

One More A: Sharper Tails Without Scaling

Majid Khabbazzian

University of Alberta, Canada

Abstract

Repeat-accumulate-accumulate (RAA) codes have minimum distance linear in the block length with probability tending to one, both with and without random coordinate scaling. Sharp results, however, reveal a tradeoff between the two constructions. For block length $N = rn$ and fixed repetition factor $r \geq 4$, the probability that the minimum distance is at most δN is $\Theta(N^{2-r})$ for unscaled RAA and $\Theta(N^{1-r})$ for scaled RAA, on their common proved range $0 < \delta \leq 1/10$. Thus scaling reduces the failure probability by a factor of order N . This improvement comes at a cost: the scaled result requires $q = \Omega(N)$ over $\mathbb{F}_q$, and the encoder uses two length- N layers of coordinatewise field multiplications. In contrast, unscaled RAA works over a fixed field of characteristic greater than r , and its accumulator stages use only field additions.

In this work, we show that adding a third accumulator provides a substantially larger reliability gain without random scaling. For the unscaled repeat-accumulate-accumulate-accumulate ensemble

$$G_3 = R\Pi_1 A\Pi_2 A\Pi_3 A,$$

where R is r -fold repetition, A is the accumulator, and the Π_i are independent uniform interleavers, we prove that

$$\mathbb{P}[d_{\min}(G_3) \leq \delta N] = \Theta_{r,\delta}\left(N^{2-r-\lceil r/2 \rceil}\right)$$

for every fixed $r \geq 4$ and $0 < \delta \leq 1/10$, uniformly over all finite fields of characteristic greater than r . Hence the field size need not grow with N , and the encoder requires three accumulator passes but no coordinatewise field multiplications. On the common threshold range, its failure probability is smaller by a factor of order $N^{\lceil r/2 \rceil}$ than that of unscaled RAA and by a factor of order $N^{\lceil r/2 \rceil - 1}$ than that of scaled RAA. For example, when $r = 4$, the respective failure probabilities have orders N^{-2} , N^{-3} , and N^{-4} .

1 Introduction

Repeat-accumulate codes and their multiple-accumulator extensions combine simple encoding operations with strong minimum-distance guarantees. They are built from repetition, random coordinate permutations, called interleavers, and accumulators, which replace a word by its sequence of prefix sums [2]. With a fixed number of stages, encoding requires only linearly many field operations. In the classical binary setting, fixed-repeat RA ensembles have sublinear minimum distance, whereas RAA and further-accumulator ensembles can have minimum distance linear in the block length with probability tending to one, for suitable repetition factors [1, 4].

Once linear minimum distance is known to hold with high probability, a finer question is how rapidly the exceptional probability decays. For a full-row-rank generator G , write

$$d_{\min}(G) := \min_{\mathbf{x} \neq 0} \text{wt}(\mathbf{x}G),$$

where wt counts the nonzero coordinates. For block length N and a fixed relative-distance threshold $\delta > 0$, we study

$$\mathbb{P}[d_{\min}(G) \leq \delta N].$$

This lower tail measures the probability that a randomly sampled code fails to meet the prescribed distance requirement. Its asymptotic order can distinguish ensembles that all have linear minimum distance but produce bad codes with substantially different probabilities.

1.1 The RAA tradeoff: reliability and encoder arithmetic

Let n be the message length, let $r \geq 4$ be a fixed repetition factor, and put $N = rn$. Work over a finite field $\mathbb{F}_q$, with characteristic p . Write R for r -fold repetition, A for the length- N accumulator, and Π_i for independent uniform permutation matrices. With messages viewed as row vectors, the unscaled repeat-accumulate-accumulate (RAA) ensemble has generator

$$G_2 := R\Pi_1 A\Pi_2 A. \quad (1.1)$$

Its randomly scaled counterpart inserts two independent diagonal matrices V_1, V_2 , whose diagonal entries are independent and uniform in $\mathbb{F}_q^\times$, independently of the interleavers:

$$G_{\text{sc}} := R\Pi_1 V_1 A\Pi_2 V_2 A. \quad (1.2)$$

Both constructions generate codes of rate $1/r$.

A prior sharp analysis establishes the following comparison [3]. For unscaled RAA, every fixed $0 < \delta \leq 1/10$ satisfies

$$\mathbb{P}[d_{\min}(G_2) \leq \delta N] = \Theta_{r,\delta}(N^{2-r}) \quad (1.3)$$

uniformly over fields with $p > r$. For scaled RAA,

$$\mathbb{P}[d_{\min}(G_{\text{sc}}) \leq \delta N] = \Theta_{r,\delta,\gamma}(N^{1-r}) \quad (1.4)$$

for every fixed $0 < \delta \leq 1/2$ and $\gamma > 0$, provided $q - 1 \geq \gamma N$.

Thus, on the common proved range $0 < \delta \leq 1/10$, random scaling reduces the failure probability by a factor of order N . This improvement comes with two costs: the sharp scaled law requires $q = \Omega(N)$, and encoding uses two length- N layers of coordinatewise field multiplications. Unscaled RAA, in contrast, permits a fixed field with $p > r$ and uses only additions in its accumulator stages. These RAA results serve as benchmarks; the RAA proof in this paper is self-contained.

This raises a natural design question:

Can one more accumulator improve the minimum-distance failure probability while preserving fixed-field operation and avoiding random scaling?

1.2 Main result: a third accumulator

We study the unscaled repeat-accumulate-accumulate-accumulate (RAAA) ensemble

$$G_3 := R\Pi_1 A\Pi_2 A\Pi_3 A. \quad (1.5)$$

This construction adds one independent interleaver and one accumulator to unscaled RAA, retains rate $1/r$, and introduces no coordinatewise field multiplications.

Table 1: Comparison for fixed $r \geq 4$ and $0 < \delta \leq 1/10$. Here $p = \text{char}(\mathbb{F}_q)$. Arithmetic counts exclude repetition, permutations, and memory movement.

Ensemble	Field condition	Additions	Multiplications	Sharp tail
Unscaled RAA	$p > r$	$2(N-1)$	0	$\Theta(N^{2-r})$
Scaled RAA	$q = \Omega(N)$	$2(N-1)$	$2N$	$\Theta(N^{1-r})$
Unscaled RAAA	$p > r$	$3(N-1)$	0	$\Theta(N^{2-r-\lceil r/2 \rceil})$

Theorem 1.1 (Sharp unscaled RAAA tail). *Fix $r \geq 4$ and $0 < \delta \leq 1/10$. There exist positive constants $c_{r,\delta}$, $C_{r,\delta}$, and $N_{r,\delta}$ such that, for every multiple $N \geq N_{r,\delta}$ of r and every finite field $\mathbb{F}_q$ of characteristic greater than r ,*

$$c_{r,\delta} N^{2-r-\lceil r/2 \rceil} \leq \mathbb{P}_{\Pi_1, \Pi_2, \Pi_3}[d_{\min}(G_3) \leq \delta N] \leq C_{r,\delta} N^{2-r-\lceil r/2 \rceil}. \quad (1.6)$$

All three constants are independent of the field.

The theorem gives a sharp probability of order $N^{2-r-\lceil r/2 \rceil}$, uniformly over the stated fields. In particular, the field size need not grow with N . Compared with unscaled RAA, the third accumulator reduces the failure probability by a factor of order $N^{\lceil r/2 \rceil}$. Compared with scaled RAA, the improvement is of order $N^{\lceil r/2 \rceil - 1}$. These comparisons concern $0 < \delta \leq 1/10$; a same-field comparison with scaled RAA additionally requires field sequences satisfying both sets of assumptions.

For example, when $r = 4$, the three failure probabilities have orders

$$\text{unscaled RAA} : N^{-2}, \quad \text{scaled RAA} : N^{-3}, \quad \text{unscaled RAAA} : N^{-4}.$$

Thus, the third accumulator provides a larger improvement in the failure exponent than random scaling, while retaining an unscaled encoder.

Table 1 summarizes the field and arithmetic requirements. Each accumulator uses $N-1$ field additions, and each scaling layer uses N field multiplications. Relative to scaled RAA, RAAA replaces two multiplication layers with one additional accumulator pass. This can be advantageous when field multiplication is costly, although actual running time also depends on the field representation, permutations, and memory movement.

1.3 Why one more accumulator helps

The improved exponent can be understood through a simple cancellation construction. Consider a message with value $+1$ at one coordinate, value -1 at another, and zeros elsewhere. After repetition, the first interleaver can arrange its $2r$ nonzero symbols into r adjacent opposite-value pairs. Within each pair, the accumulator becomes nonzero at the first position and returns to zero at the second. Its output therefore has only r nonzero coordinates, regardless of the distances between the pairs.

For a fixed message pair, this arrangement has probability of order N^{-r} . In unscaled RAA, the second interleaver can then place the remaining r nonzero coordinates in the final $\lfloor \delta N \rfloor$ positions with probability bounded away from zero. The last accumulator output is consequently supported in that terminal interval. There are $\Theta(N^2)$ choices of the message pair, explaining the unscaled RAA scale

$$N^2 \cdot N^{-r} = N^{2-r}.$$

Random scaling disrupts this automatic pairwise cancellation, leading to the smaller RAA failure probability.

