 \le r \le 8$ gives $N = 7K + r$, so the rate is at most $1/7$. The run $2K - 1, \ldots, e - 1$ starts and ends inside a block, so S is not an affine subspace. Table 4 lists the four configurations.

Corollary 5.19 (Longfellow's version-7 codes)**.** Let (e, N, K) be one of the four rows of Table 4, let S be the corresponding domain, and put $\mathbb{F} = \mathbb{F}_{2^{128}}$. There is a fixed pair over $\mathbb{F}$ with $\mathrm{CA}_K(f, g) = K$ and at least 5,843,376 distinct nonzero exceptional challenges at agreement $T = K + 384$. For a uniformly sampled challenge in $\mathbb{F}$, the exceptional probability is greater than $2^{-105.522}$.

Proof. In all four rows $2K - 1 \le 2048$ and $e \ge 4096$, so S contains

$$U = \{\mathrm{inj}(j) : 2048 \le j < 4096\} = g^{11} + \mathrm{span}_{\mathbb{F}_2}\{1, g, \ldots, g^{10}\},$$

an affine 11-space in $\mathbb{F}_{2^{16}}$. The Gold family of Lemma 5.12 and Lemma 5.13, translated to U, with $d = 11$, $m = 16$, $t = 2$, and $\Delta = 6$, gives

$$L = 16(2^6 - 1)\begin{bmatrix} 5 \\ 2 \end{bmatrix}_4 = 5{,}843{,}376$$

distinct polynomials $P_i = R + C_i$, each with 768 roots in U and $\deg C_i = 384$. Let A be the locator of any $K - 384$ points in $S \setminus U$. Then $AP_i = AR + AC_i$ has correction degree K and at least $K + 384$ roots in S. Pole reduction on S (Lemma 3.11) gives common agreement exactly K and combination agreement at least $T = K + 384$.

Each nonzero polynomial $A(C_i - C_j)$ or AC_i has degree at most K. Thus at most $K\binom{L}{2} + L < 2^{128} - N$ poles cause a challenge collision or a zero challenge. Some pole outside S therefore retains all L nonzero challenges, giving probability $L/2^{128} = 2^{-105.521629\ldots} > 2^{-105.522}$. □

The common agreement K is about 14.3% of N, the least possible, since any two words agree with a pair of codewords on any K positions. The exceptional combinations have agreement about 12 percentage points below the Johnson agreement of about 37.8% (Table 4). Longfellow's security analysis uses the unique-decoding radius, at agreement about 57.1% [28]. The specification states a security target of at

least 115 bits [29, Section 5.1], and the implementation records about 109 bits of statistical security. A proximity-gap guarantee for these codes at agreement T/N or lower, with proximity loss below 384 positions, has error greater than $2^{-105.522}$, which is too large for either figure. The thresholds between T/N and Johnson remain open.

5.9 Superpolynomial decoding lists and exceptional sets at further rates

This subsection extends the Gold construction to every characteristic (Theorem 5.22) and, on dense binary domains, to every fixed rate with both individual agreements equal to the common agreement (Corollary 5.24). The proof of Theorem 5.22 follows that of Theorem 5.1, with bth powers in place of squares (as before Lemma 3.13) and a classical family of quadratic forms in place of the Gold moments.

5.9.1 Quadratic-form constructions in every characteristic

Definition 5.20 (Quadratic forms, radicals, and rank)**.** Let W be a vector space over $\mathbb{F}_b$, where b is a prime power. A *quadratic form* $\psi : W \to \mathbb{F}_b$ is a function represented by a homogeneous polynomial of degree two in linear coordinates. Its polar form is $B_\psi(x, y) = \psi(x + y) - \psi(x) - \psi(y)$. Its *quadratic radical* is

$$\operatorname{rad}(\psi) = \{u \in W : B_\psi(x, u) = 0 \text{ for every } x \in W,\ \psi(u) = 0\}.$$

The *rank* of ψ is the codimension of $\operatorname{rad}(\psi)$ in W.

In contrast to the polar radical in Definition 3.15, this definition also requires $\psi(u) = 0$. We use the quadratic rank throughout this subsection. A form ψ induces a form with zero radical on the quotient $W/\operatorname{rad}(\psi)$. A form of rank $2t$ has *elliptic type* if this induced form is an orthogonal sum of $t - 1$ hyperbolic planes, each equivalent to xy, and one plane on which the form vanishes only at zero. The induced form then has nondegenerate polar form, so the polar radical of ψ equals $\operatorname{rad}(\psi)$ and ψ vanishes on it. For a function χ that is a quadratic form plus a linear function plus a constant, we write $B_\chi(x, y) = \chi(x + y) - \chi(x) - \chi(y) + \chi(0)$, which is again bilinear.

As in Section 5.3, ψ and χ denote functions, and Q and G denote polynomials representing them.

Write $\operatorname{Tr}_j = \operatorname{Tr}_{\mathbb{F}_{b^j}/\mathbb{F}_b}$.

Proposition 5.21 (The trace family)**.** Let b be a prime power, $m = 2n$, $\mathbb{B} = \mathbb{F}_{b^m}$, and $2 \le t \le n$. Consider the quadratic forms on $\mathbb{B}$

$$\psi(x) = \sum_{i=t}^{n-1} \operatorname{Tr}_m(a_i x^{b^i+1}) + \operatorname{Tr}_n(a_n x^{b^n+1}), \qquad a_i \in \mathbb{B}, \quad a_n \in \mathbb{F}_{b^n}.$$

1. At least $(b^t - 1)\begin{bmatrix} n \\ t \end{bmatrix}_{b^2}$ of these forms have rank $2t$ and *elliptic* type [44, Theorems 5.6 and 4.9].
2. A form of rank $2t$ and elliptic type on a space of size N has exactly $N/b - (b - 1)N/b^{t+1}$ zeros.
3. The canonical representative Q of ψ is a combination of monomials $X^{b^j+b^k}$ with $0 \le j < k < m$ and $t \le k - j \le m - t$. Its derivative is

$$Q' = \sum_{i=t}^{n-1} \left(a_i X^{b^i} + a_i^{b^{m-i}} X^{b^{m-i}}\right) + a_n X^{b^n},$$

   which contains only powers X^{b^i} with $t \le i \le m - t$.
4. The polar form of ψ determines ψ within the family, in every characteristic.

5. For every $\xi \in \mathbb{B}^*$, the dilation $x \mapsto \xi x$ maps the family to itself and preserves rank and type.

The proof is in Appendix A.2.

Theorem 5.22 (Quadratic-form families on full fields and hyperplanes)**.** Let b be a prime power, $m = 2n$, and $\mathbb{B} = \mathbb{F}_{b^m}$. Let $D = \mathbb{B}$ or an $\mathbb{F}_b$-hyperplane in $\mathbb{B}$, and write $d = \dim_{\mathbb{F}_b} D$, $h = m - d \in \{0, 1\}$, and $N = b^d$. Choose $2 \le t \le n - h$, and put

$$K = \frac{N}{b^2}, \qquad T = \frac{N}{b} - \frac{(b-1)N}{b^{t+1}}, \qquad L = b^{2t}\,\frac{b^t - 1}{b - 1}\begin{bmatrix} n-h \\ t \end{bmatrix}_{b^2}, \qquad \delta = \frac{(b-1)N}{b^{2t}}.$$

Then there is a received word on D over $\mathbb{B}$ with at least L distinct codewords of $C_K(D;\mathbb{B})$, each agreeing with it on exactly T coordinates. For every finite extension $\mathbb{F} \supseteq \mathbb{B}$, with $q = |\mathbb{F}| > N$, there is a received pair satisfying $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$ and having at least Z distinct nonzero exceptional challenges at agreement T, where Z is given by (5.1) with these values of L, δ, and q. The pair can be chosen to satisfy $\mathrm{agr}_K(f) \le (b+1)N/(2b^2) - 1 < T$.

The proof is in Appendix A.2.

Corollary 5.23 (Decoding lists approaching Johnson)**.** Fix a prime power b. For $N = b^{2n}$ and all sufficiently large n, the full-length Reed–Solomon code over $\mathbb{F}_N$ of dimension $K = N/b^2$ has a received word with at least $N^{\Omega_b(\log N)}$ distinct codewords agreeing on a fraction

$$\frac{1}{b} - \Theta_b(N^{-1/4}) = \sqrt{K/N} - \Theta_b(N^{-1/4})$$

of its coordinates. The received word can be chosen as $r(x) = x^{N/b}$. In particular, $b = 2^k$ gives rate 4^{-k} for every fixed integer $k \ge 1$, over an alphabet of size N.

The proof is in Appendix A.2.

For fixed b, the same choice $t = \lfloor n/2 \rfloor$ in Theorem 5.22, with a sufficiently large containing field, also gives quasipolynomial exceptional sets. Their fractional common-agreement gap approaches $(b-1)/b^2$. For example, $b = 4$ gives rate $1/16$ and agreement approaching $1/4$, while $b = 3$ gives rate $1/9$ and agreement approaching $1/3$. These are fields of fixed characteristic, so the examples do not contradict bounds for prime fields or sufficiently large characteristic.

For $b = 2$, Theorem 5.1 gives at least as large a count at the same rate and agreement, on the full field and on its hyperplanes, and a strictly larger one when $t < n$: its factor is $2^{2n-t} - 1$ in place of $2^t - 1$. It also applies to every additive domain with $\Delta \ge 1$. The count is larger because Theorem 5.1 uses every alternating form of rank $2t$ that satisfies the moment equations. In characteristic two an added linear function and, if necessary, the complement give each such form a level set of size T. For $b > 2$ a level set of a quadratic function has size T only if it is a translate of the zero set of a form of elliptic type, so Theorem 5.22 counts those forms alone.

5.9.2 Superpolynomial lists and exceptional sets at every fixed binary rate

Restricting the agreement sets of Theorem 5.22 to a prescribed dense binary domain and applying balanced padding reaches every fixed rate. Corollary 5.17 already gives such bounds; here the agreement is $\alpha_{b,c}(\rho)$, and both individual agreements equal the common one.

