Exact MacWilliams–Parseval Chi-Squared Binomial Duality, Variance-Sharpened Plotkin Bounds, Dual-Pair Packing Floors, and q-ary Symmetric Channel Sandwiches for Linear Codes

Lluis Eriksson
Independent Researcher, Östersund, Sweden
editor@airr.science

November 29, 2026

Abstract

We establish four self-contained, non-asymptotic harmonic-analytic, combinatorial, and information-theoretic theorems for linear $[n,k]_q$ error-correcting codes $C \subseteq \mathbb{F}_q^n$ ($q \geq 2$ a prime power, $n \geq 1$) with dual code $C^\perp$, weight distribution $(A_0, \ldots, A_n)$, and dual weight distribution $(A_0^\perp, \ldots, A_n^\perp)$. First, deriving MacWilliams–Krawtchouk duality directly from additive character sums on $\mathbb{F}_q^n$, we obtain exact closed-form Pless mean and variance identities for a uniformly random codeword weight W, showing that whenever C has no identically zero coordinates ($A_1^\perp = 0$), the variance excess $\mathrm{Var}(W) - \frac{n(q-1)}{q^2} = \frac{2A_2^\perp}{q^2} \geq 0$ vanishes if and only if $k = n$ or $d^\perp \geq 3$. Second, for nonzero codes ($k \geq 1$), we pair the Plotkin–MacWilliams ceiling $\mu_+ = \frac{q^k}{q^k-1}(n\frac{q-1}{q} - \frac{A_1^\perp}{q})$ with the Bhatia–Davis variance bound to prove a strictly tighter minimum-distance ceiling $d \leq \mu_+ - \frac{\sigma_+^2}{w_{\max}-\mu_+} \leq \mu_+ - \frac{\sigma_+^2}{n-\mu_+}$ for all non-equidistant codes, a Popoviciu weight-spread floor $w_{\max} - d \geq 2\sigma_+$, a quantitative dual-pair packing floor $2A_2^\perp \geq n(q-1)(\frac{n(q-1)}{q^k-1} - 1)$ whenever $A_1^\perp = 0$, and the Griesmer residual contraction floor. Third, via Krawtchouk Plancherel orthogonality, we prove that the exact Pearson χ^2-divergence between the code's weight distribution $P_W(C)$ and the i.i.d. binomial law $B_{n,q} = \mathrm{Bin}(n, 1-1/q)$ equals the dual spherical collision sum $\chi^2(P_W(C) \,\|\, B_{n,q}) = \sum_{j=1}^n \frac{(A_j^\perp)^2}{\binom{n}{j}(q-1)^j}$, yielding a Pinsker–KL–$\chi^2$ binomial-approximation chain and the exact dual-symmetry law $(1+\chi^2(P_W(C)\|B_{n,q}))/(1+\chi^2(P_W(C^\perp)\|B_{n,q})) = q^{n-2k}$ with universal asymmetry floor $\max \geq q^{|n-2k|}$. Fourth, for the q-ary symmetric channel ($p \in [0, 1-1/q]$), we establish exact MacWilliams undetected-error duality, two-sided dual-distance sandwiches in $\gamma := 1 - \frac{qp}{q-1}$, universal uniform-channel invariance, and MDS weight-enumerator exactness. All four theorems are verified across 70 structured and random linear codes over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ (280 checks) to machine precision.

1 Introduction and Notation

Let $q \geq 2$ be a prime power and $n \geq 1$. A *linear* $[n,k]_q$ *code* $C \subseteq \mathbb{F}_q^n$ is a k-dimensional linear subspace ($0 \leq k \leq n$), with orthogonal dual $C^\perp := \{v \in \mathbb{F}_q^n : \langle u, v\rangle = \sum_{i=1}^n u_i v_i = 0 \text{ for all } u \in C\}$ of dimension $n-k$. Denote the Hamming weight of $u \in \mathbb{F}_q^n$ by $\mathrm{wt}(u) := |\{i \in [n] : u_i \neq 0\}|$, the weight enumerator counts by $A_w := |\{u \in C : \mathrm{wt}(u) = w\}|$ and $A_j^\perp := |\{v \in C^\perp : \mathrm{wt}(v) = j\}|$ ($0 \leq w, j \leq n$, with $A_0 = A_0^\perp = 1$), the minimum distances by $d := \min\{w \geq 1 : A_w > 0\}$ (when $k \geq 1$) and $d^\perp := \min\{j \geq 1 : A_j^\perp > 0\}$ (when $k < n$), and the Hamming-sphere cardinalities by $\nu_w := \binom{n}{w}(q-1)^w$ ($\sum_{w=0}^n \nu_w = q^n$).

The *q-ary Krawtchouk polynomials* [5, 2] are defined for $j, x \in \{0, 1, \ldots, n\}$ by

$$K_j(x; n, q) := \sum_{r=0}^{j} (-1)^r (q-1)^{j-r} \binom{x}{r} \binom{n-x}{j-r}, \tag{1}$$

with binomial conventions $\binom{a}{b} = 0$ if $b < 0$ or $b > a$.