For RAAA, we extend the construction by arranging a second collapse. Choose the orientations of the first-stage pairs so that the resulting r nonzero values can be paired with their opposites at the next stage. The second interleaver places these pairs adjacently; if r is odd, it also places the unmatched value at the final coordinate. This event costs a further factor of order $N^{-\lceil r/2 \rceil}$ and leaves only $\lceil r/2 \rceil$ nonzero coordinates after the second accumulator. The final interleaver places this bounded support in the terminal interval with constant probability. The resulting scale is

$$N^2 \cdot N^{-r} \cdot N^{-\lceil r/2 \rceil} = N^{2-r-\lceil r/2 \rceil}.$$

This construction supplies the matching lower bound once overlaps among different message-pair events are controlled. It illustrates the additional geometric cost imposed by the third accumulator. Proving that this cost determines the full minimum-distance tail requires ruling out every other message and cancellation pattern that could produce a more likely failure.

1.4 Proof overview

The upper bound follows the cancellation patterns and output weights through all three stages. A bound on the first two accumulators alone does not record the additional rare arrangement responsible for the improved exponent. Moreover, cancellations at different stages are linked by the same underlying message values. The analysis therefore combines probabilistic information about the interleavers with algebraic information about the cancellations.

The proof has four main components.

1. *Separating order from position.* A uniform interleaver independently determines the order of the active values and the set of their positions. The indices of the vanishing active prefix sums form a cancellation trace, determined by the order. The positions determine the lengths of the nonzero output intervals. This separation gives exact random-gap laws for the output weight associated with each trace.
2. *Counting cancellations through a shared rank bound.* Every cancellation is a homogeneous linear equation in the original message values. For a message supported on w coordinates, the equations satisfied by a nonzero message can have rank at most $w - 1$. All three stages share this restriction, even though later equations depend on earlier cancellations. Counting the resulting trace patterns allows us to consider all message values without a bound that grows with the field size.
3. *Separating the message-weight regimes.* Exact gap estimates control fixed message weights, and further uniform bounds handle growing sparse weights. For messages with weight proportional to N , we combine the three transitions in an entropy bound and prove a uniformly negative exponent. This makes their total contribution exponentially small. The entropy argument is fully analytic and requires no numerical optimization or computer-assisted certificate.
4. *Matching the upper bound.* The two successive pair collapses described above give explicit weight-two witnesses. Controlling the intersections of these events shows that their union has the claimed polynomial order. Under the stated characteristic assumption, the upper estimates also show that all other message weights contribute a smaller order.

Organization. Section 2 defines the ensemble and records two basic reductions. Section 3 develops the trace, gap, and rank tools and combines them into a master probability bound. The matching lower bound is proved in section 4. The sparse and linear-density upper bounds appear in sections 5

and 6, respectively. Section 7 assembles the main theorem and its consequences, including a weaker characteristic condition for even repetition factors. Section 8 concludes with further directions.

2 Model and Preliminaries

2.1 Notation and the code ensemble

All vectors are row vectors. For a positive integer M , write $[M] := \{1, \dots, M\}$, and let e_i denote the i th standard basis vector of the appropriate dimension. For a vector z , put

$$\text{supp}(z) := \{i : z_i \neq 0\}, \quad \text{wt}(z) := |\text{supp}(z)|.$$

A coordinate is *active* if its value is nonzero; its entry is an *active value*. Thus the active support is simply $\text{supp}(z)$.

For integers a, b , set $\binom{a}{b} = 0$ unless $0 \leq b \leq a$. All logarithms are natural. Asymptotics are taken as $N \rightarrow \infty$ with r fixed; subscripts on asymptotic notation specify the allowed dependence of implicit constants. Field-uniform bounds have constants and sufficiently-large- N thresholds independent of the field.

Let $q = p^\ell$, where p is prime and $\ell \geq 1$. Fix integers $r \geq 2$, $n \geq 1$, and put $N := rn$. The repetition matrix $R \in \mathbb{F}_q^{n \times N}$ maps

$$\mathbf{x} = (x_1, \dots, x_n) \mapsto \mathbf{x}R = (\underbrace{x_1, \dots, x_1}_r, \dots, \underbrace{x_n, \dots, x_n}_r).$$

The accumulator $A \in \mathbb{F}_q^{N \times N}$ is defined by

$$(zA)_j = \sum_{i=1}^j z_i, \quad j \in [N].$$

It is upper triangular with diagonal entries one, hence invertible.

Let Π_1, Π_2, Π_3 be independent uniform permutation matrices on $[N]$. Our convention is

$$e_i \Pi = e_{\pi(i)};$$

thus $\text{supp}(z\Pi) = \pi(\text{supp}(z))$. The *active order* is the order of the original active coordinate labels in the permuted word. Equal-valued entries remain distinct labelled occurrences.

The unscaled three-accumulator generator is

$$G_3 := R\Pi_1 A \Pi_2 A \Pi_3 A. \tag{2.1}$$

The rows of R have disjoint nonempty supports, and all subsequent matrices are invertible. Therefore G_3 has row rank n and generates an $[N, n]$ linear code of rate $1/r$.

For a full-row-rank generator $G \in \mathbb{F}_q^{n \times N}$, define

$$d_{\min}(G) := \min_{\mathbf{x} \in \mathbb{F}_q^n \setminus \{0\}} \text{wt}(\mathbf{x}G).$$

A field subscript, as in $d_{\min, \mathbb{F}_p}(G)$, specifies the field over which messages are chosen. For $0 < \delta \leq 1$, put $L_\delta := \lfloor \delta N \rfloor$, and define

$$\mathcal{E}_{3,w}(\delta) := \left\{ \exists \mathbf{x} \in \mathbb{F}_q^n : \text{wt}(\mathbf{x}) = w, \text{wt}(\mathbf{x}G_3) \leq L_\delta \right\}, \quad 1 \leq w \leq n.$$

A message satisfying these conditions is a *witness*. Probability is taken over the interleavers; messages are existentially quantified and may depend on their realization. The *terminal interval* of length L is $\{N - L + 1, \dots, N\}$, with the empty-set convention when $L = 0$.

For a nonzero message, write

$$y_0 := \mathbf{x}R, \quad y_i := y_{i-1}\Pi_i A \quad (i = 1, 2, 3),$$

and set

$$w := \text{wt}(\mathbf{x}), \quad m := rw, \quad h := \text{wt}(y_1), \quad k := \text{wt}(y_2).$$

Thus m, h, k are the input weights of the three accumulators.

A *cancellation trace* records the indices of vanishing prefix sums of the active values. Each nonvanishing active prefix contributes an output interval, extending to the next active position or to the end of the word. We call this a *contributing gap*. An input of weight M with trace size a has $M - a$ such gaps; the precise identity is given in [lemma 3.2](#).

Writing a, b, c for the three trace sizes, the stage parameters for a witness are:

Stage	Input weight	Trace size	Contributing gaps	Output condition
1	$m = rw$	a	$m - a$	weight h
2	h	b	$h - b$	weight k
3	k	c	$k - c$	weight at most L_δ

2.2 Basic reductions

The first reduction explains why extending the field does not change the minimum distance of a fixed realization.

Lemma 2.1 (Prime-field reduction). *Every entry of G_3 lies in the prime subfield $\mathbb{F}_p$, and*

$$d_{\min, \mathbb{F}_q}(G_3) = d_{\min, \mathbb{F}_p}(G_3).$$

Proof. Choose an $\mathbb{F}_p$ -basis $\beta_1, \dots, \beta_\ell$ of $\mathbb{F}_q$. Every message has a unique decomposition

$$\mathbf{x} = \sum_{j=1}^{\ell} \beta_j \mathbf{x}^{(j)}, \quad \mathbf{x}^{(j)} \in \mathbb{F}_p^n.$$

Since G_3 has entries in $\mathbb{F}_p$,

$$\mathbf{x}G_3 = \sum_{j=1}^{\ell} \beta_j (\mathbf{x}^{(j)} G_3).$$

At each output coordinate, this sum is zero if and only if all its $\mathbb{F}_p$ -components are zero. Hence

$$\text{supp}(\mathbf{x}G_3) = \bigcup_{j: \mathbf{x}^{(j)} \neq 0} \text{supp}(\mathbf{x}^{(j)} G_3).$$

Every nonzero message therefore has output weight at least the minimum prime-field output weight. The reverse inequality follows from $\mathbb{F}_p^n \subseteq \mathbb{F}_q^n$. $\square$

This reduction need not preserve the weight of a witnessing message: a component $\mathbf{x}^{(j)}$ may have smaller support than $\mathbf{x}$. We use it for the global minimum-distance interpretation, not to identify the individual events $\mathcal{E}_{3,w}(\delta)$.

The second reduction will let us use a two-accumulator estimate for growing sparse messages.

Lemma 2.2 (Difference support). *For every $z \in \mathbb{F}_q^N$,*

$$\text{wt}(zA^{-1}) \leq 2 \text{wt}(z).$$

Consequently,

$$\text{wt}(y_2) \leq 2 \text{wt}(y_3). \quad (2.2)$$

Proof. The inverse accumulator is the first-difference operator:

$$(zA^{-1})_1 = z_1, \quad (zA^{-1})_j = z_j - z_{j-1} \quad (j \geq 2).$$

Therefore

$$\text{supp}(zA^{-1}) \subseteq \text{supp}(z) \cup \{j+1 : j \in \text{supp}(z), j < N\}.$$

Since permutations preserve weight,

$$\text{wt}(y_2) = \text{wt}(y_2 \Pi_3) = \text{wt}(y_3 A^{-1}) \leq 2 \text{wt}(y_3).$$

□

3 Cancellation Traces and Random Gaps

This section separates the algebraic and geometric parts of an accumulator transition. The active order determines which prefix sums vanish, while the active support determines how much weight each nonvanishing prefix contributes. We then combine these one-stage facts using a rank bound shared by all three stages.