Corollary 5.24 (Every fixed rate on dense binary domains)**.** Fix a binary codimension $c \ge 0$ and a binary power $b > 2^c$. Let $\mathbb{B} = \mathbb{F}_{b^{2n}}$, and let $D \subseteq \mathbb{B}$ be any affine binary subspace of codimension c, of size $N = |\mathbb{B}|/2^c$. Fix a rate ρ with

$$\frac{2^c}{b^2} < \rho < 1 - \frac{2^c}{b} + \frac{2^c}{b^2},$$

and put

$$K = \lfloor \rho N \rfloor, \qquad \alpha_{b,c}(\rho) = \frac{1}{b} + \left(\rho - \frac{2^c}{b^2}\right)\left(1 - \frac{1}{b}\right).$$

There are received words on D, over the alphabet $\mathbb{B}$ of size $2^c N$, with $N^{\Omega_b(\log N)}$ distinct codewords of $C_K(D;\mathbb{B})$ at agreement at least $\alpha_{b,c}(\rho) - O_{b,c}(N^{-1/4})$ as a fraction of the domain. There are also pairs on D, over extensions $\mathbb{F} \supseteq \mathbb{B}$ of size $N^{O_{b,c}(\log N)}$, with $\mathrm{agr}_K(f) = \mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = K$ and $N^{\Omega_b(\log N)}$ distinct nonzero exceptional challenges at that agreement. The estimates are uniform over D. Moreover,

$$\rho < \alpha_{b,c}(\rho) < \sqrt{\rho}.$$

For every fixed c and $\rho \in (0,1)$, a sufficiently large fixed binary power b places ρ in this interval.

The proof is in Appendix A.2.

6 Decision-tree constructions at half agreement and half rate

This section proves the decision-tree results outlined in Section 2.4: Corollary 6.7 at agreement $1/2$ and Theorem 6.10 at rate $1/2$. Throughout, D is a binary additive domain of size N, and the challenge field is any field of size $q > N$ that contains D.

6.1 From unions of flats to exceptional challenges

Both constructions use the following consequence of pole reduction. In it, T_0 is the common size of the sets, w bounds the degree gap of the locators of their flats, and W is the reserved set: it is empty in the first construction and a subspace of size w in the second. The message length is K and the agreement is T.

Lemma 6.1 (Unions of flats give exceptional challenges)**.** Let $D \subseteq \mathbb{F}$ be binary additive of size N, with $q = |\mathbb{F}| > N$. Let $w \geq 1$ be an integer, and let $W \subseteq D$ be empty or of size w. Let $\mathcal{A}$ be a family of $M \geq 1$ distinct nonempty subsets of $D \setminus W$ of a common size T_0, each a disjoint union of affine flats of size at least $2w$. Put

$$K = T_0 - w + |W|, \qquad T = T_0 + |W|,$$

write I_x for the number of sets of $\mathcal{A}$ containing x, and let F be any number with

$$F \geq (K - |W|)\binom{M}{2} - \sum_{x \in D \setminus W} \binom{I_x}{2}. \tag{6.1}$$

Then there is a pair of words on D with

$$\mathrm{CA}_K(f,g) = \mathrm{agr}_K(g) = K, \qquad \mathrm{agr}_K(f) \leq T - 1,$$

and at least

$$Z(M,F) = \max\left\{M - \left\lfloor \frac{F}{q-N} \right\rfloor, \left\lceil \frac{(q-N)M^2}{(q-N)M + 2F} \right\rceil\right\} \tag{6.2}$$

distinct nonzero exceptional challenges at agreement T. If $F \leq NM^2/8$, then $Z(M,F) \geq \min\{M/2, q/N\}$.

The right side of (6.1) bounds the number of triples of two sets and a pole for which the two sets give the same challenge. The sum subtracts the points that two sets share, since a shared point is a common root inside D and leaves one fewer possible collision outside D. The first term of $Z(M,F)$ is the better one when collisions are rare, and the second when the sets outnumber the available challenges.

Proof. We write L_S for the locator of a set S, and $L_\emptyset = 1$.

Step 1: shared coefficients. An affine flat of size 2^r with $r \geq 1$ has locator X^{2^r} plus terms of degree at most 2^{r-1} (Section 3.2). For $A \in \mathcal{A}$, multiply the locators of its flats. Using a nonleading term of any factor lowers the degree by at least w, so

$$L_A = X^{T_0} + G_A, \qquad \deg G_A \leq T_0 - w.$$

Put $R = X^{T_0} L_W$ and $C_A = L_W G_A$. Then $R + C_A = L_{W \cup A}$ is monic of degree T with all its roots in D, and $\deg C_A \leq K$, where $1 \leq K < T \leq N$. Distinct sets give distinct corrections C_A.

Step 2: pole reduction. For each $\beta \in \mathbb{F} \setminus D$, the second pair of Lemma 3.11 has the stated common and individual agreements. Its second input is $1/(x - \beta)$; the overview's $L_W(x)/(x - \beta)$ equals $L_W(\beta)/(x - \beta)$ plus a polynomial of degree less than w, so it gives the same exceptional set up to the factor $L_W(\beta)$. For each A it gives the nonzero challenge $L_{W \cup A}(\beta)$, with a witness of degree less than K that agrees with the combination exactly on $W \cup A$.

Step 3: collisions. Two sets $A \neq A'$ give the same challenge at β exactly when β is a root of $C_A - C_{A'}$. This nonzero polynomial has degree at most K and vanishes on $W \cup (A \cap A')$, so it has at most $K - |W| - |A \cap A'|$ roots outside D. Summing over unordered pairs, and using $\sum_{\{A,A'\}} |A \cap A'| = \sum_x \binom{I_x}{2}$, the total number of colliding pairs over all $q - N$ poles is at most the right side of (6.1). Lemma 3.19 gives a pole with at least $Z(M, F)$ distinct challenges.

Step 4: the simplified bound. Since q and N are powers of two, $q \geq 2N$. If $2F \leq NM^2/4$, the second term of $Z(M, F)$ is at least

$$\frac{(q - N)M}{q - N + NM/4} \geq \min\left\{\frac{M}{2}, \frac{2(q - N)}{N}\right\} \geq \min\left\{\frac{M}{2}, \frac{q}{N}\right\}. \qquad \square$$

6.2 Counting balanced tree supports

We now construct many sets with this decomposition, as supports of balanced Boolean functions (Definition 3.14): the root sets of Section 2.4 are these supports, and its leaves are their flats. For independent linear functionals s, a, b, the function $(1 + s)a + sb$ of Figure 2 tests s and then outputs a or b.

To count the functions we must recognize when two trees define the same one. We do this with two invariants of a Boolean function: the directions it ignores, and the linear functionals it depends on.

Definition 6.2 (Translation periods and essential coordinates)**.** For a Boolean function $\varphi : U \to \mathbb{F}_2$ on a finite binary vector space U, its *translation-period space* is

$$\mathrm{Per}(\varphi) = \{u \in U : \varphi(x + u) = \varphi(x) \text{ for every } x \in U\}.$$

Write U^* for the space of *linear functionals* $U \to \mathbb{F}_2$, and $E^\perp \leq U$ for the common kernel of a subspace $E \leq U^*$. The *essential dual space* of φ is the space of linear functionals vanishing on $\mathrm{Per}(\varphi)$, and its dimension is the *essential dimension* of φ.

A period is a direction that φ ignores. The function φ can be written in terms of the functionals in its essential dual space, and of no smaller space of functionals, so the essential dimension is the least number of linear tests that determine φ. In linear coordinates $x_1, \ldots, x_d$ on U, every Boolean function is a unique polynomial in which each variable has exponent at most one. Products are reduced using $x_i^2 = x_i$. The *degree* of the function is the degree of this polynomial; it is preserved by invertible affine changes of coordinates.

For $h \geq 3$, a function computed by such a tree of height h determines the first test and the two functions computed below it (Lemma 6.5), so a recursive definition counts each function once. At height two this fails. On a three-dimensional space the support of $(1 + s)a + sb$ consists of four points, which can be split into two lines in three ways, and each way gives a different first test for the same function. We therefore define height two by properties of the function, and show in Lemma 6.4 that these are the functions computed by trees of height two with three independent functionals.

Definition 6.3 (Tree functions)**.** Put $t_h = 2^h - 1$, and let U be a finite binary vector space. A *height-two tree function* on U is a balanced Boolean function of degree two and essential dimension three. For $h \geq 3$, a Boolean function φ on U is a *height-h tree function* if there are a nonzero $s \in U^*$, a point p with $s(p) = 1$, and subspaces $L_0, L_1 \leq (\ker s)^*$ such that:

1. L_0 and L_1 have dimension t_{h-1}, and $L_0 \cap L_1 = 0$;
2. the restriction φ_0 of φ to $\ker s$ is a height-$(h-1)$ tree function with essential dual space L_0;
3. the function $\varphi_1 : x \mapsto \varphi(p + x)$ on $\ker s$ is a height-$(h-1)$ tree function with essential dual space L_1.

We call s a *root functional* of φ and φ_0, φ_1 its *children*.

In coordinates s, x, y adapted to s, L_0, and L_1, such a function is

$$\varphi = (1 + s)\varphi_0(x) + s\varphi_1(y).$$

It tests s and then evaluates one of two trees of height $h - 1$. The condition $L_0 \cap L_1 = 0$ says that the two subtrees use independent functionals. The essential dimension is then $t_h = 1 + 2t_{h-1}$, although each path makes only h tests (Section 2.4).

Lemma 6.4 (Structure of tree functions)**.** Fix $h \geq 2$ and a binary vector space U of dimension $d \geq t_h$.

1. Every height-h tree function on U is balanced and has degree h and essential dimension t_h. Its support is a union of 2^{h-1} disjoint affine flats of codimension h.
2. The height-h tree functions are closed under invertible affine changes of coordinates and under complementation.
3. Let φ be a Boolean function on U and let $P \leq \mathrm{Per}(\varphi)$. Then φ is a height-h tree function exactly when the function it induces on U/P is one.
4. There are exactly 56 height-two tree functions on a space of dimension three.