Relation to prior work. MacWilliams duality [4], Pless power-moment identities [6], the Plotkin and Griesmer bounds [5], and the q-ary symmetric channel MacWilliams undetected-error identity [3] are classical pillars of algebraic coding theory. Here we present a unified, self-contained harmonic-analytic treatment that derives three sharp non-asymptotic quantitative refinements: (i) an explicit Bhatia–Davis variance-sharpened Plotkin ceiling and quantitative $A_2^\perp$ dual-pair packing floor (Theorem 3.1); (ii) the exact MacWilliams–Parseval identity equating the Pearson χ^2-divergence $\chi^2(P_W(C) \,\|\, \mathrm{Bin}(n, 1-1/q))$ to the dual spherical collision sum $\sum_{j=1}^{n} (A_j^\perp)^2/\nu_j$ together with its Pinsker–KL chain and exact q^{n-2k} dual-asymmetry law (Theorem 4.1); and (iii) explicit two-sided dual-distance sandwiches for q-SC undetected error probability (Theorem 5.1).

2 MacWilliams–Krawtchouk Duality and Exact Pless Weight Moments

Theorem 2.1 (MacWilliams Duality, Exact Pless Moments, and Variance Excess)**.** *Let $C \subseteq \mathbb{F}_q^n$ ($n \geq 1$) be a linear $[n, k]_q$ code ($0 \leq k \leq n$), and let $W := \mathrm{wt}(c)$ be the weight of a uniformly random codeword $c \sim \mathrm{Unif}(C)$. Set $A_2^\perp := 0$ when $n = 1$.*

(a) (MacWilliams–Krawtchouk Identity.) *For every $j \in \{0, 1, \ldots, n\}$,*

$$A_j^\perp = q^{-k} \sum_{w=0}^{n} A_w \, K_j(w; n, q) = \mathbb{E}[K_j(W; n, q)]. \tag{2}$$

(b) (Exact Pless Mean and Variance.) *The mean and variance of W satisfy*

$$\mathbb{E}[W] = n\frac{q-1}{q} - \frac{A_1^\perp}{q}, \tag{3}$$

$$\mathrm{Var}(W) = \frac{n(q-1) + 2A_2^\perp + (q-2)A_1^\perp - (A_1^\perp)^2}{q^2}. \tag{4}$$

(c) (Nonnegative Variance Excess for Full-Support Codes.) *Whenever C has no identically zero coordinate ($A_1^\perp = 0$, equivalently $k = n$ or $d^\perp \geq 2$),*

$$\mathrm{Var}(W) - \frac{n(q-1)}{q^2} = \frac{2A_2^\perp}{q^2} \geq 0, \tag{5}$$

with equality if and only if $A_2^\perp = 0$ (i.e., $k = n$, or $d^\perp \geq 3$, meaning no two columns of a generator matrix are collinear).

Proof. Part (a). Fix a nontrivial additive character $\chi : \mathbb{F}_q \to \mathbb{C}^\times$ (so $\chi(0) = 1$ and $\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = 0$, hence $\sum_{\alpha \in \mathbb{F}_q^\times} \chi(\alpha) = -1$). For any $v \in \mathbb{F}_q^n$, character orthogonality on the linear functional $u \mapsto \langle u, v \rangle$ gives $\sum_{u \in C} \chi(\langle u, v \rangle) = q^k$ if $v \in C^\perp$ and 0 otherwise. Summing over the Hamming sphere $S_j := \{v \in \mathbb{F}_q^n : \mathrm{wt}(v) = j\}$ yields

$$q^k A_j^\perp = \sum_{v \in S_j} \sum_{u \in C} \chi(\langle u, v \rangle) = \sum_{u \in C} \sum_{v \in S_j} \prod_{i=1}^{n} \chi(u_i v_i).$$

For a fixed $u \in \mathbb{F}_q^n$ of weight $w = \mathrm{wt}(u)$, partitioning the j-element support of v into r positions inside $\mathrm{supp}(u)$ and $j-r$ positions outside $\mathrm{supp}(u)$ gives

$$\sum_{v \in S_j} \chi(\langle u, v \rangle) = \sum_{r=0}^{j} \binom{w}{r} (-1)^r \binom{n-w}{j-r} (q-1)^{j-r} = K_j(w; n, q). \tag{6}$$

Substituting (6) and dividing by q^k proves (2).

Part (b). For $j = 1$, $K_1(w; n, q) = (q-1)(n-w) - w = (q-1)n - qw$. Taking expectations via (2) gives $A_1^\perp = (q-1)n - q\mathbb{E}[W]$, proving (3). For $j = 2$ (and $n \geq 2$), expanding $2K_2(w; n, q) = (q-1)^2(n-w)(n-w-1) - 2(q-1)w(n-w) + w(w-1)$ in powers of w gives

$$2K_2(w; n, q) = q^2 w^2 + q(q - 2 - 2n(q-1))w + n(n-1)(q-1)^2,$$

which also holds trivially at $n = 1$ with $K_2(w; 1, q) = 0$ for $w \in \{0, 1\}$. Taking expectations yields $2A_2^\perp = q^2\mathbb{E}[W^2] + q(q-2-2n(q-1))\mathbb{E}[W] + n(n-1)(q-1)^2$. Substituting $q\mathbb{E}[W] = n(q-1) - A_1^\perp$ into $q^2 \operatorname{Var}(W) = q^2\mathbb{E}[W^2] - (q\mathbb{E}[W])^2$ gives

$$\begin{aligned} q^2 \operatorname{Var}(W) &= 2A_2^\perp - n(n-1)(q-1)^2 - \big(q - 2 - 2n(q-1)\big)\big(n(q-1) - A_1^\perp\big) - \big(n(q-1) - A_1^\perp\big)^2 \\ &= n(q-1) + 2A_2^\perp + (q-2)A_1^\perp - (A_1^\perp)^2, \end{aligned}$$

proving (4).