3.1 Random interleavers and cancellation traces

Let $B \subseteq [N]$ be a fixed set of M active coordinates, and let π be a uniform permutation. Write

$$\pi(B) = \{p_1 < \dots < p_M\}, \quad \lambda_j := \pi^{-1}(p_j).$$

The set $\{p_1, \dots, p_M\}$ is the active support, while $(\lambda_1, \dots, \lambda_M)$ is the active order.

Lemma 3.1 (Order-support decomposition). *The active support is a uniform M -subset of $[N]$. Conditional on that support, the active order is a uniform ordering of B . In particular, active support and active order are independent.*

Proof. The restriction of a uniform permutation to B is a uniform injection into $[N]$. Every M -subset is the range of exactly $M!$ injections, and conditional on the range all $M!$ assignments are equally likely. □

Now consider an accumulator input z with active positions $p_1 < \dots < p_M$ and active values $c_i = z_{p_i} \neq 0$. Define

$$\sigma_i := \sum_{j=1}^i c_j, \quad Z(z) := \{i \in [M] : \sigma_i = 0\}.$$

The set $Z(z)$ is its cancellation trace. Its indices refer to the active sequence, not to the original coordinate positions. Put

$$p_{M+1} := N+1, \quad \Delta_i := p_{i+1} - p_i.$$

Lemma 3.2 (Nonadjacency and gap identity). *For every active sequence:*

- (i) $1 \notin Z(z)$;
- (ii) $Z(z)$ contains no consecutive indices;
- (iii)

$$\text{wt}(zA) = \sum_{i \in [M] \setminus Z(z)} \Delta_i. \quad (3.1)$$

The number of possible traces of size a is at most

$$D(M, a) := \binom{M-a}{a}. \quad (3.2)$$

Proof. The first active prefix is $c_1 \neq 0$. If $\sigma_i = \sigma_{i+1} = 0$, then $c_{i+1} = \sigma_{i+1} - \sigma_i = 0$, a contradiction. Between p_i and $p_{i+1} - 1$, the ordinary coordinate prefix sum equals σ_i , proving the weight identity.

For the count, write $Z(z) = \{i_1 < \dots < i_a\}$. The conditions are $i_1 \geq 2$ and $i_{j+1} \geq i_j + 2$. The map

$$(i_1, \dots, i_a) \mapsto (i_1 - 1, i_2 - 2, \dots, i_a - a)$$

is a bijection from these nonadjacent sets onto the a -subsets of $[M - a]$. Not all such sets need be algebraically realizable, so (3.2) is an upper bound on the number of traces. $\square$

3.2 Exact gap laws

A uniform M -subset

$$1 \leq p_1 < \dots < p_M \leq N$$

corresponds bijectively to a uniform weak composition of $N - M$:

$$g_0 = p_1 - 1, \quad g_i = p_{i+1} - p_i - 1 \quad (1 \leq i \leq M), \quad p_{M+1} = N + 1.$$

Here a weak composition is an ordered tuple of nonnegative integers with the specified sum, and $\Delta_i = g_i + 1$.

Lemma 3.3 (Exact prescribed-gap sum). *For a fixed nonempty $S \subseteq [M]$, put $j = |S|$. For every integer h ,*

$$\mathbb{P} \left[\sum_{i \in S} \Delta_i = h \right] = \frac{\binom{h-1}{j-1} \binom{N-h}{M-j}}{\binom{N}{M}}.$$

The probability is zero unless $j \leq h \leq N - M + j$, and the law depends on S only through j .

Proof. The event is equivalent to $\sum_{i \in S} g_i = h - j$. There are $\binom{h-1}{j-1}$ possible selected gaps. The $M + 1 - j$ unselected gaps, including g_0 , have total $N - M - h + j$, giving $\binom{N-h}{M-j}$ possibilities. Divide by the total number $\binom{N}{M}$ of weak compositions. $\square$

For $1 \leq M \leq N$, $0 \leq a \leq M - 1$, and output weight H , define

$$g_{1,N}(M, a, H) := \frac{\binom{H-1}{M-a-1} \binom{N-H}{a}}{\binom{N}{M}}. \quad (3.3)$$

This is the exact output-weight law for a prescribed trace of size a when the support is uniform. In particular,

$$\sum_{H=1}^N g_{1,N}(M, a, H) = 1. \quad (3.4)$$

For the last accumulator, let $L = L_\delta$. For input weight K and trace size c , define

$$g_{2,N,\delta}(K, c) := \frac{1}{\binom{N}{K}} \sum_{\ell=K-c}^L \binom{\ell-1}{K-c-1} \binom{N-\ell}{c}. \quad (3.5)$$

Thus $g_{2,N,\delta}(K, c)$ is the prescribed-trace probability of output weight at most L .

Lemma 3.4 (Hypergeometric form). *Let X count the points of a uniform K -subset of $[N]$ lying in the terminal interval of length L . Then*

$$X \sim \text{Hyp}(N, L, K), \quad g_{2,N,\delta}(K, c) = \mathbb{P}[X \geq K - c].$$

Proof. Put $j = K - c$. By exchangeability of the weak-composition gaps, any prescribed sum of j contributing gaps has the same law as the sum of the final j gaps. For ordered support $p_1 < \dots < p_K$,

$$\sum_{i=c+1}^K \Delta_i = N + 1 - p_{c+1}.$$

This is at most L exactly when $p_{c+1} \geq N - L + 1$, or equivalently when at least $K - c$ support points lie in the terminal interval. $\square$

We will use the following two consequences of the exact laws.

Lemma 3.5 (Fixed-trace final tail). *For $0 < \delta \leq 1/2$, $1 \leq K \leq N$, and $0 \leq c \leq \lfloor K/2 \rfloor$,*

$$g_{2,N,\delta}(K, c) \leq \rho_\delta^K, \quad \rho_\delta := 2\sqrt{\delta(1-\delta)}.$$

In particular,

$$g_{2,N,1/10}(K, c) \leq (3/5)^K.$$

Proof. By lemma 3.4,

$$g_{2,N,\delta}(K, c) \leq \mathbb{P}[X \geq K/2].$$

If $L = 0$, this probability is zero. Otherwise put $\delta_N = L/N$. For $z \geq 1$, the binomial moments of the hypergeometric variable give

$$\begin{aligned} \mathbb{E}[z^X] &= \sum_{i=0}^K (z-1)^i \binom{K}{i} \frac{\binom{L}{i}}{\binom{N}{i}} \\ &\leq \sum_{i=0}^K (z-1)^i \binom{K}{i} \delta_N^i = (1 - \delta_N + \delta_N z)^K. \end{aligned}$$

The inequality uses $\binom{L}{i}/\binom{N}{i} \leq (L/N)^i$, obtained by comparing the factors in the corresponding product.

Markov's inequality with $z = (1 - \delta_N)/\delta_N \geq 1$ therefore yields

$$\mathbb{P}[X \geq K/2] \leq (2\sqrt{\delta_N(1-\delta_N)})^K \leq \rho_\delta^K.$$

$\square$

Lemma 3.6 (First-gap generating transform). *Let $1 \leq M \leq N$, $0 \leq a \leq M - 1$, and $0 < \rho < 1$. Put $j = M - a$. Then*

$$\sum_{H=1}^N g_{1,N}(M, a, H) \rho^H \leq \left(\frac{M}{N} \frac{\rho}{1-\rho} \right)^j.$$

Proof. Every nonzero term has $H \geq j$, so

$$\begin{aligned} \sum_H g_{1,N}(M, a, H) \rho^H &\leq \frac{\binom{N-j}{a}}{\binom{N}{M}} \sum_{H \geq j} \binom{H-1}{j-1} \rho^H \\ &= \frac{\binom{N-j}{a}}{\binom{N}{M}} \left(\frac{\rho}{1-\rho} \right)^j. \end{aligned}$$

Since $M = a + j$,

$$\frac{\binom{N-j}{a}}{\binom{N}{M}} = \prod_{i=1}^j \frac{a+i}{N-j+i} \leq \left(\frac{M}{N} \right)^j.$$

Indeed,

$$M(N-j+i) - N(a+i) = (N-M)(j-i) \geq 0$$

for $1 \leq i \leq j$. □

3.3 A shared rank bound

Fix a message support of size w . Once the current active order and the earlier supports and traces are fixed, each accumulator prefix is a homogeneous linear form in the original w message values. Later families of forms can depend on the earlier trace history.

The next theorem controls this adaptive dependence. Its essential point is that all vanishing forms annihilate the same nonzero message, so their combined rank is at most $w - 1$.

For $M \geq 0$ and $w \geq 1$, define

$$\mathcal{A}(M, w) := \sum_{d=0}^{w-1} \binom{M}{d}.$$

Theorem 3.7 (Three-stage shared-rank trace bound). *Let U be a w -dimensional vector space, with $w \geq 1$. For $i = 1, 2, 3$ and every possible earlier trace history $\tau_{<i}$, let*

$$\mathcal{L}_i(\tau_{<i}) = (\ell_{i,1}, \dots, \ell_{i,M_i})$$

be an indexed family of elements of the dual space U^* . Assume that this family is determined by $\tau_{<i}$ and fixed auxiliary data, with no further dependence on the witness $v \in U$.