Proof. We use induction on h. A Boolean function φ on U and the function it induces on the quotient by a subspace $P \leq \mathrm{Per}(\varphi)$ have the same degree and essential dimension, and one is balanced exactly when the other is. This proves the third part at height two.

Height two. On $\mathbb{F}_2^3$ there are $\binom{8}{4} = 70$ four-point sets, of which 14 are affine planes. The indicator of a four-point set equals one at an even number of points, so it has no cubic term, and it is affine exactly when the set is a plane. The balanced functions of degree two on $\mathbb{F}_2^3$ are therefore the indicators of the 56 nonplanar sets. None has a nonzero period, which would split its support into two parallel lines, whose union is a plane. So all 56 have essential dimension three, which is the fourth part. Any partition of a nonplanar support into two pairs writes it as a union of two nonparallel affine lines, and a linear functional separating them is the first test of a tree of height two for the function. Affine changes and complementation preserve the 56 sets. This proves the first two parts on $\mathbb{F}_2^3$. On U, a height-two tree function with essential dual space E is induced from one on the three-dimensional quotient $U/E^\perp$, and the first two parts follow on U.

The recursive step. Let $h \geq 3$, put $r = t_{h-1}$, and let φ be a height-h tree function with data s, L_0, L_1. By induction the height-$(h-1)$ tree functions are closed under translations, and changing the point p translates φ_1, so the definition holds for every choice of p. Each child is balanced with 2^{h-2} disjoint flats of codimension $h-1$ in its slice ($\ker s$ or $p + \ker s$), so φ is balanced and its support has the stated form. A period $u \in \ker s$ of φ is a period of both children, that is, a vector of $(L_0 + L_1)^\perp$, and conversely. Here $\perp$ denotes the annihilator in $\ker s$. A period $u \notin \ker s$ would make a translate of one child equal to the other. A function of the functionals in L_0 that is also a function of those in L_1 is constant on $L_0^\perp + L_1^\perp = \ker s$, which contradicts balance. Hence $\mathrm{Per}(\varphi) = (L_0 + L_1)^\perp$ has dimension $d - 1 - 2r = d - t_h$. Affine changes and complementation transport the data and the children, possibly exchanging the two slices.

For the degree, choose coordinates on U consisting of s, coordinates x and y whose restrictions to $\ker s$ are bases of L_0 and L_1 and which vanish at p, and further coordinates z. Then

$$\varphi = (1 + s)\varphi_0(x) + s\varphi_1(y), \tag{6.3}$$

where φ_0, φ_1 have degree $h-1$ by induction. Let $\Omega_0(x)$ and $\Omega_1(y)$ be their parts of degree $h-1$. The part of φ of degree h is $s(\Omega_0 + \Omega_1)$, which is nonzero because Ω_0 and Ω_1 involve different variables.

For the third part, the data s, L_0, L_1 vanish on $\mathrm{Per}(\varphi)$, so they are defined on U/P. Every period lies in $\ker s$ and is a period of both children, so the children are defined on the two slices of U/P, with the same essential dual spaces. By the induction hypothesis applied to the children, the function induced on U/P is a height-h tree function with these data, and conversely. □

Lemma 6.5 (The root functional is unique)**.** Let $h \geq 3$. A height-h tree function φ has only one root functional s: it is the only nonzero linear functional ℓ for which $\ell\varphi$ has degree at most h. It determines the child φ_0 and, once the point p is fixed, the child φ_1, and hence their essential dual spaces L_0 and L_1.

Proof. Use the coordinates s, x, y, z and the notation of (6.3). First, $s\varphi = s\varphi_1(y)$ has degree at most h. Conversely, write $\ell = as + u(x) + v(y) + c(z)$ with $a \in \mathbb{F}_2$ and linear forms u, v, c. The part of $\ell\varphi$ of degree $h+1$ is s times the part of degree h of

$$(u + v + c)(\Omega_0 + \Omega_1).$$

The products $v\Omega_0$, $c\Omega_0$, $u\Omega_1$, and $c\Omega_1$ need no reduction, and their monomials contain, respectively, $h-1$ variables x and one y; $h-1$ variables x and one z; one x and $h-1$ variables y; and $h-1$ variables y and one z. The remaining products $u\Omega_0$ and $v\Omega_1$ involve only x and only y. Since $h - 1 \geq 2$, these six kinds of monomials are all different, so each product vanishes in degree h. As Ω_0 and Ω_1 are nonzero, $v = c = 0$ and $u = 0$, so $\ell = s$. The functional s determines the restrictions of φ to its two slices, which are the children. □

At height two the kinds of $v\Omega_0$ and $u\Omega_1$ coincide and the two products can cancel. This is the algebraic form of the three root decompositions of one function noted before Definition 6.3.

Lemma 6.6 (Counting tree functions)**.** Fix $h \geq 2$ and a binary vector space U of dimension $d \geq t_h$. The number of height-h tree functions on U is

$$B_h(d) = \begin{bmatrix} d \\ t_h \end{bmatrix}_2 C_h, \qquad C_2 = 56, \qquad C_h = (2^{t_h} - 1)\begin{bmatrix} 2t_{h-1} \\ t_{h-1} \end{bmatrix}_2 2^{t_{h-1}^2} C_{h-1}^2 \quad (h \geq 3),$$

and C_h of them have any prescribed essential dual space. For fixed h, $B_h(d) = \Theta_h(2^{dt_h})$. Every point of U lies in the supports of exactly half of these functions.

Proof. First let $d = t_h$. For $h = 2$ the count is the fourth part of Lemma 6.4. Let $h \geq 3$ and $r = t_{h-1}$, so $d = 2r + 1$. There are $2^{t_h} - 1$ choices of s; fix a point p for each. There are then $\begin{bmatrix} 2r \\ r \end{bmatrix}_2 2^{r^2}$ ordered pairs of complementary r-spaces L_0, L_1 in the $2r$-dimensional space $(\ker s)^*$, and by induction C_{h-1} children with each prescribed essential dual space. By Lemma 6.5 different choices give different functions, which proves the recurrence for C_h.

In general, by the third part of Lemma 6.4, the tree functions with a prescribed essential dual space E are induced from the C_h tree functions on the t_h-dimensional space $U/E^\perp$, and there are $\begin{bmatrix} d \\ t_h \end{bmatrix}_2$ spaces E. The Gaussian coefficient has order 2^{dt_h} for fixed h. Finally, complementation pairs the functions, and each point lies in the support of exactly one function of each pair. □

Corollary 6.7 (Half agreement on the whole domain)**.** Let $D \subseteq \mathbb{F}$ be binary additive of size $N = 2^d$, with $q = |\mathbb{F}| > N$. Fix $h \geq 2$ with $d \geq t_h = 2^h - 1$, and put

$$T = N/2, \qquad K = N/2 - N/2^{h+1}, \qquad M = B_h(d), \qquad F = K\binom{M}{2} - N\binom{M/2}{2},$$

where B_h is defined in Lemma 6.6. There is a pair of words on D with

$$\mathrm{CA}_K(f, g) = \mathrm{agr}_K(g) = K, \qquad \mathrm{agr}_K(f) \leq T - 1,$$

and at least $Z(M, F)$ distinct nonzero exceptional challenges at agreement T, with Z as in (6.2). For fixed h, this count is $\Omega_h(\min\{N^{2^h-1}, q/N\})$. In particular, at rate $3/8$ it is $\Omega(\min\{N^3, q/N\})$ at agreement $1/2$, and hence cubic in N when $q \geq N^4$.

Proof. Apply Lemma 6.1 to the supports of the height-h tree functions on D, with W empty, $T_0 = N/2$, and $w = N/2^{h+1}$. By Lemmas 6.4 and 6.6, these are M distinct unions of flats of size $N/2^h = 2w$, and every point lies in exactly $M/2$ of them, so (6.1) holds with equality. Since $F = \frac{1}{2}[(N/4 - w)M^2 + wM] \leq NM^2/8$, the count is at least $\min\{M/2, q/N\}$, and $M = \Theta_h(N^{2^h-1})$. □

6.3 Rate one half: supports avoiding a subspace

To reach rate $1/2$ we keep the same flats and reserve a subspace W of size $w = N/2^{h+1}$ for additional agreement points (Figure 3). The supports must now be disjoint from W. We impose this recursively, in a form that is easy to count. The root functional is required to vanish on W. Then W lies in the slice where it equals zero, the other slice is disjoint from W whatever its child is, and the child on the first slice must again avoid W.

Definition 6.8 (Tree functions avoiding a subspace)**.** Let $W \leq U$ be a subspace of codimension $h + 1$. A height-two tree function on U is *W-avoiding* if it vanishes on W. For $h \geq 3$, a height-h tree function is W-avoiding if its root functional s vanishes on W and its restriction φ_0 to $\ker s$ is W-avoiding.

The support of a W-avoiding tree function is disjoint from W. For $h \geq 3$ there may be other tree functions with this property. We do not count them, and a lower bound on the number of supports is all we need.

Lemma 6.9 (Counting tree supports that avoid a subspace)**.** Let $h \geq 2$, let U be a binary vector space of dimension $d \geq t_h$, and let $W \leq U$ have codimension $h + 1$. The number $M_h(d)$ of W-avoiding height-h tree functions on U satisfies

$$M_2(d) = 28\big(6 \cdot 2^{d-3} - 5\big),$$
$$M_h(d) = (2^{h+1} - 1)\, M_{h-1}(d-1)\, 2^{t_{h-1}^2} \begin{bmatrix} d - 1 - t_{h-1} \\ t_{h-1} \end{bmatrix}_2 C_{h-1} \qquad (h \geq 3),$$

with C_{h-1} as in Lemma 6.6. For each fixed h, $M_h(d) = \Theta_h(2^{d(2^h-h-1)})$.

Proof. We use induction on h, counting the functions by their recursive data.