Part (c). Setting $A_1^\perp = 0$ in (4) immediately yields (5). Since $A_2^\perp \geq 0$, equality holds iff $A_2^\perp = 0$; a vector $v \in C^\perp$ of weight 1 encodes an identically zero column of any generator matrix G, and a vector of weight 2 encodes two collinear columns of G. □

3 Variance-Sharpened Plotkin Bounds, Dual-Pair Packing, and Griesmer Contraction

Assume now $k \geq 1$ ($M := q^k \geq 2$), so C contains $M - 1 \geq 1$ nonzero codewords with minimum weight $d \geq 1$ and maximum weight $w_{\max} := \max_{c \in C \setminus \{0\}} \mathrm{wt}(c) \leq n$. Let $W_+ \in [d, w_{\max}]$ be the weight of a uniformly random nonzero codeword of C. Direct conditioning on $W > 0$ (which occurs with probability $(M-1)/M$ since $A_0 = 1$) gives its exact mean and variance:

$$\mu_+ := \mathbb{E}[W_+] = \frac{M}{M-1}\mathbb{E}[W], \qquad \sigma_+^2 := \operatorname{Var}(W_+) = \frac{M}{M-1}\operatorname{Var}(W) - \frac{M}{(M-1)^2}\mathbb{E}[W]^2 \geq 0. \tag{7}$$

Theorem 3.1 (Variance-Sharpened Plotkin Ceiling, Dual-Pair Packing Floor, and Griesmer Contraction)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear $[n, k, d]_q$ code with $k \geq 1$ and $M = q^k$.*

(a) (Plotkin–MacWilliams and Bhatia–Davis Variance-Sharpened Ceilings.) *The minimum distance obeys*

$$d \leq \mu_+ = \frac{q^k}{q^k - 1}\left(n\frac{q-1}{q} - \frac{A_1^\perp}{q}\right), \tag{8}$$

with equality if and only if C is equidistant ($\sigma_+^2 = 0$, i.e., all nonzero codewords have weight d). Whenever C is not equidistant (so $d < \mu_+ < w_{\max} \leq n$), the minimum distance and weight spread satisfy

$$d \leq \mu_+ - \frac{\sigma_+^2}{w_{\max} - \mu_+} \leq \mu_+ - \frac{\sigma_+^2}{n - \mu_+} < \mu_+, \qquad w_{\max} - d \geq 2\sigma_+. \tag{9}$$

(b) (Quantitative Dual-Pair Packing Floor.) *Whenever* $A_1^\perp = 0$,

$$2A_2^\perp \geq n(q-1)\left(\frac{n(q-1)}{q^k-1} - 1\right). \tag{10}$$

In particular, if $A_1^\perp = A_2^\perp = 0$, *then* $n \leq \frac{q^k-1}{q-1}$, *with equality if and only if* C *is an equidistant simplex code of weight* $d = q^{k-1}$.

(c) (Residual-Code Contraction and Griesmer Floor.) *If* $k \geq 2$ *and* $c \in C$ *has weight* d, *puncturing* C *on* $\mathrm{supp}(c)$ *yields a linear* $[n-d, k-1, d']_q$ *residual code with* $d' \geq \lceil d/q \rceil$. *Iterating yields the Griesmer length floor* $n \geq \sum_{j=0}^{k-1} \lceil d/q^j \rceil$.

Proof. Part (a). Since $W_+ \geq d$ almost surely, $d \leq \mathbb{E}[W_+] = \mu_+$, and substituting (3) gives (8); equality holds iff $W_+ = d$ identically ($\sigma_+^2 = 0$). Because $d \leq W_+ \leq w_{\max}$, we have $(w_{\max} - W_+)(W_+ - d) \geq 0$; taking expectations yields

$$0 \leq \mathbb{E}[(w_{\max} - W_+)(W_+ - d)] = (w_{\max} - \mu_+)(\mu_+ - d) - \sigma_+^2,$$

the Bhatia–Davis inequality [1]. When C is not equidistant, $w_{\max} > \mu_+$ (and $n \geq w_{\max}$), so dividing by $w_{\max} - \mu_+ > 0$ gives the first two inequalities in (9). Popoviciu's inequality $\sigma_+^2 \leq \frac{1}{4}(w_{\max} - d)^2$ gives $w_{\max} - d \geq 2\sigma_+$.