For $v \neq 0$, define recursively

$$\tau_i(v) := \{j \in [M_i] : \ell_{i,j}(\tau_{<i}(v))(v) = 0\}.$$

Then the number of trace triples realized by nonzero witnesses is at most

$$\mathcal{A}(M_1 + M_2 + M_3, w).$$

Proof. Fix a realized trace triple and a witness $v \neq 0$. Let $V_0 = \{0\}$. Recursively, let $V_i \subseteq U^*$ be the span of V_{i-1} and all stage- i forms that vanish at v . Every form in V_i annihilates v , so

$$V_i \subseteq v^\perp, \quad \dim V_3 \leq w - 1.$$

At stage i , use a deterministic rule, such as greedy lexicographic selection, to choose $B_i \subseteq \tau_i(v)$ whose forms extend the already selected basis of V_{i-1} to a basis of V_i . If $d_i = |B_i|$, then

$$d_1 + d_2 + d_3 = \dim V_3 \leq w - 1.$$

The sets B_1, B_2, B_3 determine the traces recursively. Once the earlier traces are known, the current form family is known. The selected forms determine V_i , and

$$\tau_i(v) = \{j \in [M_i] : \ell_{i,j} \in V_i\}.$$

One inclusion follows from the definition of V_i ; the other holds because every form in V_i annihilates v . Thus distinct trace triples have distinct canonical labels. Counting these labels and using Vandermonde's identity gives

$$\sum_{d_1+d_2+d_3 \leq w-1} \prod_{i=1}^3 \binom{M_i}{d_i} = \sum_{d=0}^{w-1} \binom{M_1 + M_2 + M_3}{d}.$$

□

For the coding application, the relevant family sizes are m, h, k . Accordingly, define

$$J_3(m, h, k, w) := \sum_{d=0}^{w-1} \binom{m + h + k}{d}. \quad (3.6)$$

The bound is field-independent: it counts possible zero patterns through their defining equations, rather than enumerating assignments of message values.

3.4 The master probability bound

Fix a message support $T \subseteq [n]$ of size w , and put $m = rw$. For trace sizes a, b, c and intermediate weights h, k , consider the event that some message supported exactly on T realizes these parameters and has final weight at most L_δ .

Proposition 3.8 (Three-stage master bound). *For every $1 \leq w \leq n$,*

$$\begin{aligned} \mathbb{P}[\mathcal{E}_{3,w}(\delta)] &\leq \binom{n}{w} \sum_{a=0}^{\lfloor m/2 \rfloor} \sum_{h=1}^N \sum_{b=0}^{\lfloor h/2 \rfloor} \sum_{k=1}^N \sum_{c=0}^{\lfloor k/2 \rfloor} g_{1,N}(m, a, h) g_{1,N}(h, b, k) g_{2,N,\delta}(k, c) \\ &\quad \times \min\{J_3(m, h, k, w), D(m, a)D(h, b)D(k, c)\}. \end{aligned} \quad (3.7)$$

Proof. Fix T, a, h, b, k, c . We give two ways to label possible witnesses. In both cases, the labels are fixed before the interleavers are exposed.

For the shared-rank bound, fix index sets

$$B_1 \subseteq [m], \quad B_2 \subseteq [h], \quad B_3 \subseteq [k], \quad |B_1| + |B_2| + |B_3| \leq w - 1.$$

Starting with $V_0 = \{0\}$, process the stages sequentially. At stage i , expose the active order and hence the current prefix forms. Reconstruct

$$V_i = V_{i-1} + \text{span}\{\ell_{i,j} : j \in B_i\}, \quad Z_i = \{j : \ell_{i,j} \in V_i\}.$$

Discard the candidate if Z_i has the wrong prescribed size or violates the trace constraints. Otherwise expose the current active support, independently of the active order, and test the required output-weight condition.

This reconstruction uses neither the current random support nor any later interleaver. By [lemmas 3.1 and 3.3](#), the successive conditional probabilities of the three required gap events are therefore

$$g_{1,N}(m, a, h), \quad g_{1,N}(h, b, k), \quad g_{2,N,\delta}(k, c).$$

After each stage, its exact output support is determined by the trace and gaps. This support supplies the active coordinate labels for the next stage. The next interleaver is fresh and uniform, so the same argument applies again. The tower property bounds the success probability of each fixed label by the product of the three kernels.

Every genuine witness is covered by its canonical basis-extension label from [theorem 3.7](#). The number of possible index-set triples is $J_3(m, h, k, w)$.

Alternatively, fix the three zero sets themselves. There are at most $D(m, a)D(h, b)D(k, c)$ choices by [lemma 3.2](#). The same sequential support exposure bounds each label's probability by the same kernel product. Algebraically infeasible labels only enlarge this upper bound.

Apply the union bound using either label family, take the smaller bound, and sum over the five parameters and the $\binom{n}{w}$ choices of T . $\square$

We call the two terms inside the minimum in (3.7) the *shared-rank branch* and the *nonadjacency branch*. The former is useful for sparse messages; the latter exposes the entropy governing linear-density messages.

4 A Matching Lower Bound

The lower bound uses weight-two messages and two successive adjacent-pair collapses. Put

$$s := \lfloor r/2 \rfloor, \quad t_r := \lceil r/2 \rceil.$$

Proposition 4.1 (Matching lower bound). *For every fixed $r \geq 4$ and $\delta > 0$,*

$$\mathbb{P}[d_{\min}(G_3) \leq \delta N] = \Omega_{r,\delta}(N^{2-r-t_r})$$

as $N \rightarrow \infty$ through multiples of r , uniformly over finite fields of odd characteristic.

The weaker characteristic hypothesis here is sufficient because the construction uses only the distinct values $+1$ and -1 . It will also supply the lower bound for the refinement in [corollary 7.2](#).

4.1 A weight-two construction

By monotonicity, it suffices to consider $0 < \delta \leq 1$. Take N large enough that $L_\delta \geq t_r$. For an unordered message pair $e = \{u, v\}$, write $u < v$ and set

$$\mathbf{x}_e := e_u - e_v.$$

For the first interleaver, require the $2r$ repeated copies to form r disjoint adjacent mixed pairs. A path on N vertices has $\binom{N-r}{r}$ matchings of size r : if the left endpoints are $i_1 < \dots < i_r$, shift i_j to $i_j - (j - 1)$. Each matching has 2^r mixed assignments of its endpoints to the u - and v -blocks. Thus the unrestricted mixed-pair probability is

$$\frac{\binom{N-r}{r}}{\binom{N}{2r}} \frac{2^r}{\binom{2r}{r}} = \frac{2^r}{\binom{N}{r}} = \Theta_r(N^{-r}). \quad (4.1)$$

If $r = 2s$, require exactly s pairs to have their $+1$ endpoint first. If $r = 2s + 1$, require exactly $s + 1$ pairs to have their $+1$ endpoint first. Conditional on the unrestricted event, these restrictions have probabilities

$$2^{-2s} \binom{2s}{s}, \quad 2^{-(2s+1)} \binom{2s+1}{s+1},$$

respectively. They are positive constants depending only on r .

Each pair contributes one nonzero coordinate after accumulation. The first output therefore has weight r , with s copies of each sign when $r = 2s$, or $s + 1$ copies of $+1$ and s copies of -1 when $r = 2s + 1$.

For even $r = 2s$, require the second interleaver to place these values into s adjacent opposite-sign pairs. Its conditional probability is

$$\frac{\binom{N-s}{s}}{\binom{N}{2s}} \frac{2^s}{\binom{2s}{s}} = \frac{2^s}{\binom{N}{s}} = \Theta_r(N^{-s}).$$

The second accumulator output then has weight $s = t_r$.

For odd $r = 2s + 1$, require an excess-sign entry at coordinate N , and require the remaining values to form s adjacent opposite-sign pairs in $[N - 1]$. The conditional probability is

$$\frac{\binom{N-s-1}{s}}{\binom{N}{2s+1}} \frac{2^s}{\binom{2s+1}{s+1}} = \Theta_r(N^{-(s+1)}) = \Theta_r(N^{-t_r}).$$

The second accumulator output again has weight t_r : one coordinate from each pair and one from the terminal singleton.

Finally, require the third interleaver to map this weight- t_r support into the terminal interval of length L_δ . The probability is

$$\frac{\binom{L_\delta}{t_r}}{\binom{N}{t_r}} \longrightarrow \delta^{t_r} > 0.$$

The final accumulator output is supported in that interval and is nonzero because $\Pi_3 A$ is invertible.

Let $\mathcal{F}_e$ denote the complete event. Independence of the interleavers gives

$$\mathbb{P}(\mathcal{F}_e) = \Theta_{r,\delta}(N^{-r-t_r}), \quad \mathcal{F}_e \subseteq \mathcal{E}_{3,2}(\delta). \quad (4.2)$$

4.2 Counting witnesses and their intersections

Proof of proposition 4.1. There are $\binom{n}{2} = \Theta_r(N^2)$ message pairs, so (4.2) gives

$$\sum_e \mathbb{P}(\mathcal{F}_e) = \Theta_{r,\delta}(N^{2-r-t_r}).$$

We bound intersections under the same three global interleavers.

Suppose distinct pairs e, f share one message coordinate. Fix the r positions of the shared repeated block. Each of the other two blocks must occupy an r -subset of the at most $2r$ neighboring positions. There are $O_r(1)$ such subsets, whereas an unconstrained disjoint r -subset has $\Theta_r(N^r)$ possibilities. Hence the two first-stage conditions jointly have probability $O_r(N^{-2r})$, and

$$\mathbb{P}(\mathcal{F}_e \cap \mathcal{F}_f) = O_r(N^{-2r}).$$

There are $O_r(N^3)$ overlapping pairs of message pairs. Their total contribution is

$$O_r(N^{3-2r}) = o_r(N^{2-r-t_r}),$$

since $1 - r + t_r < 0$.

For disjoint message pairs, the first-stage conditions jointly cost $O_r(N^{-2r})$: choose one block from each pair freely, after which each partner has only $O_r(1)$ neighboring supports among $\Theta_r(N^r)$ possibilities.