Step 1: height two. A height-two tree function φ is $ab + e + c$ with linearly independent $a, b, e \in U^*$ and $c \in \mathbb{F}_2$. Indeed, on its three-dimensional essential quotient its polar form (Definition 3.15) is nonzero and alternating, so it has rank two and is the polar form of ab for independent a, b; then $\varphi + ab$ is affine, say $e + c$, and $e \notin \langle a, b\rangle$ because the essential dimension is three. Conversely, each such expression is a height-two tree function. The function determines $E = \langle a, b\rangle$, which is spanned by the functionals $x \mapsto \varphi(x + y) + \varphi(x) + \varphi(y) + \varphi(0)$, and the functions with a given E are the $ab + e + c$ with $e \notin E$, for any fixed basis a, b of E. Let $W^\perp \le U^*$ be the three-dimensional space of functionals vanishing on W. There are three cases.

- If $E \le W^\perp$, then ab vanishes on W, so the function vanishes on W exactly when $c = 0$ and $e \in W^\perp \setminus E$. The seven spaces E give $7 \cdot 4 = 28$ functions.
- If $E \cap W^\perp = \langle a\rangle$, again ab vanishes on W, and the condition is $c = 0$ and $e \in W^\perp \setminus \{0, a\}$, giving six functions. There are seven choices of $\langle a\rangle \le W^\perp$, and then $2^{d-1} - 4$ planes through a not contained in $W^\perp$, so there are $28(2^{d-3} - 1)$ such spaces E.
- If $E \cap W^\perp = 0$, then a and b are independent on W, so ab is not affine on W and no function vanishes on W.

In total $M_2(d) = 28 + 6 \cdot 28(2^{d-3} - 1)$.

Step 2: the recurrence. Let $h \ge 3$ and $r = t_{h-1}$. There are $2^{h+1} - 1$ nonzero functionals s vanishing on W. In $\ker s$, which has dimension $d - 1$, the space W has codimension h, so there are $M_{h-1}(d - 1)$ choices of a W-avoiding child. Let L_0 be its essential dual space. The r-spaces $L_1 \le (\ker s)^*$ with $L_0 \cap L_1 = 0$ number $2^{r^2}\begin{bmatrix} d-1-r \\ r \end{bmatrix}_2$: choose the image of L_1 in $(\ker s)^*/L_0$, then a linear map from it to L_0. Such a space exists because $d \ge 2r + 1$. Finally there are C_{h-1} children on the other slice with essential dual space L_1. By Lemma 6.5, different choices give different functions.

Step 3: the order of growth. For fixed h, the Gaussian coefficient has order 2^{dr} and the other new factors are constants. The exponent e_h of 2^d therefore satisfies $e_2 = 1$ and $e_h = e_{h-1} + 2^{h-1} - 1$, so $e_h = 2^h - h - 1$. □

At height three, which gives agreement $9/16$ below, and with $w = 2^d/16$,

$$M_3(d) = 71680(6w - 5)(w - 1)(w - 2)(w - 4) \sim (105/16)\, 2^{4d}.$$

Theorem 6.10 (Decision-tree construction at rate $1/2$)**.** Let $D \subseteq \mathbb{F}$ be binary additive of size $N = 2^d$, let $q = |\mathbb{F}| > N$, and fix $h \ge 3$ with $d \ge 2^h - 1$. Put $K = N/2$ and $w = N/2^{h+1}$, and let $M = M_h(d) = \Theta_h(N^{2^h-h-1})$ be the count of Lemma 6.9. There is one received pair with

$$\mathrm{CA}_K(f, g) = \mathrm{agr}_K(g) = K, \qquad \mathrm{agr}_K(f) \le K + w - 1,$$

and at least $\min\{M/2,\ q/N\} = \Omega_h(\min\{N^{2^h-h-1}, q/N\})$ distinct nonzero exceptional challenges at agreement $K + w = (1/2 + 2^{-h-1})N$. More precisely, the count is at least $Z(M, F)$ of (6.2) with

$$F = \frac{1}{2}\left[\left(K - w - \frac{K^2}{N - w}\right) M^2 + wM\right];$$

Section 6.4 evaluates this bound.

Proof. Fix a subspace $W \le D$ of size w, and apply Lemma 6.1 to the supports A of the W-avoiding height-h tree functions on D, with $T_0 = K$. By Lemmas 6.4 and 6.9, these are M distinct subsets of $D \setminus W$, each a union of flats of size $N/2^h = 2w$. Since $\sum_{x \notin W} I_x = KM$, Cauchy–Schwarz over the $N - w$ points outside W gives

$$\sum_{x \notin W} \binom{I_x}{2} \ge \frac{1}{2}\left(\frac{K^2M^2}{N-w} - KM\right),$$

so

$$(K-w)\binom{M}{2} - \sum_{x \notin W} \binom{I_x}{2} \le F,$$

which is (6.1). This gives the pair and the bound $Z(M, F)$. Since $K - K^2/(N-w) < N/4$ and $M \ge 1$, we have $F \le NM^2/8$, so $Z(M, F) \ge \min\{M/2, q/N\}$, and $M = \Theta_h(N^{2^h - h - 1})$. □

Heights $h = 3, 4, 5$ give agreement fractions $9/16$, $17/32$, and $33/64$, with $M_h(d)$ of order N^4, N^{11}, and N^{26}, for d at least 7, 15, and 31. The counted supports give $\Theta_h(M_h(d))$ distinct challenges once $q \ge NM_h(d)$, and for every $h \ge 3$ the guaranteed count grows faster than N^2 whenever $q/N^3 \to \infty$. The same proof applies at height two, at agreement $5/8$, where $M_2(d) = \Theta(N)$ gives only $\Omega(\min\{N, q/N\})$ challenges.

Suppose D lies in a proper subfield $\mathbb{B}$ of $\mathbb{F}$ with $|\mathbb{B}| > N$. Then the theorem over $\mathbb{B}$, followed by Lemma 3.12, gives a pair over $\mathbb{F}$ at the same agreement $K + w$ whose two individual agreements both equal the common agreement K. The count is that of the theorem with $|\mathbb{B}|$ in place of q, since the conversion preserves every counted nonzero challenge.

6.4 Concrete bounds for the parameters of LeanVM and Flock

LeanVM and Flock both have configurations at rate $1/2$ on additive domains of length $N = 2^{22}$, spanned by the first 22 powers of a generator of $\mathbb{F}_{2^{64}}$ and of $\mathbb{F}_{2^{128}}$ respectively (Section 5.1). LeanVM draws its challenges from $\mathbb{F}_{2^{192}}$ and Flock from $\mathbb{F}_{2^{256}}$ [25, 42].[3] These domains are too sparse for the Gold construction, but Theorem 6.10 applies to every additive domain of this length. The received words of our pairs take values in the challenge field $\mathbb{F}$.

Take $\mathbb{F} = \mathbb{F}_{2^{192}}$ and $N = 2^{22}$. At height three, Theorem 6.10 gives more than 2.0309×10^{27} distinct nonzero challenges at rate $1/2$ and agreement $9/16$. The exceptional probability is greater than $2^{-101.286}$.

At height four the same theorem gives a much larger exceptional set at agreement $17/32$ (Table 6). For $N = 2^{22}$ and $\mathbb{F} = \mathbb{F}_{2^{192}}$, the bound $Z(M, F)$ of (6.2) exceeds 2^{172}, and the exceptional probability is at least 2^{-20}. For $\mathbb{F} = \mathbb{F}_{2^{256}}$ and the same N, put $M = M_4(22)$ and take F as in the theorem. Direct substitution gives $(2^{256} - N)(M - 2^{229} - 1) > F$, and the first term of $Z(M, F)$ then counts more than 2^{229} nonzero exceptional challenges, a probability greater than 2^{-27}. A proximity-gap guarantee at agreement $17/32$ with proximity loss below $1/32$ can therefore certify at most 20 bits of soundness for LeanVM and fewer than 27 for Flock.

The two fields are in different regimes of the collision bound. At $d = 22$ the support count is $M_4(22) \approx 2^{229.5}$, well below its asymptotic order $N^{11} = 2^{242}$. Over $\mathbb{F}_{2^{192}}$ the supports far outnumber the distinct challenges that the collision bound can guarantee: the second term of $Z(M, F)$ is approximately $q/(0.21N)$, so the probability bound is about $4.7/N$ and does not improve as the challenge field shrinks. Over $\mathbb{F}_{2^{256}}$ nearly all M supports give distinct challenges, and the probability is about M/q.

[3] The Flock paper specifies $\mathbb{F}_{2^{128}}$ throughout [17, Section 5], whereas the implementation snapshot we analyze uses $\mathbb{F}_{2^{256}}$ for proximity-test challenges [25].

Result and rate	Domain and challenge field	Agreement of combination α	Common γ	Exceptional count
Superpolynomial count at every rate Any fixed $0 < \rho < 1$ Corollary 5.17	Every affine translate of a dense binary additive domain; suitable $q = N^{O(\log N)}$	$\alpha_0 - o(1)$, $\rho < \alpha_0 < \sqrt{\rho}$	$\lfloor \rho N \rfloor / N$	$N^{\Omega(\log N)}$
Every challenge at every rate Any fixed $0 < \rho < 1$ Theorem 4.5	Every additive domain; $q \le N^a$ for any fixed $a \ge 1$	A fixed threshold $\rho < \alpha < \sqrt{\rho}$	$\lfloor \rho N \rfloor / N$	q exactly
Cubic count at half agreement $\rho = 3/8$ Corollary 6.7	Every additive domain; $q > N$	$1/2$	$3/8$	$\Omega(\min\{N^3, q/N\})$ Cubic in N when $q \ge N^4$
Higher powers at half rate $\rho = 1/2$ Theorem 6.10	Every additive domain; $q > N$, fixed $h \ge 3$, and $\log_2 N \ge 2^h - 1$	$1/2 + 2^{-h-1}$	$1/2$	$\Omega_h(\min\{N^{e_h}, q/N\})$ $e_h = 2^h - h - 1$

Table 5: Counterexamples at a fixed positive gap above the code rate, with agreement bounded away from Johnson. Notation is as in Table 1, and N is sufficiently large.