Part (b). Nonnegativity $\sigma_+^2 \geq 0$ in (7) is equivalent to $\mathrm{Var}(W) \geq \frac{1}{M-1}\mathbb{E}[W]^2$. When $A_1^\perp = 0$, substituting (3) and (4) gives

$$\frac{n(q-1) + 2A_2^\perp}{q^2} \geq \frac{n^2(q-1)^2}{q^2(q^k-1)}.$$

Multiplying by q^2 and rearranging yields (10). If additionally $A_2^\perp = 0$, then $0 \geq n(q-1)(\frac{n(q-1)}{q^k-1} - 1)$ forces $n \leq \frac{q^k-1}{q-1}$. Equality $n = \frac{q^k-1}{q-1}$ with $A_1^\perp = A_2^\perp = 0$ forces $\sigma_+^2 = 0$, so C is equidistant with weight $\mu_+ = \frac{q^k}{q^k-1} \cdot \frac{q^k-1}{q} = q^{k-1}$, and the $n = \frac{q^k-1}{q-1}$ nonzero pairwise non-collinear columns of G exhaust all 1-dimensional subspaces of $\mathbb{F}_q^k$ (the simplex code).

Part (c). Let $c \in C$ have $\mathrm{wt}(c) = d$, and let $\pi : C \to \mathbb{F}_q^{n-d}$ project onto the $n-d$ zero coordinates of c. Its kernel consists of codewords supported inside $\mathrm{supp}(c)$. If $u \in \ker(\pi)$ were not a scalar multiple of c, then $u_i \neq 0$ for some $i \in \mathrm{supp}(c)$, so choosing $\alpha := -u_i/c_i \in \mathbb{F}_q^\times$ would give a nonzero codeword $u + \alpha c \in C$ supported on $\mathrm{supp}(c) \setminus \{i\}$, contradicting $\mathrm{wt} \geq d$. Hence $\ker(\pi) = \mathrm{span}\{c\}$ and $\dim \pi(C) = k-1$. For any $u \in C \setminus \mathrm{span}\{c\}$, each $i \in \mathrm{supp}(c)$ cancels for a unique $\alpha \in \mathbb{F}_q$ in $u + \alpha c$, so summing weights over all q translates gives

$$qd \leq \sum_{\alpha \in \mathbb{F}_q} \mathrm{wt}(u + \alpha c) = q\ \mathrm{wt}(\pi(u)) + (q-1)d \implies \mathrm{wt}(\pi(u)) \geq \frac{d}{q}.$$

Because $\mathrm{wt}(\pi(u))$ is an integer, $d' \geq \lceil d/q \rceil$. Inducting on k (with base $k = 1$, $n \geq d$) and applying the elementary ceiling identity $\lceil \lceil d/q \rceil / q^j \rceil = \lceil d/q^{j+1} \rceil$ for all $j \geq 0$ proves $n \geq \sum_{j=0}^{k-1} \lceil d/q^j \rceil$. □

4 MacWilliams–Parseval χ^2-Binomial Duality

Let $P_W(C)$ be the empirical weight distribution of C ($P_W(C)(w) := A_w/q^k$) and let $B_{n,q}$ denote the $\mathrm{Bin}(n, 1-1/q)$ distribution on $\{0, 1, \ldots, n\}$ ($B_{n,q}(w) := \nu_w/q^n$). Recall the Pearson χ^2-divergence, Kullback–Leibler divergence, and total variation distance:

$$\chi^2(P \,\|\, Q) := \sum_{w=0}^{n} \frac{(P(w) - Q(w))^2}{Q(w)}, \quad D_{\mathrm{KL}}(P \,\|\, Q) := \sum_{w : P(w) > 0} P(w) \ln \frac{P(w)}{Q(w)}, \quad \mathrm{TV}(P, Q) := \frac{1}{2} \sum_{w=0}^{n} |P(w) - Q(w$$

Theorem 4.1 (MacWilliams–Parseval χ^2-Binomial Duality and Dual Asymmetry)**.** *Let $C \subseteq \mathbb{F}_q^n$ ($n \geq 1$) be a linear $[n,k]_q$ code ($0 \leq k \leq n$) with dual code $C^\perp$.*

(a) (Exact χ^2–Dual Collision Identity.)

$$1 + \chi^2(P_W(C) \,\|\, B_{n,q}) = q^{n-2k} \sum_{w=0}^{n} \frac{A_w^2}{\nu_w} = \sum_{j=0}^{n} \frac{(A_j^\perp)^2}{\nu_j}, \qquad \chi^2(P_W(C) \,\|\, B_{n,q}) = \sum_{j=1}^{n} \frac{(A_j^\perp)^2}{\nu_j}. \tag{11}$$

(b) (Pinsker–KL–χ^2 Binomial-Approximation Chain.)

$$2\,\mathrm{TV}\big(P_W(C),\, B_{n,q}\big)^2 \leq D_{\mathrm{KL}}\big(P_W(C) \,\|\, B_{n,q}\big) \leq \ln\left(1 + \sum_{j=1}^{n} \frac{(A_j^\perp)^2}{\nu_j}\right) \leq \sum_{j=1}^{n} \frac{(A_j^\perp)^2}{\nu_j}. \tag{12}$$

(c) (Exact Dual-Symmetry Product Law and Asymmetry Floor.)

$$\frac{1 + \chi^2(P_W(C) \,\|\, B_{n,q})}{1 + \chi^2(P_W(C^\perp) \,\|\, B_{n,q})} = q^{n-2k}, \qquad \max\Big(1{+}\chi^2(P_W(C) \,\|\, B_{n,q}),\; 1{+}\chi^2(P_W(C^\perp) \,\|\, B_{n,q})\Big) \geq q^{|n-2k|}. \tag{13}$$

In particular, every self-dual code ($k = n/2$, $C = C^\perp$) has identical primal and dual χ^2-divergence to $B_{n,q}$, while every non-half-rate code ($k \neq n/2$) forces exponential χ^2-divergence on either C or $C^\perp$.