Conditional on these events, the two first-output supports are disjoint. If r is odd, their prescribed second-stage events are incompatible, since both require an active entry at coordinate N . If $r = 2s$, there are $O_r(N^{2s})$ ordered pairs of disjoint size- s path matchings, compared with $\Theta_r(N^{4s})$ ordered pairs of disjoint $2s$ -subsets. Thus the two second-stage conditions jointly cost $O_r(N^{-2s})$. In either parity,

$$\mathbb{P}(\mathcal{F}_e \cap \mathcal{F}_f) = O_r(N^{-2r-2t_r}).$$

The total over disjoint pairs is therefore

$$O_r(N^{4-2r-2t_r}) = o_r(N^{2-r-t_r}),$$

because $2 - r - t_r < 0$.

Bonferroni's inequality now gives

$$\begin{aligned} \mathbb{P}\left(\bigcup_e \mathcal{F}_e\right) &\geq \sum_e \mathbb{P}(\mathcal{F}_e) - \sum_{\{e,f\}: e \neq f} \mathbb{P}(\mathcal{F}_e \cap \mathcal{F}_f) \\ &= \Omega_{r,\delta}(N^{2-r-t_r}), \end{aligned}$$

where the second sum is over unordered pairs of distinct events. The union is contained in $\{d_{\min}(G_3) \leq L_\delta\}$. All constants are independent of the odd-characteristic field. $\square$

5 Upper Bound for Sparse Messages

The shared-rank branch of the master bound is effective when the message weight is small. We first treat fixed weights using nested gap transforms, then give a uniform estimate for the remaining sparse range. Define

$$\psi(j) := j + \lceil j/2 \rceil.$$

5.1 Fixed message weights

Lemma 5.1 (A uniform pointwise kernel bound). *Fix $M \geq 1$. For every $N \geq M$, $0 \leq a \leq \lfloor M/2 \rfloor$, $j = M - a$, and $1 \leq H \leq N$,*

$$g_{1,N}(M, a, H) \leq M^M N^{-j} \binom{H-1}{j-1}.$$

Proof. From (3.3),

$$g_{1,N}(M, a, H) \leq \frac{N^a \binom{H-1}{j-1}}{\binom{N}{M}}.$$

Also,

$$\binom{N}{M} = \prod_{i=0}^{M-1} \frac{N-i}{M-i} \geq \left(\frac{N}{M}\right)^M,$$

since every factor is at least N/M . Substitution gives the result, with an explicit constant depending only on M . $\square$

Lemma 5.2 (Nested transform for fixed input weight). *Fix integers $w, M \geq 1$ and $0 < \delta < 1/2$. For $N \geq M$ and $1 \leq H \leq N$, define*

$$F_{N,M,w,\delta}(H) := \sum_{b=0}^{\lfloor H/2 \rfloor} \sum_{K=1}^N \sum_{c=0}^{\lfloor K/2 \rfloor} g_{1,N}(H, b, K) g_{2,N,\delta}(K, c) J_3(M, H, K, w). \quad (5.1)$$

There exist $C_0, C_1 > 0$, $D \geq 0$, and $0 < \rho < 1$, depending only on M, w, δ , such that

$$F_{N,M,w,\delta}(H) \leq C_1(1+H)^D \eta_N(H)^{\lceil H/2 \rceil}, \quad \eta_N(H) := \min \left\{ C_0 \frac{H}{N}, \rho \right\}.$$

In particular, for each fixed H ,

$$F_{N,M,w,\delta}(H) = O_{M,w,\delta,H}(N^{-\lceil H/2 \rceil}).$$

Proof. Since M, w are fixed,

$$J_3(M, H, K, w) \leq C_{M,w}(1+H+K)^{w-1}.$$

By lemma 3.5, the final fixed-trace probability is at most ρ_δ^K . Summing over c costs at most a factor $K+1$.

Choose ρ_1 with $\rho_\delta < \rho_1 < 1$. A geometric decay absorbs any fixed polynomial, giving

$$(K+1)(1+H+K)^{w-1} \rho_\delta^K \leq C'(1+H)^{w-1} \rho_1^K.$$

For fixed b , lemma 3.6 yields

$$\sum_K g_{1,N}(H, b, K) \rho_1^K \leq \left(\frac{H}{N} \frac{\rho_1}{1-\rho_1} \right)^{H-b}.$$

On the other hand, nonzero terms have $K \geq H-b$; normalization (3.4) gives

$$\sum_K g_{1,N}(H, b, K) \rho_1^K \leq \rho_1^{H-b}.$$

Set $C_0 = \rho_1/(1-\rho_1)$ and $\rho = \rho_1$. The two bounds together give $\eta_N(H)^{H-b}$. Since $H-b \geq \lceil H/2 \rceil$, $\eta_N(H) < 1$, and there are at most $H+1$ choices of b , the claim follows with $D = w$. $\square$

Proposition 5.3 (Fixed message weights). *Fix $r \geq 4$. For every fixed $w \geq 2$, uniformly over all finite fields,*

$$\mathbb{P}[\mathcal{E}_{3,w}(1/10)] = O_{r,w}\left(N^{w-\psi(\lceil rw/2 \rceil)}\right). \quad (5.2)$$

If $p > r$, then also

$$\mathbb{P}[\mathcal{E}_{3,1}(1/10)] = O_r\left(N^{1-\psi(r)}\right). \quad (5.3)$$

Proof. Fix a message support T , put $m = rw$, and use the shared-rank branch of [proposition 3.8](#). For a fixed first trace size a , put $j = m - a$. Nonadjacency gives $j \geq \lceil m/2 \rceil$.

By [lemmas 5.1](#) and [5.2](#), the contribution for this trace size is at most

$$C_2 N^{-j} \sum_{H=j}^N \binom{H-1}{j-1} (1+H)^D \eta_N(H)^{\lceil H/2 \rceil}.$$

Put $k_0 = \lceil j/2 \rceil$ and $s_H = \lceil H/2 \rceil$. Since $s_H \geq k_0$,

$$\min\{A, B\}^{s_H} \leq A^{k_0} B^{s_H - k_0} \quad (A, B > 0)$$

gives

$$\eta_N(H)^{s_H} \leq \left(\frac{C_0 H}{N}\right)^{k_0} \rho^{s_H - k_0}.$$

Consequently,

$$\begin{aligned} & \sum_{H=j}^N \binom{H-1}{j-1} (1+H)^D \eta_N(H)^{\lceil H/2 \rceil} \\ & \leq \frac{C_3}{N^{k_0}} \sum_{H=j}^{\infty} (1+H)^{j+D+k_0-1} \rho^{H/2} = O_{r,w}(N^{-k_0}). \end{aligned}$$

Thus the contribution for this first trace size is $O_{r,w}(N^{-\psi(j)})$. There are only finitely many a , and ψ is increasing, so the largest bound uses $j = \lceil rw/2 \rceil$. Multiplication by $\binom{n}{w} = O_{r,w}(N^w)$ proves (5.2).

For $w = 1$, the first active increments are r identical nonzero values. If $p > r$, their prefixes $c, 2c, \dots, rc$ are all nonzero. Thus only $a = 0$ is possible, and the same calculation with $j = r$ proves (5.3). $\square$

For $w = 2$, the bound becomes

$$O_r(N^{2-r-\lceil r/2 \rceil}),$$

matching [proposition 4.1](#). To record the other fixed weights used below, let

$$E_2 := 2 - r - \lceil r/2 \rceil.$$

Their upper-bound exponents satisfy

w	upper-bound exponent
1	$E_2 - 1$
3	$E_2 + 1 - \lceil (r + \lceil r/2 \rceil)/2 \rceil \leq E_2 - 2$
4	$4 - 3r \leq E_2 - 4$

for $r \geq 4$. Thus weights 1, 3, 4 contribute $o_r(N^{E_2})$ under $p > r$.

5.2 Growing sparse weights

Let $G_2 = R\Pi_1 A\Pi_2 A$ be the two-accumulator prefix of G_3 . We prove the sparse estimate needed here directly, at the doubled threshold supplied by [lemma 2.2](#).

Lemma 5.4 (Sparse two-accumulator estimate). *Fix $r \geq 4$. There exist $B_r < \infty$ and $x_r > 0$ such that, for $N = rn$, $2 \leq w \leq n$, and $m = rw$ satisfying $m/N \leq x_r$,*

$$\mathbb{P}[\exists \mathbf{x} \in \mathbb{F}_q^n : \text{wt}(\mathbf{x}) = w, \text{wt}(\mathbf{x}G_2) \leq L_{1/5}] \leq \left[B_r \left(\frac{w}{N} \right)^{r/2-1} \right]^w.$$

The constants are uniform over all finite fields.

Proof. At threshold $1/5$, [lemma 3.5](#) gives

$$\rho_{1/5} = 2\sqrt{\frac{1}{5}\frac{4}{5}} = \frac{4}{5}.$$

Fix a message support T , and expose the first active order. The one-stage case of [theorem 3.7](#) gives at most $\mathcal{A}(m, w)$ first traces. For each, expose its exact output support before the second active order. Conditional on that history, at most $\mathcal{A}(H, w)$ second traces are possible. Using the fixed-trace final tail and averaging over the conditioned data gives

$$\mathbb{P}[\text{a witness on } T] \leq \mathcal{A}(m, w) \max_{0 \leq a \leq \lfloor m/2 \rfloor} \sum_{H=1}^N g_{1,N}(m, a, H) \mathcal{A}(H, w) (4/5)^H.$$

Nonzero terms have $H \geq m/2 \geq 2w$. For $M \geq 2w$,

$$\mathcal{A}(M, w) \leq w \binom{M}{w-1} \leq \left(\frac{4eM}{w} \right)^w.$$

Write

$$\frac{4}{5} = \frac{8}{9} \cdot \frac{9}{10}, \quad \kappa := \log(9/8).$$

Since

$$\sup_{y \geq 0} y^w (8/9)^y = \left(\frac{w}{e\kappa} \right)^w,$$

we obtain

$$\mathcal{A}(H, w) (4/5)^H \leq \left(\frac{4}{\kappa} \right)^w (9/10)^H.$$

By [lemma 3.6](#),

$$\sum_H g_{1,N}(m, a, H) (9/10)^H \leq \left(9 \frac{m}{N} \right)^{m-a}.$$

Choose $x_r \leq 1/9$. Then $9m/N \leq 1$, and $m-a \geq m/2$ makes the last expression at most $(9m/N)^{m/2}$.