Domain	N	$\log_2 q$	ρ	Agreement α	Common γ	Probability	Source
Binius64's V_{27}	2^{27}	128	$1/4$	0.49417	$1/4$	$> 2^{-29.889}$	Cor. 5.18
Binius64's V_{27}	2^{27}	128	$1/2$	0.61914	$1/2$	$> 2^{-29.877}$	Cor. 5.15
Every additive domain in $\mathbb{F}_{2^{128}}$	2^{20}	128	$1/16$	$1/4 - 1/N$	$1/8 - 1/N$	$> 2^{-90.585}$	Cor. 4.2
Every additive domain in $\mathbb{F}_{2^{64}}$	2^{20}	64	$1/8$	$3/16$	$1/8$	$> 2^{-28.585}$	Cor. 4.6
Every additive domain in $\mathbb{F}_{2^{192}}$	2^{22}	192	$1/2$	$17/32$	$1/2$	$\ge 2^{-20}$	Thm. 6.10
Every additive domain in $\mathbb{F}_{2^{256}}$	2^{22}	256	$1/2$	$17/32$	$1/2$	$> 2^{-27}$	Thm. 6.10

Table 6: Concrete lower bounds on the probability that $f + zg$ agrees with a codeword on at least an α fraction of positions, for a uniformly random challenge z in a field of size q. Here γ is the inputs' common agreement fraction. The fourth row covers the domains of the 2018 implementation of Ben-Sasson, Bentov, Horesh, and Riabzev [5]; its probability is per challenge, and that implementation draws two independent challenges.

7 Summary of results and deployed systems

Table 1, in the introduction, summarizes the results that approach or reach Johnson, and Table 5 summarizes those at a fixed gap above the rate, with their domain and field assumptions. Table 6 gives numerical bounds for selected parameters, and the rest of this section relates them to deployed binary-field systems.

Scope. None of the current systems discussed here (Binius64, BinarySpartan, Longfellow, LeanVM, and Flock) relies on beyond-Johnson proximity-gap conjectures. Binius64, BinarySpartan, and Longfellow use guarantees at the unique-decoding radius [13, 28, 45]. LeanVM uses Johnson-bound guarantees, as does Flock's default configuration, which targets 128 bits of security [25, 42]. Flock's configuration named Secure targets 120-bit security and uses the smaller unique-decoding radius, requiring more queries and larger proofs.

Our counterexamples therefore do not show that these systems are insecure as currently configured; they rule out the proposed proof-size reductions from beyond-Johnson proximity-gap guarantees in the parameter regimes covered by our results. Our received words also take values in the challenge field. If both words take values in a subfield $\mathbb{B}$ containing the domain, then by (3.1) every challenge that is exceptional at an agreement above $\mathrm{CA}_K(f, g)$ lies in $\mathbb{B}$, and the exceptional probability is at most $|\mathbb{B}|/|\mathbb{F}|$.

Dense and sparse domains. The Gold construction applies to Binius64, whose domains lie in a 32-bit subfield of its challenge field (Section 5.7 and the first two rows of Table 6), and to Longfellow, whose domains contain a 2048-point affine subspace: there the bound is $2^{-105.522}$ at agreement about 26%, against a Johnson agreement of about 37.8% (Corollary 5.19). LeanVM and Flock evaluate on domains that lie in no small subfield (Section 5.1). On them our rate-$1/2$ bounds (Section 6.4 and the last two rows of the table) hold at agreement $17/32$, close to capacity and well below Johnson (about 70.71%), and leave beyond-Johnson guarantees at that rate open.

Small challenge fields. Many hash-based SNARKs use challenge fields of about 128 bits and target 100 to 120 bits of security; BinarySpartan [45], for example, uses $\mathbb{F}_{2^{128}}$. Over such fields, the quadratic count of Corollary 4.2 already limits what a beyond-Johnson guarantee can certify on additive domains (Table 6, third row). The same holds for the 2018 implementation of Ben-Sasson, Bentov, Horesh, and Riabzev [5, Appendix B.8] (fourth row): an analysis that counts each exceptional challenge as a failure can certify at most 57.17 of its targeted 60 bits (Section 4.2), a limit on the analysis rather than an attack on the implementation.

8 Discussion and open questions

Sparse domains near Johnson. On prescribed sparse domains, such as spans of the first few powers of a fixed field element, Theorem 4.1 gives $\Omega(N^2)$ exceptional challenges at rate $1/16$, within a constant number of positions of Johnson and with a common-agreement gap of $N/8$ positions. Can the count grow faster than N^2 at such thresholds, with a fixed positive fractional common-agreement gap? The classification in Theorem 4.1 shows that this requires a different pair f, g: the pair constructed there has no further challenges with more than $N/8$ agreements. The Gold moment equations still define valid candidates on sparse domains, but the LeanVM and Flock domains fail the hypothesis $\Delta \geq 1$ under which Lemma 5.13 gives solutions of the required rank. At rate $1/4$ even a quadratic count near Johnson is open on these domains: Theorem 4.7 gives $2N - 2$ challenges at agreement $1/2$.

Rates other than $1/b^2$. Even on dense domains, our counterexamples approach Johnson only at rates $1/b^2$. Removing the linear term of an $\mathbb{F}_b$-subspace locator leaves a bth power, which gives agreement b times the degree, and this equals Johnson only at rate $1/b^2$. We reach the other rates by padding, which raises the degree bound faster than the agreement. At rate $1/2$, for instance, Corollary 5.15 gives superpolynomial counts at agreement approaching $5/8 = 0.625$, while Johnson is $1/\sqrt{2} \approx 0.707$. Whether a proximity gap, or a polynomial list-size bound, holds between these two thresholds is open, as it is at every rate covered only by Corollary 5.16, 5.17, or 5.24.

Explicit domains in binary fields. Every construction in this paper uses the vanishing polynomial of a subspace, and Theorem 4.1 excludes additive domains at rate $1/16$. Over a binary field, by contrast, randomly chosen evaluation points satisfy guarantees up to capacity with high probability [31, 32], as do the explicit points of Alrabiah, Goyal, and Guruswami [1] in binary extension fields of polynomial size. Is there an

explicit family of domains in binary fields that supports fast encoding and on which proximity gaps hold beyond Johnson?

Protocols. Can pairs like ours, with values in the challenge field, arise in a proof system configured beyond Johnson? A prover must also satisfy the protocol's constraints on the received words and its other verification checks, and such constraints can restore a bound, as they do for words with values in a subfield containing the domain (Section 7).

Formal verification in Lean

All of our results are formally verified in Lean, building on the mathematical library ArkLib [3]. This covers every theorem, proposition, corollary, and lemma of this paper, the remarks and numerical bounds derived from them, and the finite arithmetic underlying our concrete bounds for the systems of Section 7. The formal statements include the degree and agreement bounds, guarantees for the individual inputs, and distinct-challenge counts of each result. The formalization and its annotated main-theorem statements are publicly available [21]. Its README maps each statement of this paper to the Lean declarations that prove it. Descriptions of deployed systems and results quoted from the literature for comparison are outside the formalization.

AI methodology

GPT-5.6 Sol, GPT-6 Sol, GPT-6.1 Sol, GPT-6 Astra, Claude Fable 5.1, and Claude Opus 5.5 discovered and refined the main results, including the counterexample constructions and their concrete specializations, with our close prompting and guidance. These models also carried out the Lean formalization [21] and assisted with the writing under our direction. They materially affected the results, proofs, and exposition of every section. We verified the correctness and originality of all content, including the references, and take full responsibility for the results, proofs, and exposition.

A Deferred proofs

This appendix proves Corollary 5.16 and the results of Section 5.9, which the rest of the paper does not use.

A.1 Proof of Corollary 5.16

Proof of Corollary 5.16. Choose D_0, N_0, T_0, and the polynomials $R + C_i$ $(1 \le i \le L)$ with root sets $S_i \subseteq D_0$ as in the first paragraph of the proof of Corollary 5.17; in particular $\log_2 L = \Theta_{c,r}((\log N)^2)$.

Put $K_0 = N - 3N_0/4$ and $w = K - K_0$. The hypothesis on ρ gives $0 \le w < N_0/2$. If $w = 0$, put $B = \emptyset$. Otherwise apply Lemma 3.18 inside D_0 to the sets $S_1, \dots, S_L$. It gives a set $B \subseteq D_0$ of size w with

$$|B \cup S_i| \ge T_1, \qquad T_1 = \left\lceil w + \left(1 - \frac{w}{N_0}\right) T_0 - \sqrt{(w/2)\ln(2L)} \right\rceil = \frac{N_0 + w}{2} - o(N),$$

for every i, because $\ln L = O((\log N)^2)$. If $w = 0$, the same holds with $T_1 = T_0$. Put

$$\Pi = L_{D \setminus D_0} L_B, \qquad \deg \Pi = N - N_0 + w = K - N_0/4.$$

Each polynomial $\Pi(R + C_i) = \Pi R + \Pi C_i$ vanishes on $(D \setminus D_0) \cup B \cup S_i$, a set of size at least

$$T = N - N_0 + T_1 = N - N_0 + \frac{N_0 + w}{2} - o(N) = \frac{N + K}{2} - \frac{N_0}{8} - o(N),$$

which is the stated agreement because $K = \rho N + O(1)$ and $N_0 = 2^{-r}N$. The polynomials ΠC_i are distinct, have coefficients in $\mathbb{B}$, and have degree less than K. The word $(\Pi R)|_D$ agrees with each of them on at least T points. This proves the first part.

For the second part, the paragraph "Distinct challenges" of the proof of Corollary 5.17 applies to this Π, whose roots also lie in D. That argument gives an extension $\mathbb{F}$ of $\mathbb{B}$ of size $N^{O_{c,r}(\log N)}$ and a pole $\beta \notin \mathbb{B}$ for which $f(x) = \Pi(x)R(x)/(x-\beta)$ and $g(x) = 1/(x-\beta)$ satisfy $\mathrm{agr}_K(g) = \mathrm{CA}_K(f,g) = K$, with at least $3L/4 - 1$ distinct nonzero challenges in $\mathrm{Bad}_T(f,g)$.