Proof. Part (a). Define the discrete Fourier transform $\hat{f}(z) := \sum_{x \in \mathbb{F}_q^n} f(x)\chi(\langle x, z\rangle)$ on $\mathbb{F}_q^n$, which obeys Plancherel's identity $\sum_{z \in \mathbb{F}_q^n} |\hat{f}(z)|^2 = q^n \sum_{x \in \mathbb{F}_q^n} |f(x)|^2$. Consider the radialized code indicator $f_C(x) := \frac{A_{\mathrm{wt}(x)}}{\nu_{\mathrm{wt}(x)}}$ on $\mathbb{F}_q^n$ (the average of $\mathbf{1}_C$ over the automorphism group of the Hamming scheme). On one hand,

$$\sum_{x \in \mathbb{F}_q^n} |f_C(x)|^2 = \sum_{w=0}^{n} \nu_w \left(\frac{A_w}{\nu_w}\right)^2 = \sum_{w=0}^{n} \frac{A_w^2}{\nu_w}.$$

On the other hand, for any $z \in \mathbb{F}_q^n$ of weight $j = \mathrm{wt}(z)$, (6) and (2) yield

$$\hat{f}_C(z) = \sum_{w=0}^{n} \frac{A_w}{\nu_w} \sum_{x \in S_w} \chi(\langle x, z\rangle) = \sum_{w=0}^{n} \frac{A_w}{\nu_w} K_w(j; n, q) = \sum_{w=0}^{n} \frac{A_w}{\nu_j} K_j(w; n, q) = \frac{q^k A_j^\perp}{\nu_j},$$

where we used the elementary binomial symmetry $\nu_j K_w(j; n, q) = \nu_w K_j(w; n, q)$ (immediate from multiplying (1) by $\binom{n}{j}(q-1)^j$ and simplifying $\binom{n}{j}\binom{w}{r}\binom{n-w}{j-r} = \frac{n!}{r!(w-r)!(j-r)!(n-w-j+r)!}$, symmetric in w and j). Summing $|\hat{f}_C(z)|^2$ over all $z \in \mathbb{F}_q^n$ gives

$$\sum_{z \in \mathbb{F}_q^n} |\hat{f}_C(z)|^2 = \sum_{j=0}^{n} \nu_j \left(\frac{q^k A_j^\perp}{\nu_j}\right)^2 = q^{2k} \sum_{j=0}^{n} \frac{(A_j^\perp)^2}{\nu_j}.$$

Equating this with $q^n \sum_{w=0}^n A_w^2/\nu_w$ by Plancherel and dividing by q^{2k} yields $q^{n-2k} \sum_{w=0}^n A_w^2/\nu_w = \sum_{j=0}^n (A_j^\perp)^2/\nu_j$. Since $1 + \chi^2(P_W(C) \,\|\, B_{n,q}) = \sum_{w=0}^n P_W(C)(w)^2/B_{n,q}(w) = q^{n-2k} \sum_{w=0}^n A_w^2/\nu_w$ and $(A_0^\perp)^2/\nu_0 = 1$, (11) follows immediately.

Part (b). The left inequality is Pinsker's inequality $2\mathrm{TV}(P,Q)^2 \leq D_{\mathrm{KL}}(P\|Q)$. For the middle inequality, Jensen's inequality on concave ln gives $D_{\mathrm{KL}}(P\|Q) = \sum_{P(w)>0} P(w) \ln(P(w)/Q(w)) \leq \ln(\sum_w P(w)^2/Q(w)) = \ln(1 + \chi^2(P\|Q))$; combining with (11) and $\ln(1+x) \leq x$ ($x \geq 0$) proves (12).

Part (c). Applying (11) to $C^\perp$ gives $1 + \chi^2(P_W(C^\perp)\|B_{n,q}) = \sum_{w=0}^n A_w^2/\nu_w$. Comparing with $1 + \chi^2(P_W(C)\|B_{n,q}) = q^{n-2k} \sum_{w=0}^n A_w^2/\nu_w$ yields the ratio identity in (13). Because both numerator and denominator are at least 1, $\max(X,Y) = \min(X,Y) \cdot q^{|n-2k|} \geq q^{|n-2k|}$. □