Finally,

$$\mathcal{A}(m, w) \leq (4er)^w, \quad \binom{n}{w} \leq \left(\frac{eN}{rw} \right)^w.$$

Combining these estimates yields

$$\begin{aligned} \mathbb{P}[\exists \text{ a witness of weight } w] &\leq \binom{n}{w} \mathcal{A}(m, w) \left(\frac{4}{\kappa} \right)^w \left(\frac{9m}{N} \right)^{m/2} \\ &\leq \left[\frac{16e^2}{\kappa} (9r)^{r/2} \left(\frac{w}{N} \right)^{r/2-1} \right]^w. \end{aligned}$$

Thus one may take

$$B_r := \frac{16e^2}{\log(9/8)} (9r)^{r/2}.$$

□

Proposition 5.5 (Growing sparse weights). *For fixed $r \geq 4$, after decreasing x_r if necessary,*

$$\sum_{\substack{5 \leq w \leq n \\ rw/N \leq x_r}} \mathbb{P}[\mathcal{E}_{3,w}(1/10)] = o_r \left(N^{2-r-\lceil r/2 \rceil} \right),$$

uniformly over all finite fields.

Proof. By lemma 2.2,

$$\mathcal{E}_{3,w}(1/10) \subseteq \{ \exists \mathbf{x} : \text{wt}(\mathbf{x}) = w, \text{wt}(\mathbf{x}G_2) \leq L_{1/5} \}.$$

Here $2 \lfloor N/10 \rfloor \leq \lfloor N/5 \rfloor$ handles the integer thresholds.

Apply lemma 5.4 and put

$$\alpha := r/2 - 1 > 0, \quad U_w := \lfloor B_r (w/N)^\alpha \rfloor^w.$$

For consecutive indices in the sparse range,

$$\begin{aligned} \frac{U_{w+1}}{U_w} &= B_r \left(\frac{w+1}{N} \right)^\alpha \left(1 + \frac{1}{w} \right)^{\alpha w} \\ &\leq B_r e^\alpha \left(\frac{2x_r}{r} \right)^\alpha. \end{aligned}$$

Decrease x_r so that this is at most $1/2$. With $W_N = \lfloor x_r N/r \rfloor$, the resulting geometric bound is

$$\sum_{w=5}^{W_N} U_w \leq 2U_5 = O_r \left(N^{-5(r/2-1)} \right).$$

If $W_N < 5$, the sum is empty.

The excess of this decay exponent over the target one is

$$5(r/2 - 1) - (r + \lceil r/2 \rceil - 2) = \begin{cases} r - 3, & r \text{ even}, \\ r - \frac{7}{2}, & r \text{ odd}, \end{cases}$$

which is positive for every $r \geq 4$.

□

6 Upper Bound for Linear-Density Messages

For messages whose weight is proportional to N , we use the nonadjacency branch of the master bound. Its exact combinatorial counts lead to an entropy expression involving all three accumulator transitions. We prove that this expression is uniformly negative on the relevant domain.

6.1 The three-stage entropy bound

For a probability vector p , write

$$H(p) := - \sum_i p_i \log p_i, \quad h(v) := -v \log v - (1-v) \log(1-v),$$

with $0 \log 0 = 0$. Also define binary relative entropy by

$$\text{kl}(v \parallel \theta) := v \log \frac{v}{\theta} + (1-v) \log \frac{1-v}{1-\theta}.$$

For an accumulator transition with input weight M , trace size a , and output weight H , the combined nonadjacency and gap counts involve the five integer cells

$$(a, a, M - 2a, H - M + a, N - H - a).$$

Normalize $M/N = \xi$, $H/N = \tau$, and $a/N = \zeta$. The feasible trace-density interval is

$$I(\xi, \tau) := [\max\{0, \xi - \tau\}, \min\{\xi/2, 1 - \tau\}]. \quad (6.1)$$

For $0 \leq \xi, \tau \leq 1$, it is nonempty exactly when $\xi \leq 2\tau$.

For $\zeta \in I(\xi, \tau)$, define the probability vector

$$\mathbf{c}(\xi, \tau, \zeta) := (\zeta, \zeta, \xi - 2\zeta, \tau - \xi + \zeta, 1 - \tau - \zeta),$$

and set

$$\mathcal{M}(\xi, \tau) := \max_{\zeta \in I(\xi, \tau)} \{H(\mathbf{c}(\xi, \tau, \zeta)) - h(\xi) - h(\tau)\}. \quad (6.2)$$

If $I(\xi, \tau)$ is empty, set $\mathcal{M}(\xi, \tau) = -\infty$.

The following bound will let us control $\mathcal{M}$ without explicitly solving the maximization over ζ .

Lemma 6.1 (A one-transition dual bound). *For every feasible pair (ξ, τ) and every $\lambda > 0$, put*

$$P(\lambda) := \frac{\lambda(2 + \lambda)}{1 + \lambda^2}, \quad \Lambda_\tau(\lambda) := \log(1 + \lambda^2) - 2\tau \log \lambda - h(\tau).$$

Then

$$\mathcal{M}(\xi, \tau) \leq \Lambda_\tau(\lambda) + \xi \log P(\lambda). \quad (6.3)$$

Proof. We use the log-sum inequality

$$H(p) + \sum_i p_i \log z_i \leq \log \sum_i z_i \quad (z_i > 0),$$

which follows from nonnegativity of relative entropy.

Fix a feasible ζ . For $0 < \xi < 1$, define

$$p^{(1)} := \frac{1}{\xi}(\zeta, \zeta, \xi - 2\zeta), \quad p^{(2)} := \frac{1}{1 - \xi}(\tau - \xi + \zeta, 1 - \tau - \zeta).$$

Then

$$H(\mathbf{c}) - h(\xi) = \xi H(p^{(1)}) + (1 - \xi) H(p^{(2)}).$$

Apply the log-sum inequality to $p^{(1)}$ with weights $(\lambda, \lambda, \lambda^2)$, and to $p^{(2)}$ with weights $(\lambda^2, 1)$. The total coefficient of $\log \lambda$ is

$$2\zeta + 2(\xi - 2\zeta) + 2(\tau - \xi + \zeta) = 2\tau.$$

Therefore

$$H(\mathbf{c}) - h(\xi) \leq \xi \log(\lambda(2 + \lambda)) + (1 - \xi) \log(1 + \lambda^2) - 2\tau \log \lambda.$$

Subtract $h(\tau)$ and maximize over ζ . Cases with a zero total mass follow by continuity. $\square$

Corollary 6.2 (A simple envelope). *For $0 < \tau < 1$, put*

$$\mathbf{B}(\tau) := \tau + 2\sqrt{\tau(1-\tau)}.$$

Then

$$\mathcal{M}(\xi, \tau) \leq \xi \log \mathbf{B}(\tau). \quad (6.4)$$

Proof. Choose $\lambda = \sqrt{\tau/(1-\tau)}$ in lemma 6.1. Then $\Lambda_\tau(\lambda) = 0$ and $P(\lambda) = \mathbf{B}(\tau)$. $\square$

For the three-stage chain, normalize

$$x := \frac{rw}{N} = \frac{w}{n}, \quad t := \frac{h}{N}, \quad u := \frac{k}{N}.$$

The scalar x denotes a normalized weight; the bold symbol $\mathbf{x}$ continues to denote a message vector.