For the final claims, the gap is positive exactly when $\rho < 1 - 2^{-r-2}$. Also $(1+\rho)/2 - \sqrt{\rho} = (1-\sqrt{\rho})^2/2$. Since $\rho \geq 5/8$ gives $(1+\sqrt{\rho})^2 > 3$, and $1 - \rho \leq 3 \cdot 2^{-r-2}$,

$$\frac{(1-\sqrt{\rho})^2}{2} = \frac{(1-\rho)^2}{2(1+\sqrt{\rho})^2} < \frac{3 \cdot 2^{-2r-4}}{2} \leq 2^{-r-3},$$

so the limiting agreement is below $\sqrt{\rho}$. The window for r is $[1 - 3 \cdot 2^{-r-2}, 1 - 2^{-r-2})$; consecutive windows overlap, and the first begins at $5/8$. □

A.2 Proofs for Section 5.9

Proof of Proposition 5.21. For the first part, the family is closed under addition, so the inner distribution that Schmidt computes for it in [44, Theorems 5.6 and 4.9] is the distribution of the ranks and types of its members. In [44, Theorem 4.9], take $q = b$, $m = 2n$, $\delta = s = t$, and $\tau = -1$. Only the term $j = 0$ remains, and the number of members of rank $2t$ and elliptic type is

$$\tfrac{1}{2}(b^t - 1)\begin{bmatrix} n \\ t \end{bmatrix}_{b^2} \big(1 - (-1)\big) = (b^t - 1)\begin{bmatrix} n \\ t \end{bmatrix}_{b^2}.$$

For the second part, let z_j be the number of zeros of an elliptic form with zero radical on a space of dimension $2j$. A plane on which the form vanishes only at zero has $z_1 = 1$. Adding a hyperbolic plane xy, which has $2b - 1$ zeros and takes each nonzero value $b - 1$ times, gives

$$z_j = (2b-1)z_{j-1} + (b-1)\big(b^{2j-2} - z_{j-1}\big) = bz_{j-1} + (b-1)b^{2j-2},$$

so $z_t = b^{2t-1} - (b-1)b^{t-1}$. Multiplying by the size N/b^{2t} of the radical gives the stated count. For the third, expand the traces and reduce exponents using $x^{b^m} = x$:

$$\mathrm{Tr}_m(a_i x^{b^i+1}) = \sum_{k=0}^{m-1} a_i^{b^k} x^{b^{k+i}+b^k}, \qquad \mathrm{Tr}_n(a_n x^{b^n+1}) = \sum_{k=0}^{n-1} a_n^{b^k} x^{b^{k+n}+b^k},$$

with the index $k + i$ read modulo m. The two indices in each monomial differ by i or $m - i$, both between t and $m - t$, and every exponent is less than b^m. A monomial $X^{b^j+b^k}$ with $j < k$ has nonzero derivative only when $j = 0$, where the derivative is X^{b^k}. In the first sum, one of the two exponents is b^0 exactly for the summation indices 0 and $m - i$, and in the second sum only for the summation index 0. These terms give the displayed formula.

For the fourth part, the family is closed under subtraction, so it suffices to show that a member ψ with zero polar form is zero. Let Q be its canonical representative. For each $y \in \mathbb{B}$, the polynomial $Q(X+y) - Q(X) - Q(y)$ has degree less than $|\mathbb{B}|$ and takes the values $B_\psi(x,y) = 0$ on $\mathbb{B}$, so it is the zero polynomial. Differentiating in X gives $Q'(X+y) = Q'(X)$. Since Q' is additive, $Q'(y) = 0$ for every $y \in \mathbb{B}$, and $\deg Q' < |\mathbb{B}|$ forces $Q' = 0$. The distinct powers of X in the formula for Q' then give $a_i = 0$ for every i. The last part holds because a_i is replaced by $a_i \xi^{b^i+1}$, with $\xi^{b^n+1} \in \mathbb{F}_{b^n}$, and a linear change of variable preserves rank and type. □

Proof of Theorem 5.22. Steps 1 to 4 below correspond to Lemmas 5.6, 5.8, 5.9, and 5.10, and Steps 5 to 7 to the three parts of the proof of Lemma 5.12. The differences are these: the trace family replaces the moment equations and their count; translates of a form replace the added linear functions, and elliptic type replaces the signed-sum count; G has multiple roots, so the conversion to P is direct; and distinctness holds only up to factors in $\mathbb{F}_b^*$.

The forms. We show that D carries at least $(b^t-1)\begin{bmatrix} n-h \\ t \end{bmatrix}_{b^2}$ quadratic forms of rank $2t$ and elliptic type, each induced by a form of Proposition 5.21. For $D = \mathbb{B}$ this is the first part of that proposition. Otherwise $D = \{x : \mathrm{Tr}_m(x/v) = 0\}$ for some $v \in \mathbb{B}^*$, and the $\mathbb{F}_b$-linear map $s_v(X) = X - v^{1-b}X^b$ has kernel $\mathbb{F}_b v$ and image D, since $s_v(vy) = v(y - y^b)$ and $\mathrm{Tr}_m(y - y^b) = 0$. By the last part of Proposition 5.21, dilations permute the forms of rank $2t$ and elliptic type and act transitively on nonzero vectors, so every nonzero vector lies in the radicals of equally many of them. Counting pairs of such a form and a nonzero vector of its radical, at least

$$(b^t-1)\begin{bmatrix} n \\ t \end{bmatrix}_{b^2} \cdot \frac{b^{m-2t}-1}{b^m-1} = (b^t-1)\begin{bmatrix} n-1 \\ t \end{bmatrix}_{b^2}$$

of them have v in their radical (Section 3.1). Such a form is constant on the cosets of $\mathbb{F}_b v$, so it equals $\psi_D \circ s_v$ for a form ψ_D on D of the same rank and type, and different forms give different ψ_D. Let $Q_{\mathbb{B}}$ be the canonical polynomial of the trace form, and let Q_D be the polynomial of degree less than N representing ψ_D. Then $Q_{\mathbb{B}}$ and $Q_D \circ s_v$ have degree less than $bN = |\mathbb{B}|$ and agree on $\mathbb{B}$, so

$$Q_{\mathbb{B}} = Q_D \circ s_v \tag{A.1}$$

as polynomials. From now on ψ denotes a selected form on D, Q denotes its polynomial of degree less than N, and V denotes its radical, of size N/b^{2t}. Since ψ has elliptic type, V is also its polar radical.

Step 1: the identity for Q. Write $L_D = \sum_{i=0}^{d} \lambda_i X^{b^i}$, with $\lambda_d = 1$, and put $\lambda = \lambda_0$. First, $\deg Q \le N/b + N/b^{t+1}$: for $D = \mathbb{B}$, the monomials $X^{b^j+b^k}$ of the third part of Proposition 5.21 have degree at most $b^{m-1} + b^{m-1-t}$, and for a hyperplane (A.1) gives $\deg Q = \deg Q_{\mathbb{B}}/b$. The polynomial $Q^b - Q$ vanishes on D because ψ has values in $\mathbb{F}_b$, so $Q^b - Q = L_D Y$ with $\deg Y \le b \deg Q - N \le N/b^t$. Differentiating gives $-Q' = \lambda Y + L_D Y'$, which forces $Y' = 0$, so

$$Q^b - Q = -\frac{L_D}{\lambda} Q'. \tag{A.2}$$

Step 2: the window of Q'. We claim that $Q' = \sum_{i=t}^{d-t} g_i X^{b^i}$. For $D = \mathbb{B}$ this is the third part of Proposition 5.21. For a hyperplane, $s_v' = 1$ gives $Q'_{\mathbb{B}} = Q' \circ s_v$. If Q' has degree $e \ge 1$, the composition has degree be, so e is a power of b. Since every power $s_v^{b^i}$ contains only powers X^{b^j}, removing the leading term of Q' and inducting on the degree shows that Q' contains only powers X^{b^i}; a constant term would remain in the composition, so there is none. In

$$Q' \circ s_v = \sum_i y_i \left(X^{b^i} - v^{(1-b)b^i} X^{b^{i+1}}\right),$$

the lowest and highest indices with $y_i \neq 0$ produce the powers X^{b^i} and $X^{b^{i+1}}$. As $Q'_{\mathbb{B}}$ contains only X^{b^i} with $t \le i \le m-t$, the indices of Q' lie between t and $m-t-1 = d-t$.

Step 3: the roots of Q' are the radical. For $y \in D$, the polynomial $B_Q(X, y) = Q(X + y) - Q(X) - Q(y)$ has degree less than N and represents $B_\psi(\cdot, y)$ on D. Since $L_D(X + y) = L_D(X)$, $Q(y)^b = Q(y)$, and Q' is additive by Step 2, applying (A.2) at $X + y$ and at X gives

$$B_Q(X, y)^b - B_Q(X, y) = -\frac{L_D(X)}{\lambda} Q'(y).$$

If $Q'(y) = 0$, then $B_Q(X, y)$ is a constant vanishing at $X = 0$, hence zero. If $Q'(y) \neq 0$, it is a nonzero polynomial of degree less than N, so it does not vanish on all of D. Thus $V = \{y \in D : Q'(y) = 0\}$, and $Q' \neq 0$ because $V \neq D$. By Step 2, Q' is the b^t-th power of a linearized polynomial of degree at most N/b^{2t} that vanishes on V, so $Q' = \mathrm{lc}(Q')L_V^{b^t}$.

Step 4: translates. For $u \in D$ put

$$\psi_u(x) = \psi(x - u) = \psi(x) - B_\psi(x, u) + \psi(u),$$

represented by the polynomial $G = Q(X - u)$. The linear function $B_\psi(\cdot, u)$ depends exactly on the class of u modulo V, so each form gives b^{2t} distinct functions ψ_u. Different forms give different functions, because $B_{\psi_u} = B_\psi$ and the polar form determines the form within the family (the fourth part of Proposition 5.21 and (A.1)). Altogether there are at least $b^{2t}(b^t - 1)\begin{bmatrix} n-h \\ t \end{bmatrix}_{b^2} = (b-1)L$ functions ψ_u. Each has exactly T zeros on D by the second part of Proposition 5.21, and it vanishes on $u + V$, because ψ vanishes on its radical. Since $L_D(X-u) = L_D(X)$, the identity (A.2) also holds for G, and by Step 3, $G' = Q'(X-u) = \mathrm{lc}(Q')L_V(X-u)^{b^t}$. The roots of G' are the points of $u + V$, each with multiplicity b^t.