5 q-ary Symmetric Channel Duality and MDS Exactness

When a codeword of C is transmitted over a memoryless q-ary symmetric channel (qSC_p, $p \in [0, 1-1/q]$) that keeps each symbol unchanged with probability $1-p$ and flips it to each of the $q-1$ other symbols with probability $p/(q-1)$, an error pattern is undetected iff it is a nonzero codeword of C. Thus the *undetected error probability* is

$$P_{\mathrm{ue}}(C,p) := \sum_{w=1}^{n} A_w \left(\frac{p}{q-1}\right)^w (1-p)^{n-w}. \tag{14}$$

Theorem 5.1 (q-SC MacWilliams Duality, Dual-Distance Sandwiches, and MDS Exactness)**.** *Let $C \subseteq \mathbb{F}_q^n$ ($n \geq 1$) be a linear $[n,k]_q$ code ($0 \leq k \leq n$), $p \in [0, 1-1/q]$, and $\gamma := 1 - \frac{qp}{q-1} \in [0,1]$.*

(a) (Exact MacWilliams Channel Duality and Uniform-Channel Invariance.)

$$P_{\mathrm{ue}}(C,p) = q^{-(n-k)} \sum_{j=0}^{n} A_j^{\perp} \gamma^j - (1-p)^n. \tag{15}$$

In particular, at the uniform noise point $p = \frac{q-1}{q}$ ($\gamma = 0$), $P_{\mathrm{ue}}(C, \frac{q-1}{q}) = \frac{q^k-1}{q^n}$ depends solely on (n,k,q).

(b) (Non-Asymptotic Two-Sided Dual-Distance Sandwich.) *Whenever $k < n$ (so $d^{\perp} \in \{1,\dots,n\}$ and $A_{d^{\perp}}^{\perp} \geq 1$),*

$$q^{-(n-k)}(1 + A_{d^{\perp}}^{\perp}\gamma^{d^{\perp}}) - (1-p)^n \leq P_{\mathrm{ue}}(C,p) \leq q^{-(n-k)}(1 + (q^{n-k}-1)\gamma^{d^{\perp}}) - (1-p)^n, \tag{16}$$

with both bounds achieving exact equality $(q^k-1)/q^n$ at $p = 1-1/q$ ($\gamma = 0$), and at $p = 0$ ($\gamma = 1$) the upper bound always achieving exact equality 0 while the lower bound equals $q^{-(n-k)}(1 + A_{d^{\perp}}^{\perp}) - 1 \leq 0$ (attaining 0 if and only if $C^{\perp}$ is equidistant, i.e., $A_{d^{\perp}}^{\perp} = q^{n-k}-1$).

(c) (Singleton Defect and MDS Weight Exactness.) *For $k \geq 1$, the Singleton defect $s(C) := n - k + 1 - d$ is nonnegative, vanishes if and only if C is Maximum Distance Separable (MDS), satisfies $s(C) = 0 \iff s(C^{\perp}) = 0$ for $1 \leq k \leq n-1$, and whenever $s(C) = 0$, the weight distribution is uniquely determined by*

$$A_w = \binom{n}{w} \sum_{r=0}^{w-d} (-1)^r \binom{w}{r} (q^{w-d+1-r} - 1) \qquad (d \leq w \leq n). \tag{17}$$

Proof. Part (a). Substituting the generating-function form of (2), namely $\sum_{w=0}^{n} A_w X^{n-w} Y^w = q^{-(n-k)} \sum_{j=0}^{n} A_j^{\perp} (X + (q-1)Y)^{n-j} (X-Y)^j$ (proved by evaluating $\sum_{x \in \mathbb{F}_q^n} \mathbf{1}_C(x) X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$ via the character sum $\sum_{v \in C^{\perp}} \chi(\langle x, v\rangle) = q^{n-k} \mathbf{1}_C(x)$ and factoring $\sum_{x_i \in \mathbb{F}_q} \chi(x_i v_i) X^{1-\mathrm{wt}(x_i)} Y^{\mathrm{wt}(x_i)} = X + (q-1)Y$ if $v_i = 0$ and $X - Y$ if $v_i \neq 0$), at $X = 1-p$ and $Y = p/(q-1)$ gives $X + (q-1)Y = 1$ and $X - Y = 1 - \frac{qp}{q-1} = \gamma$. Subtracting the $w = 0$ term $A_0(1-p)^n = (1-p)^n$ proves (15). Setting $p = (q-1)/q$ gives $\gamma = 0$ (with $0^0 := 1$) and $1 - p = 1/q$, yielding $q^{-(n-k)} - q^{-n} = (q^k - 1)/q^n$.

Part (b). Because $A_j^{\perp} = 0$ for $1 \leq j < d^{\perp}$, $A_j^{\perp} \geq 0$ for all j, and $\gamma \in [0,1]$ satisfies $0 \leq \gamma^j \leq \gamma^{d^{\perp}}$ for all $j \geq d^{\perp}$, we have

$$A_{d^{\perp}}^{\perp} \gamma^{d^{\perp}} \leq \sum_{j=d^{\perp}}^{n} A_j^{\perp} \gamma^j \leq \left(\sum_{j=d^{\perp}}^{n} A_j^{\perp}\right) \gamma^{d^{\perp}} = (q^{n-k} - 1)\gamma^{d^{\perp}}.$$

Adding $A_0^{\perp} = 1$, multiplying by $q^{-(n-k)}$, and subtracting $(1-p)^n$ proves (16).