Lemma 6.3 (Three-transition finite-type bound). *Every nonzero summand in the nonadjacency branch of (3.7) at $\delta = 1/10$, including $\binom{n}{w}$, is at most*

$$(N+1)^7 \exp \left\{ N \left[\frac{1}{r} \mathbf{h}(x) + \mathcal{M}(x, t) + \mathcal{M}(t, u) + \mathcal{M}(u, 1/10) \right] \right\}.$$

Every such summand satisfies

$$t \geq \frac{x}{2}, \quad u \geq \frac{t}{2}, \quad u \leq \frac{1}{5}, \quad x \leq \frac{4}{5}. \quad (6.5)$$

Proof. Write

$$F(\xi, \tau, \zeta) := \mathbf{H}(\mathbf{c}(\xi, \tau, \zeta)) - \mathbf{h}(\xi) - \mathbf{h}(\tau).$$

Direct factorial cancellation gives

$$D(M, a) g_{1,N}(M, a, H) = \frac{M-a}{H} \frac{\binom{N}{a, a, M-2a, H-M+a, N-H-a}}{\binom{N}{M} \binom{N}{H}}.$$

Using

$$\binom{N}{Nv} \geq \frac{e^{N\mathbf{h}(v)}}{N+1}, \quad \binom{N}{Np_1, \dots, Np_5} \leq e^{N\mathbf{H}(p)},$$

and $(M-a)/H \leq 1$ on nonzero terms, we obtain

$$D(M, a) g_{1,N}(M, a, H) \leq (N+1)^2 e^{N\mathcal{M}(M/N, H/N)}.$$

For the last transition, put

$$L := \lfloor N/10 \rfloor, \quad j := k - c, \quad \tau_N := L/N, \quad \chi := c/N.$$

A nonzero final kernel forces $j \leq L$. Since $j \geq k/2$, it follows that $k \leq 2L$. Define the hypergeometric masses

$$p_z := \frac{\binom{L}{z} \binom{N-L}{k-z}}{\binom{N}{k}}.$$

The initial mass p_j is positive: $j \leq L$ and $c \leq k/2 \leq L \leq N-L$. For $z \geq j$, successive nonzero masses satisfy

$$\frac{p_{z+1}}{p_z} = \frac{(L-z)(k-z)}{(z+1)(N-L-k+z+1)} \leq 1.$$

Indeed, $k - z \leq z + 1$, and $L - z \leq N - L - k + z + 1$ follows from $2z \geq k$ and $2L \leq N$. Hence

$$g_{2,N,1/10}(k, c) \leq (k + 1)p_j.$$

Another factorial cancellation gives

$$D(k, c)p_j = \frac{\binom{N}{c, c, k-2c, L-k+c, N-L-c}}{\binom{N}{k} \binom{N}{L}}.$$

The same type bounds therefore yield

$$D(k, c)g_{2,N,1/10}(k, c) \leq (N + 1)^3 e^{NF(u, \tau_N, \chi)}.$$

We may replace τ_N by $1/10$ in this exponent. Indeed,

$$\chi \leq u/2 \leq \tau_N \leq 1/10.$$

Increasing τ_N to $1/10$ preserves feasibility. On the interior,

$$\partial_\tau F(u, \tau, \chi) = \log \frac{\tau(1 - \tau - \chi)}{(1 - \tau)(\tau - u + \chi)} \geq 0,$$

because the numerator minus the denominator is

$$(1 - \tau)u - \chi \geq \frac{9}{10}u - \frac{1}{2}u = \frac{2}{5}u.$$

Boundary cases follow by continuity. Thus

$$F(u, \tau_N, \chi) \leq \mathcal{M}(u, 1/10).$$

Apply the ordinary-transition bound twice and the final-transition bound once, and use

$$\binom{n}{w} \leq e^{(N/r)\mathbf{h}(x)}.$$

This gives the factor $(N + 1)^7$.

Finally, each contributing gap has length at least one, while each trace contains at most half the active indices. Therefore

$$h \geq m - a \geq m/2, \quad k \geq h - b \geq h/2, \quad k/2 \leq k - c \leq L \leq N/10.$$

Dividing by N proves (6.5). □

Define

$$\Phi_r(x, t, u) := \frac{1}{r}\mathbf{h}(x) + \mathcal{M}(x, t) + \mathcal{M}(t, u) + \mathcal{M}(u, 1/10). \quad (6.6)$$

For $r \geq 4$, it is enough to control Φ_4 , since $\mathbf{h}(x)/r \leq \mathbf{h}(x)/4$.

6.2 An analytic bound on the exponent

Set

$$\lambda_0 := \frac{3}{14}, \quad \theta_0 := \frac{\lambda_0^2}{1 + \lambda_0^2} = \frac{9}{205}, \quad \alpha_0 := -\log P(\lambda_0) = \log \frac{205}{93}. \quad (6.7)$$

We split the entropy bound by inserting $-\alpha_0 t$ after the first transition and $+\alpha_0 t$ before the last two. The first part will be at most $-x/100$; the second will be nonpositive.

Lemma 6.4 (First-transition potential). *For $0 < x \leq 2t$ and $0 < t \leq 2/5$,*

$$\frac{1}{4}\mathbf{h}(x) + \mathcal{M}(x, t) - \alpha_0 t \leq -\frac{x}{100}. \quad (6.8)$$

Proof. Put

$$c_\star := \frac{11}{5}, \quad \varepsilon := \frac{1}{4} \log \frac{25}{24} > \frac{1}{100}, \quad \lambda^2 := \frac{t}{c_\star(1-t)} \leq \frac{10}{33}.$$

The bound on ε follows from $\log y > (y-1)/y$ for $y > 1$.

Write $A_\lambda = \lambda(2 + \lambda)$ and $B_\lambda = 1 + \lambda^2$. The binary entropy identity

$$\max_{0 \leq z \leq 1} \{ \mathbf{h}(z) + z \log a + (1-z) \log b \} = \log(a+b) \quad (a, b > 0)$$

and lemma 6.1 give

$$\frac{1}{4}\mathbf{h}(x) + \mathcal{M}(x, t) + \varepsilon x \leq \frac{1}{4} \log \left(B_\lambda^4 + \frac{25}{24} A_\lambda^4 \right) - 2t \log \lambda - \mathbf{h}(t). \quad (6.9)$$

We claim

$$B_\lambda^4 + \frac{25}{24} A_\lambda^4 \leq (1 + c_\star \lambda^2)^4.$$

Indeed, expansion gives

$$\begin{aligned} & \frac{(1 + c_\star \lambda^2)^4 - B_\lambda^4 - (25/24)A_\lambda^4}{\lambda^2} \\ &= \frac{24}{5} + \lambda^2 \left[\frac{478}{75} - \frac{100}{3} \lambda + \frac{1699}{125} \lambda^2 - \frac{25}{3} \lambda^3 + \left(c_\star^4 - \frac{49}{24} \right) \lambda^4 \right] \\ &\geq \frac{24}{5} + \lambda^2 \left(\frac{478}{75} - \frac{100}{3} \lambda - \frac{25}{3} \lambda^3 \right) \\ &\geq \frac{24}{5} - \frac{1157}{75} \lambda^2 \geq \frac{62}{495} > 0. \end{aligned}$$

Here $\lambda^2 \leq 10/33 < 9/25$, so $\lambda < 3/5$. The discarded terms are positive, and

$$\frac{478}{75} - \frac{100}{3} \lambda - \frac{25}{3} \lambda^3 \geq \frac{478}{75} - 20 - \frac{9}{5} = -\frac{1157}{75}.$$

Substitution into (6.9) yields

$$\begin{aligned} \frac{1}{4}\mathbf{h}(x) + \mathcal{M}(x, t) + \varepsilon x &\leq \log(1 + c_\star \lambda^2) - 2t \log \lambda - \mathbf{h}(t) \\ &= t \log c_\star < \alpha_0 t, \end{aligned}$$

where the identity uses the chosen λ , and the last inequality uses $11/5 < 205/93$. Since $\varepsilon > 1/100$, the claim follows. $\square$

Lemma 6.5 (Input potential). *For $0 \leq \tau \leq 1/5$ and $0 \leq \xi \leq 2\tau$,*

$$\mathcal{M}(\xi, \tau) + \alpha_0 \xi \leq \begin{cases} 0, & 0 \leq \tau \leq \theta_0, \\ \text{kl}(\tau \parallel \theta_0), & \theta_0 \leq \tau \leq 1/5. \end{cases}$$

Proof. If $\tau = 0$, feasibility gives $\xi = 0$, and the claim is immediate. For $0 < \tau \leq \theta_0$, [corollary 6.2](#) gives

$$\mathcal{M}(\xi, \tau) + \alpha_0 \xi \leq \xi \log \frac{\mathbf{B}(\tau)}{\mathbf{B}(\theta_0)} \leq 0.$$

Indeed,

$$\mathbf{B}'(\tau) = 1 + \frac{1 - 2\tau}{\sqrt{\tau(1 - \tau)}} > 0 \quad (0 < \tau < 1/2),$$

and

$$\mathbf{B}(\theta_0) = P(\lambda_0) = 93/205.$$

For $\tau \geq \theta_0$, choose $\lambda = \lambda_0$ in [lemma 6.1](#). The coefficient of ξ cancels, leaving

$$\log(1 + \lambda_0^2) - 2\tau \log \lambda_0 - \mathbf{h}(\tau) = \text{kl}(\tau \parallel \theta_0).$$

□

Lemma 6.6 (Last-two-transition potential). *For $0 < t \leq 2u$ and $0 < u \leq 1/5$,*

$$\mathcal{M}(t, u) + \mathcal{M}(u, 1/10) + \alpha_0 t \leq 0. \tag{6.10}$$

Proof. If $u \leq \theta_0$, then [lemma 6.5](#) and [corollary 6.2](#) give

$$\mathcal{M}(t, u) + \alpha_0 t \leq 0, \quad \mathcal{M}(u, 1/10) \leq u \log(7/10) < 0.$$

For $u \geq \theta_0$, it suffices to bound

$$H(u) := \mathcal{M}(u, 1/10) + \text{kl}(u \parallel \theta_0).$$

For fixed $\lambda > 0$, [lemma 6.1](#) gives $H(u) \leq F_\lambda(u)$, where

$$\begin{aligned} F_\lambda(u) &:= C_\lambda + u \log \frac{P(\lambda)u}{\theta_0} + (1 - u) \log \frac{1 - u}{1 - \theta_0}, \\ C_\lambda &:= \log(1 + \lambda^2) - \frac{1}{5} \log \lambda - \mathbf{h}(1/10). \end{aligned}$$

Since

$$F_\lambda''(u) = \frac{1}{u(1 - u)} > 0,$$

an upper bound at both endpoints controls the whole interval. We use

$$\lambda = \frac{1}{4} \quad \text{on } [\theta_0, 2/15], \quad \lambda = \frac{1}{9} \quad \text{on } [2/15, 1/5].$$