Step 5: the polynomial $P = G/F$. Since G' is a b^t-th power, there is a polynomial F, a constant multiple of $L_V(X - u)^{b^{t-1}}$, with $G' = -\lambda F^b$. Then $G^b - G = L_D F^b$, the roots of F are the points of $u + V$, each with multiplicity b^{t-1}, and $\deg F = N/b^{t+1}$. At a point of $u + V$, the right side vanishes to order $b^t + 1$ and G^b to higher order than G, so G has multiplicity exactly $b^t + 1$ there. Every other root of G is simple, since G' does not vanish there, and lies in D, since it is a root of $L_D F^b$. Thus the roots of G are the T zeros of ψ_u on D, and

$$P = \frac{G}{F}$$

is a polynomial with the same T roots. Counting multiplicities gives $\deg G = T + N/b^t$, so $\deg P = N/b$, and comparing leading coefficients in $G^b - G = L_D F^b$ shows that P is monic. Dividing by F^b gives

$$P^b = L_D + \frac{G}{F^b}, \qquad F^{b-1}(P^b - L_D) = P, \tag{A.3}$$

where G/F^b is a polynomial of degree T whose roots are the zeros of ψ_u. With $R = (L_D - \lambda X)^{1/b} = \sum_{i=1}^{d} \lambda_i^{1/b} X^{b^{i-1}}$ and $C = P - R$, we get $C^b = \lambda X + G/F^b$, so $\deg C = T/b < K$.

Step 6: distinctness. The second identity in (A.3) determines F^{b-1}, hence F up to a factor in $\mathbb{F}_b^*$, and then $G = PF$ up to the same factor. So at least L of the polynomials P are distinct.

Step 7: collisions outside D. Let $P_1 \neq P_2$, with $P_i = G_i/F_i$, agree at some $\beta \notin D$. The common value and $P_i(\beta)^b - L_D(\beta)$ are nonzero, because all roots of P_i and G_i/F_i^b lie in D, so (A.3) gives $F_1(\beta) = \zeta F_2(\beta)$ for some $\zeta \in \mathbb{F}_b^*$. Since $\zeta^{b^{t-1}} = \zeta$, the polynomial $F_1 - \zeta F_2$ is the b^{t-1}-th power of a polynomial of degree at most N/b^{2t}, and it is nonzero. Indeed, if $F_1 = \zeta F_2$, then $F_1^{b-1} = F_2^{b-1}$, and subtracting the second identity in (A.3) for P_2 from that for P_1 gives $F_1^{b-1}(P_1 - P_2)^b = P_1 - P_2$. The left side has larger degree than the right unless $P_1 = P_2$. Hence two distinct polynomials agree at at most $\delta = (b-1)N/b^{2t}$ points outside D.

The received words. The proof of Theorem 5.1 now applies with message length K. The word $R|_D$ agrees with the codeword $-C_i|_D$ on the T roots of $P_i = R + C_i$, which gives the decoding list. Lemmas 3.11 and 3.19 give the pair and the stated number of distinct challenges. Replacing the first input by the one of Lemma 3.13 translates the challenges and gives $\operatorname{agr}_K(f) \le (b+1)N/(2b^2) - 1$. For $t \ge 2$,

$$T - \left(\frac{(b+1)N}{2b^2} - 1\right) \ge \frac{(b-1)(b-2)N}{2b^3} + 1 > 0,$$

so zero is not exceptional and all the selected challenges are nonzero. □

Proof of Corollary 5.23. Apply Theorem 5.22 with $D = \mathbb{F}_N$ and $t = \lfloor n/2 \rfloor$. Since $L_D = X^N - X$, the received word in its proof is $R = X^{N/b}$.

The Gaussian product formula gives

$$\log_b \begin{bmatrix} n \\ t \end{bmatrix}_{b^2} = 2t(n-t) + O_b(1).$$

Consequently the list-size lower bound in the theorem satisfies

$$\log_b L = 2t(n-t) + 3t + O_b(1) = \frac{n^2}{2} + O_b(n).$$

As $\log_b N = 2n$, this is $L = N^{\Omega_b(\log N)}$. The agreement formula follows from $T/N = b^{-1} - (b-1)b^{-t-1}$ and $t = n/2 + O(1)$. □

Proof of Corollary 5.24. We restrict the full-field agreement sets of Theorem 5.22 to D and then use the unused degree to add points to each of them.

Restriction. Apply Theorem 5.22 on $\mathbb{B}$ with $t = \lfloor n/2 \rfloor$ and message length $K_0 = |\mathbb{B}|/b^2$. As in Corollary 5.23, it gives $L = N^{\Omega_b(\log N)}$ polynomials $R + C_i$ with distinct C_i of degree less than K_0, and by Step 5 of the proof of Theorem 5.22 the roots of $R + C_i$ in $\mathbb{B}$ are the zeros of a translate ψ_u of a quadratic form of rank $2t$. For $v \in \mathbb{F}_b^*$, the binary quadratic function $\operatorname{Tr}_{\mathbb{F}_b/\mathbb{F}_2}(v\psi_u)$ has polar rank $2t \log_2 b$ on $\mathbb{B}$: replacing the second argument of the polar form by its $\mathbb{F}_b$-multiples shows that its binary polar radical is the polar radical over $\mathbb{F}_b$. After a translation, D is a subspace of codimension c, and restricting to it deletes c rows and columns of the polar matrix, so the polar radical of the restriction has at most $2^{2c}N/b^{2t}$ points. For a quadratic Boolean function χ on a binary space of size N, the computation of σ^2 in the proof of Lemma 5.10 gives $\left(\sum_x (-1)^{\chi(x)}\right)^2 = N \sum_{y \in \operatorname{rad}(B_\chi)} (-1)^{\chi(y)+\chi(0)} \le N|\operatorname{rad}(B_\chi)|$. Since $\mathbf{1}_{y=0} = b^{-1} \sum_{v \in \mathbb{F}_b} (-1)^{\operatorname{Tr}_{\mathbb{F}_b/\mathbb{F}_2}(vy)}$,

$$|\{x \in D : \psi_u(x) = 0\}| = \frac{N}{b} + \frac{1}{b} \sum_{v \in \mathbb{F}_b^*} \sum_{x \in D} (-1)^{\operatorname{Tr}_{\mathbb{F}_b/\mathbb{F}_2}(v\psi_u(x))} \ge \frac{N}{b} - \frac{b-1}{b} \cdot \frac{2^c N}{b^t} = \frac{N}{b} - O_{b,c}(N^{3/4}),$$

because $b^t \ge b^{(n-1)/2}$ and $N \le b^{2n}$. Let T_0 be the integer part of this bound, and for each i choose a set $S_i \subseteq D$ of exactly T_0 roots of $R + C_i$. The C_i remain distinct on D, since their degrees are below $K_0 < N$.

Padding. Put $w = K - K_0$, which is positive for large N because $\rho > 2^c/b^2$. Lemma 3.18 gives a set $B \subseteq D$ of size w with

$$|B \cup S_i| \ge T_0 + w\left(1 - \frac{T_0}{N}\right) - O(\sqrt{N \log L}) = \alpha_{b,c}(\rho)N - O_{b,c}(N^{3/4})$$

for every i. The word $(L_B R)|_D$ agrees with each of the distinct codewords $-(L_B C_i)|_D$, of degree less than K, on $B \cup S_i$. This proves the claim for received words.

Received pairs. The polynomials $L_B(R + C_i) = L_B R + L_B C_i$ have distinct corrections $L_B C_i$ of degree less than K, and each vanishes on $B \cup S_i$. Take an extension $\mathbb{F}_0 \supseteq \mathbb{B}$ with $|\mathbb{F}_0| > N + K\binom{L}{2}$; extension degree $O_{b,c}(\log N)$ suffices. Each nonzero polynomial $L_B(C_i - C_j)$ has fewer than K roots, so some $\beta \in \mathbb{F}_0 \setminus D$ is a root of none of them. Lemma 3.11 at this pole gives the pair $f(x) = L_B(x)R(x)/(x - \beta)$, $g(x) = 1/(x - \beta)$ with $\mathrm{agr}_K(g) = \mathrm{CA}_K(f, g) = K$, and the L challenges $(L_B C_i)(\beta)$ are distinct. At most one of them is zero, and each has the agreement bound above. Finally, Lemma 3.12 in a quadratic extension of $\mathbb{F}_0$ makes both individual agreements and the common agreement exactly K, keeps the challenges distinct and nonzero, and keeps the field size $N^{O_{b,c}(\log N)}$.

The inequalities. First, $\alpha_{b,c}(\rho) - \rho = (1 - 2^c/b + 2^c/b^2 - \rho)/b > 0$. Second, $\alpha_{b,c}(\rho) \le \alpha_{b,0}(\rho) < \sqrt{\rho}$, since for $\sqrt{\rho} > 1/b$

$$\alpha_{b,0}(\rho) - \sqrt{\rho} = \left(1 - \frac{1}{b}\right)\left(\sqrt{\rho} - \frac{1}{b}\right)\left(\sqrt{\rho} - 1 - \frac{1}{b(b-1)}\right) < 0.$$

□

References

[1] O. Alrabiah, R. Goyal, and V. Guruswami. *Explicit Reed–Solomon Subspace Designs: Optimal List and Line Decoding*. ECCC TR26-262, 2026; arXiv:2610.36215. https://eccc.weizmann.ac.il/report/2026/262/.

[2] O. Alrabiah, Z. Guo, V. Guruswami, R. Li, and Z. Zhang. *Random Reed–Solomon Codes Achieve List-Decoding Capacity with Linear-Sized Alphabets*. arXiv:2304.09445. https://arxiv.org/abs/2304.09445.