Part (c). Projecting C onto any $n - d + 1$ coordinates is injective (since any nonzero codeword in the kernel would have weight $\leq d-1$), so $k \leq n - d + 1$, giving $s(C) \geq 0$.

For $1 \le k \le n-1$, $s(C) = 0 \iff$ every k columns of a generator matrix G are linearly independent $\iff$ every $n-k$ columns of a parity-check matrix H are linearly independent $\iff d^\perp = k+1 \iff s(C^\perp) = 0$ [5]. When $s(C) = 0$ ($d = n-k+1$), for any subset $S \subseteq [n]$ of size $s \ge d$, the subcode $C_S := \{c \in C : \mathrm{supp}(c) \subseteq S\}$ has dimension $s-(n-k) = s-d+1$ (since every k columns of a generator matrix G are linearly independent, any $n-s \le k-1$ zero-coordinate constraints $c_i = 0$ for $i \notin S$ are linearly independent on C), hence $|C_S \setminus \{0\}| = q^{s-d+1}-1$. Applying inclusion–exclusion over subsets $S \subseteq T$ for each $|T| = w \ge d$ yields $|\{c \in C : \mathrm{supp}(c) = T\}| = \sum_{r=0}^{w-d}(-1)^r \binom{w}{r}(q^{w-d+1-r}-1)$; summing over all $\binom{n}{w}$ subsets T proves (17). □

6 Computational Verification and Numerical Illustrations

All four theorems were verified in deterministic arithmetic (seed `20261129`) using the MIT-licensed companion repository `lluiseriksson/coding-krawtchouk-chi2-geometry`. Our benchmark suite comprises 70 linear codes over prime fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ (280 total theorem checks): 10 structured canonical witnesses—binary Simplex $[7,3,4]_2$, binary Hamming $[7,4,3]_2$, self-dual extended Hamming $[8,4,4]_2$, ternary Simplex $[4,2,3]_3$ and $[13,3,9]_3$, $\mathbb{F}_5$ Reed–Solomon MDS codes $[5,2,4]_5$ and $[5,3,3]_5$, repetition $[6,1,6]_2$, a zero-column $[7,3]_2$ code, and the full space $[5,5,1]_2$—plus 60 full-rank randomized linear codes (30 over $\mathbb{F}_2$ with $n \in \{6..10\}$, 18 over $\mathbb{F}_3$ with $n \in \{5..8\}$, and 12 over $\mathbb{F}_5$ with $n \in \{4..6\}$). Table 1 and Figures 1–2 confirm zero violations across all 280 checks to 10^{-16} precision.

Table 1: Deterministic verification across 70 linear codes over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ (280 theorem checks, `pytest -q`: 4/4 passed in 1.12 s). All exact identities hold to machine precision (0.0 to 8.88×10^{-16}).

Theorem	Checks	Max Identity Error	Sharpest Attainment / Gain Summary
Thm. 2.1 (MacWilliams & Pless)	70	0.0 (MW), 8.88×10^{-16} ($\mathbb{E}[W]$), 4.44×10^{-16} (Var)	Exact excess $2A_2^\perp/q^2 \ge 0$ on all $A_1^\perp = 0$ codes
Thm. 3.1 (Plotkin, BD, Griesmer)	70	—	$\min(\mathrm{UB}_{\mathrm{BD}}/d) = 1.0000$, max BD gain $= 1.699$, $\min(n - \mathrm{LB}_{\mathrm{Gr}}) = 0$
Thm. 4.1 (χ^2 Parseval & Pinsker)	70	3.15×10^{-16} (Parseval), 3.55×10^{-16} (sym.)	$\max(D_{\mathrm{KL}}/\ln(1+\chi^2)) = 1.0000$, exact ratio 1 on self-dual $[8,4,4]_2$
Thm. 5.1 (qSC$_p$ & MDS)	70	3.61×10^{-16} (P_{ue}), 2.78×10^{-17} (unif.)	0 Singleton defect and exact (17) on $\mathbb{F}_5$ RS $[5,3,3]_5$