The elementary estimates

$$\log(1 + z) \leq z \quad (z > -1), \quad \log 2 < \frac{7}{10}, \quad \log 3 < \frac{11}{10}, \quad \mathbf{h}(1/10) > \frac{81}{250}$$

give

$$C_{1/4} < \frac{1}{16} + \frac{2}{5} \cdot \frac{7}{10} - \frac{81}{250} = \frac{37}{2000},$$

$$C_{1/9} < \frac{1}{81} + \frac{2}{5} \cdot \frac{11}{10} - \frac{81}{250} = \frac{2599}{20250}.$$

Using $P(1/4) = 9/17$ and $P(1/9) = 19/82$, the four endpoint expressions are

$$F_{1/4}(\theta_0) = C_{1/4} + \theta_0 \log(9/17),$$

$$F_{1/4}(2/15) = C_{1/4} + \frac{2}{15} \log(82/51) + \frac{13}{15} \log(533/588),$$

$$F_{1/9}(2/15) = C_{1/9} + \frac{2}{15} \log(19/27) + \frac{13}{15} \log(533/588),$$

$$F_{1/9}(1/5) = C_{1/9} + \frac{1}{5} \log(19/18) + \frac{4}{5} \log(41/49).$$

The inequalities

$$\log y \leq \frac{2(y-1)}{y+1} \quad (0 < y \leq 1), \quad \log(1+z) \leq z \quad (z > -1)$$

give

$$\log(9/17) \leq -\frac{8}{13}, \quad \log(533/588) \leq -\frac{110}{1121},$$

$$\log(19/27) \leq -\frac{8}{23}, \quad \log(19/18) \leq \frac{1}{18}, \quad \log(41/49) \leq -\frac{8}{45}.$$

Together with $\log(82/51) < 12/25$, substitution yields

λ	u	strict upper bound for $F_\lambda(u)$
1/4	θ_0	$-9079/1066000$
1/4	2/15	$-3421/1345200$
1/9	2/15	$-1605083/522105750$
1/9	1/5	$-28/10125$

Each bound is less than $-1/500$. By convexity, F_λ is bounded above by the line segment joining its endpoint values. Thus $H(u) < -1/500$ throughout $[\theta_0, 1/5]$, proving (6.10). $\square$

Theorem 6.7 (Three-stage entropy margin). *For every $r \geq 4$ and every feasible triple satisfying (6.5),*

$$\Phi_r(x, t, u) = \frac{1}{r} \mathbf{h}(x) + \mathcal{M}(x, t) + \mathcal{M}(t, u) + \mathcal{M}(u, 1/10) \leq -\frac{x}{100}.$$

Proof. First suppose $x, t, u > 0$. Since $r \geq 4$, replace $\mathbf{h}(x)/r$ by $\mathbf{h}(x)/4$. Feasibility gives

$$x \leq 2t, \quad t \leq 2u, \quad u \leq 1/5, \quad t \leq 2/5.$$

Add lemmas 6.4 and 6.6. The terms $\alpha_0 t$ cancel, leaving $-x/100$. Boundary cases follow by continuity on the feasible domain. $\square$

Proposition 6.8 (Linear-density messages). *For every fixed $r \geq 4$ and $x_* > 0$, for all sufficiently large $N = rn$,*

$$\sum_{\substack{1 \leq w \leq n \\ rw/N \geq x_*}} \mathbb{P}[\mathcal{E}_{3,w}(1/10)] \leq e^{-x_* N/200}.$$

The sufficiently-large- N threshold is independent of the field.

Proof. Use the nonadjacency branch of [proposition 3.8](#). By [lemma 6.3](#) and [theorem 6.7](#), every nonzero summand, including the message-support factor, is at most

$$(N+1)^7 e^{-xN/100} \leq (N+1)^7 e^{-x_*N/100}.$$

There are at most $(N+1)^6$ choices of (w, a, h, b, k, c) . Hence the total is at most

$$(N+1)^{13} e^{-x_*N/100}.$$

For sufficiently large N , $13 \log(N+1) \leq x_*N/200$, giving the claim. $\square$

7 Proof of the Main Theorem

Proof of [theorem 1.1](#). The lower bound follows from [proposition 4.1](#), since $p > r \geq 4$ implies odd characteristic.

For the upper bound, monotonicity allows us to take $\delta = 1/10$. The union bound gives

$$\mathbb{P}[d_{\min}(G_3) \leq L_{1/10}] \leq \sum_{w=1}^n \mathbb{P}[\mathcal{E}_{3,w}(1/10)].$$

We split the sum by message weight.

For $w = 1, 2, 3, 4$, [proposition 5.3](#) gives

$$\mathbb{P}[\mathcal{E}_{3,2}(1/10)] = O_r(N^{2-r-\lceil r/2 \rceil}),$$

while the other three fixed weights have strictly smaller polynomial order.

Choose $x_r > 0$ satisfying [lemma 5.4](#) and [proposition 5.5](#). Weights $w \geq 5$ with $rw/N \leq x_r$ contribute

$$o_r(N^{2-r-\lceil r/2 \rceil})$$

by [proposition 5.5](#). All remaining weights lie in the linear-density range and contribute an exponentially small quantity by [proposition 6.8](#).

Thus

$$\mathbb{P}[d_{\min}(G_3) \leq N/10] = O_r(N^{2-r-\lceil r/2 \rceil}).$$

Together with [proposition 4.1](#), this proves (1.6) for every fixed $0 < \delta \leq 1/10$.

All constants and sufficiently-large- N thresholds in the upper estimates are field-independent. The only characteristic restriction in that argument occurs for weight-one messages. The lower bound is also field-uniform, completing the proof. $\square$

Corollary 7.1 (Weight-two dominance). *Under the hypotheses of [theorem 1.1](#),*

$$\mathbb{P}[\mathcal{E}_{3,2}(\delta)] = \Theta_{r,\delta}(N^{2-r-\lceil r/2 \rceil}),$$

whereas

$$\sum_{\substack{1 \leq w \leq n \\ w \neq 2}} \mathbb{P}[\mathcal{E}_{3,w}(\delta)] = o_{r,\delta}(N^{2-r-\lceil r/2 \rceil}).$$

Proof. The construction in [proposition 4.1](#) uses only weight-two messages, and [proposition 5.3](#) gives the matching upper bound. The second claim follows from monotonicity in δ , the fixed-weight comparison in [section 5](#), and [propositions 5.5](#) and [6.8](#). $\square$

For even repetition factors, the same sharp tail holds under a weaker characteristic assumption, although the present estimates then need not isolate weight two as the sole leading message weight.

Corollary 7.2 (Even repetition factors). *Fix an even $r \geq 4$ and $0 < \delta \leq 1/10$. Uniformly over finite fields $\mathbb{F}_q$ with*

$$p = \text{char}(\mathbb{F}_q) > r/2,$$

we have

$$\mathbb{P}[d_{\min}(G_3) \leq \delta N] = \Theta_{r,\delta}\left(N^{2-r-r/2}\right).$$

Proof. Every upper-bound estimate for $w \geq 2$ is field-uniform. For a weight-one message, the first active prefixes are $c, 2c, \dots, rc$. Exactly $\lfloor r/p \rfloor$ of them vanish. Under $p > r/2$, this number is at most one, so the number j of first-stage contributing gaps satisfies $j \geq r - 1$.

The fixed-weight calculation in the proof of [proposition 5.3](#) therefore gives

$$\mathbb{P}[\mathcal{E}_{3,1}(1/10)] = O_r\left(N^{1-\psi(r-1)}\right) = O_r\left(N^{2-r-r/2}\right),$$

where the last identity uses that r is even. The upper-bound assembly is otherwise unchanged.

Finally, $p > r/2 \geq 2$ implies odd characteristic, so [proposition 4.1](#) supplies the matching lower bound. $\square$

The inequality $p > r/2$ is strict. Under this weaker assumption, the displayed weight-one bound has the same polynomial order as the total tail. Accordingly, [corollary 7.1](#) retains the stronger hypothesis $p > r$.

8 Conclusion

We have determined the sharp minimum-distance lower tail of the unscaled RAAA ensemble. For fixed $r \geq 4$ and $0 < \delta \leq 1/10$, the failure probability has order

$$N^{2-r-\lceil r/2 \rceil},$$

uniformly over fields of characteristic greater than r . Thus, on the common proved threshold range, adding a third accumulator gives a larger improvement in the failure exponent than random scaling in RAA. It also preserves fixed-field operation and an encoder with no coordinatewise field multiplications. The dominant weight-two witnesses explain the gain through two successive rare cancellation arrangements.

For even r , [corollary 7.2](#) relaxes the characteristic requirement to $p > r/2$. The key observation is that at most one weight-one active prefix can then vanish; losing one contributing gap still leaves its probability within the claimed tail order.

References

- [1] Louay Bazzi, Mohammad Mahdian, and Daniel A. Spielman. The minimum distance of turbo-like codes. *IEEE Transactions on Information Theory*, 55(1):6–15, January 2009. <https://doi.org/10.1109/TIT.2008.2008114>.
- [2] Dariush Divsalar, Hui Jin, and Robert J. McEliece. Coding theorems for “turbo-like” codes. In *Proceedings of the 36th Annual Allerton Conference on Communication, Control, and Computing*, pages 201–210, 1998.

- [3] Majid Khabbazzian. Sharp minimum-distance lower tails for RAA codes. Manuscript, 2026.
- [4] Jörg Kliewer, Kamil S. Zigangirov, Christian Koller, and Daniel J. Costello, Jr. Coding theorems for repeat multiple accumulate codes. arXiv:0810.3422, 2008. <https://arxiv.org/abs/0810.3422>.