[3] ArkLib contributors. *ArkLib: Formally Verified Arguments of Knowledge*. Lean library, revision `fa14552`. https://github.com/Verified-zkEVM/ArkLib.

[4] G. Arnon, A. Chiesa, G. Fenzi, and E. Yogev. *WHIR: Reed–Solomon Proximity Testing with Super-Fast Verification*. Cryptology ePrint Archive, Report 2024/1586, 2024. https://eprint.iacr.org/2024/1586.

[5] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev. *Scalable, transparent, and post-quantum secure computational integrity*. Cryptology ePrint Archive, Paper 2018/046, 2018. https://eprint.iacr.org/2018/046.

[6] E. Ben-Sasson, D. Carmon, U. Haböck, S. Kopparty, and S. Saraf. *On Proximity Gaps for Reed–Solomon Codes*. ECCC TR25-169, 2025. https://eccc.weizmann.ac.il/report/2025/169/.

[7] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf. *Proximity Gaps for Reed–Solomon Codes*. Journal of the ACM 70(5) (2023), Article 31. https://doi.org/10.1145/3614423.

[8] E. Ben-Sasson, L. Goldberg, S. Kopparty, and S. Saraf. *DEEP-FRI: Sampling Outside the Box Improves Soundness*. ITCS 2020. arXiv:1903.12243.

[9] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan. *Subspace Polynomials and List Decoding of Reed–Solomon Codes*. FOCS 2006. https://sites.math.rutgers.edu/~sk1233/rsld.pdf.

[10] E. R. Berlekamp. *The weight enumerators for certain subcodes of the second order binary Reed–Muller codes*. Information and Control 17 (1970), 485–500. https://doi.org/10.1016/S0019-9958(70)90399-2.

[11] A. Berman, Y. Shany, and I. Tamo. *Efficient Algorithms for Constructing Minimum-Weight Codewords in Some Extended Binary BCH Codes*. arXiv:2305.17764, 2023. https://arxiv.org/abs/2305.17764.

[12] Binius team. *Binius64: Overview*. Technical documentation. https://www.binius.xyz/blueprint/overview/.

[13] Binius64 source, commit `6e75a2d1d2e716578ae3ccb62806413fb1615176`, September 3, 2026. Field and verifier configuration, Gao–Mateer domain generation, and Reed–Solomon encoding: verifier configuration, FRI soundness parameters, GHASH field, domain generation, Reed–Solomon encoding.

[14] H. Borges and R. Conceição. *On the characterization of minimal value set polynomials*. arXiv:1108.1852, 2011. https://arxiv.org/abs/1108.1852.

[15] J. Brakensiek, Y. Chen, A. Putterman, Z. Zhang, and K. Z. Zheng. *Algorithmic List Decoding of Reed–Solomon Codes up to Capacity*. ECCC TR26-164, revision 1, 2026. https://eccc.weizmann.ac.il/report/2026/164/.

[16] J. Brakensiek, S. Gopi, and V. Makam. *Generic Reed–Solomon Codes Achieve List-Decoding Capacity*. STOC 2023. arXiv:2206.05256. https://arxiv.org/abs/2206.05256.

[17] B. Bünz, R. Rothblum, and W. Wang. *Flock: Fast Proving for Batch Boolean Computations*. Cryptology ePrint Archive, Paper 2026/1329, version dated September 19, 2026. https://eprint.iacr.org/2026/1329.

[18] A. Chatterjee, S. Ghosh, Z. Guo, R. Gurjar, R. Raj, and Z. Zhang. *Deterministic Constructions of Reed–Solomon Codes Beyond the Johnson Bound*. arXiv:2610.31922, 2026. https://arxiv.org/abs/2610.31922.

[19] E. Crites and A. Stewart. *On Reed–Solomon Proximity Gaps Conjectures*. Cryptology ePrint Archive, Report 2025/2046, 2025. https://eprint.iacr.org/2025/2046.

[20] Q. Dao, S. D. Kominers, and J. Thaler. *Reed–Solomon Codes Beyond Johnson: Efficient Decoding and Smaller Cryptographic Proofs*. Cryptology ePrint Archive, Paper 2026/2056, 2026. https://eprint.iacr.org/2026/2056.

[21] Q. Dao, S. D. Kominers, J. Thaler, and K. Z. Zheng. *Counterexamples to Beyond-Johnson Proximity Gaps over Binary Fields: Lean formalization*. Source code and annotated main-theorem statements, 2026. https://github.com/GUJustin/binary_field_gap_counterexamples.

[22] P. Delsarte and J.-M. Goethals. *Alternating bilinear forms over GF(q)*. Journal of Combinatorial Theory, Series A 19 (1975), 26–50. https://doi.org/10.1016/0097-3165(75)90090-4.

[23] B. E. Diamond and A. Gruen. *On the Distribution of the Distances of Random Words*. Cryptology ePrint Archive, Paper 2025/2010, 2025, revised August 2026. https://eprint.iacr.org/2025/2010.

[24] B. E. Diamond and J. Posen. *Polylogarithmic Proofs for Multilinears over Binary Towers*. Cryptology ePrint Archive, Paper 2024/504, 2024, revised May 2026. https://eprint.iacr.org/2024/504.

[25] Flock contributors. *Flock: Ligerito polynomial commitment implementation*. Source at commit b684b1258e4b, accessed September 17, 2026.

[26] A. Gabizon. *Linear list size bounds for Reed–Solomon beyond the Johnson radius*. Cryptology ePrint Archive, Paper 2026/2048, 2026. https://eprint.iacr.org/2026/2048.

[27] Y. Gao, H. Yang, Y. Xu, and H. Kan. *List-Decoding Counterexamples Yield Lower Bounds on Mutual Correlated Agreement Error*. arXiv:2607.10572, 2026. https://arxiv.org/abs/2607.10572.

[28] Google Longfellow contributors. *Longfellow ZK implementation*. Source at commit d5e6be773369, accessed October 6, 2026: MDOC configurations, code layout, verification, and security analysis (Theorem 4.3).

[29] M. Frigo and a. shelat. *Longfellow ZK*. Internet-Draft draft-google-cfrg-libzk-03, September 23, 2026, Sections 2.2.2 and 5.1. IETF Datatracker.

[30] R. Gold. *Maximal recursive sequences with 3-valued recursive cross-correlation functions*. IEEE Transactions on Information Theory 14 (1968), 154–156. https://doi.org/10.1109/TIT.1968.1054106.

[31] R. Goyal and V. Guruswami. *Optimal Proximity Gaps for Subspace-Design Codes and (Random) Reed–Solomon Codes*. ECCC TR25-166, revision 1, 2026. https://eccc.weizmann.ac.il/report/2025/166/.

[32] R. Goyal, V. Guruswami, Y. Sun, and M. Wootters. *Improved LCL Equivalences and Curve Decoding Alphabet Sizes*. arXiv:2610.38862, 2026. https://arxiv.org/abs/2610.38862.

[33] Z. Guo and Z. Zhang. *Randomly Punctured Reed–Solomon Codes Achieve the List Decoding Capacity over Polynomial-Size Alphabets*. FOCS 2023. arXiv:2304.01403v2. https://arxiv.org/abs/2304.01403v2.

[34] V. Guruswami and A. Rudra. *Limits to List Decoding Reed–Solomon Codes*. STOC 2005. https://www.cs.cmu.edu/~venkatg/pubs/papers/rs-limits.pdf.

[35] F. G. Jeronimo. *Algorithmic List Decoding at Capacity and Optimal Proximity Gaps for Reed–Solomon Codes*. ECCC TR26-169, 2026. https://eccc.weizmann.ac.il/report/2026/169/.

[36] S. Jo. *Reed–Solomon Mutual Correlated Agreement Beyond the Johnson Radius*. Cryptology ePrint Archive, Report 2026/1432, 2026. https://eprint.iacr.org/2026/1432.

[37] J. Justesen and T. Høholdt. *Bounds on list decoding of MDS codes*. IEEE Transactions on Information Theory 47 (2001), 1604–1609. https://doi.org/10.1109/18.923744.

[38] A. Kambiré. *Proximity Gaps Conjecture Fails Near Capacity over Prime Fields*. arXiv:2604.09724, 2026. https://arxiv.org/abs/2604.09724.

[39] T. Kasami and S. Lin. *Some results on the minimum weight of primitive BCH codes*. IEEE Transactions on Information Theory 18 (1972), 824–825. https://doi.org/10.1109/TIT.1972.1054903.

[40] S. D. Kominers, J. Thaler, and K. Z. Zheng. *The One-and-a-Half Johnson Bound Is Tight for Proximity Gaps of General Linear Codes*. Cryptology ePrint Archive, Paper 2026/1894, 2026; ECCC TR26-235. https://eprint.iacr.org/2026/1894.

[41] D. Krachun, S. Kazanin, and U. Haböck. *Failure of proximity gaps close to capacity*. Cryptology ePrint Archive, Report 2026/782, 2026. https://eprint.iacr.org/2026/782.

[42] leanEthereum contributors. *LeanVM*. Source repository, commit 022ec377a39d, accessed September 17, 2026.

[43] rs-ld-mca project. *Mutual Correlated Agreement for Reed–Solomon Codes up to Capacity in the Low-Rate Regime*. AI-generated manuscript, September 2026. GitHub repository, commit 9699ee7a6143, accessed October 3, 2026.

[44] K.-U. Schmidt. *Quadratic and symmetric bilinear forms over finite fields and their association schemes*. Algebraic Combinatorics 3 (2020), 161–189. https://doi.org/10.5802/alco.88.

[45] S. Setty. *BinarySpartan: Spartan over binary fields*. Cryptology ePrint Archive, Paper 2026/1656, September 3, 2026 revision. Archived version.

[46] M. Zhu. *Superpolynomial Lists for Reed–Solomon Codes over Binary Extension Fields*. arXiv:2610.15815, 2026. https://arxiv.org/abs/2610.15815.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il