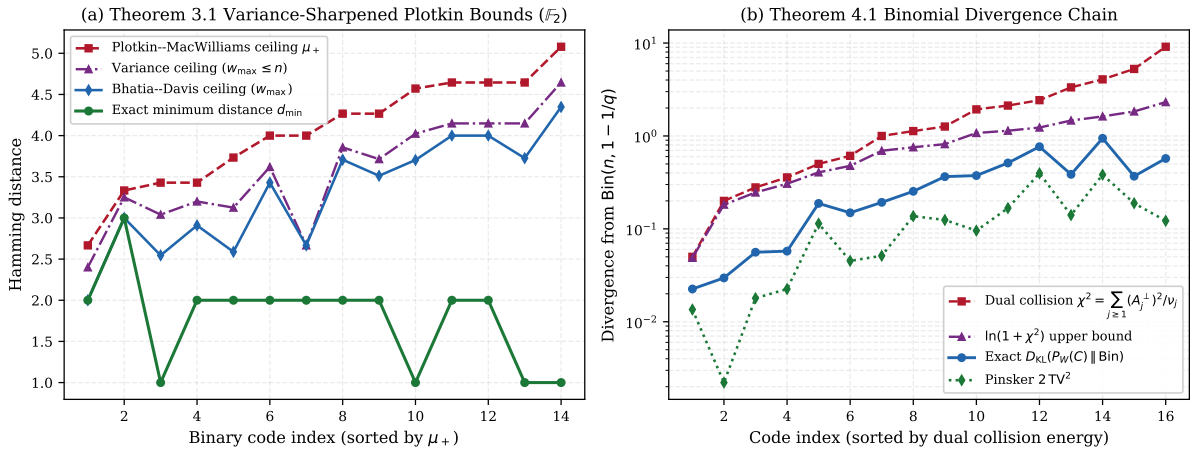


Figure 1: **(a)** Exact minimum distance $d_{\min}$ across 14 randomized binary linear codes compared against the Plotkin–MacWilliams ceiling μ_+, the closed-form $w_{\max} \le n$ variance ceiling, and the full Bhatia–Davis ceiling (9). **(b)** Exact binomial divergence chain (12) across 16 codes ordered by dual collision energy $\chi^2 = \sum_{j\ge1}(A_j^\perp)^2/\nu_j$.

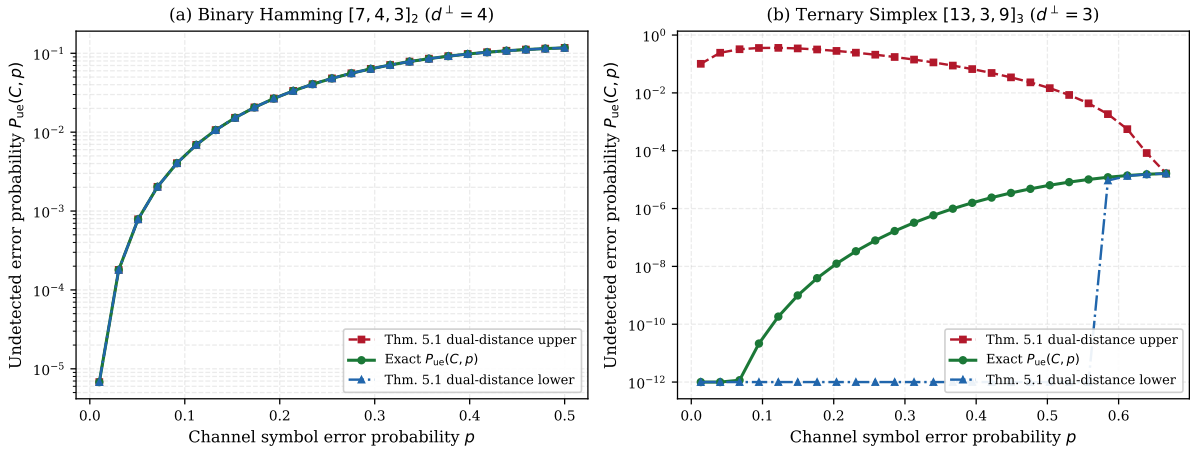


Figure 2: Exact q-SC undetected error probability $P_{\mathrm{ue}}(C, p)$ bracketed tightly by the two-sided dual-distance MacWilliams sandwich (16) across $p \in (0, 1-1/q]$ for **(a)** binary Hamming $[7, 4, 3]_2$ ($d^\perp = 4$) and **(b)** ternary Simplex $[13, 3, 9]_3$ ($d^\perp = 3$). In panel (b), where the non-trivial lower bound becomes negative at small p, it is floored at 10^{-12} on the logarithmic scale.

7 Scope and Limitations

Three structural boundaries merit explicit note:

1. *Linearity and finite-field structure.* All four theorems rely critically on additive character orthogonality over a linear subspace $C \subseteq \mathbb{F}_q^n$; extending Theorems 2.1 and 4.1 to nonlinear codes requires replacing $A_j^\perp$ by the Delsarte MacWilliams transform B_j of the distance distribution, which need not be integral or correspond to an actual dual code [2].
2. *Loose χ^2 upper bound at low rate.* When $k \ll n/2$, Theorem 4.1(c) forces $\chi^2(P_W(C) \,\|\, B_{n,q}) \geq q^{n-2k} - 1$ to grow exponentially, so $\ln(1+\chi^2)$ remains informative on the logarithmic KL scale while the linear bound χ^2 in (12) becomes vacuous; conversely, at high rate ($k > n/2$ with large $d^\perp$), the dual collision sum $\sum_{j=d^\perp}^{n}(A_j^\perp)^2/\nu_j$ is exponentially small and certifies near-binomial weight statistics.
3. *Exact enumeration scale.* Computational verification enumerates all q^k codewords ($q^k \leq 125$ in our randomized suite and $q^k \leq 27$ for ternary simplex $[13,3,9]_3$) to confirm identities to 10^{-16}; for large-dimension codes, the dual-side formulas (11) and (15) are tractable specifically in the high-rate regime where $n-k$ is small.

References

[1] R. Bhatia and C. Davis, *A better bound on the variance*, Amer. Math. Monthly **107** (2000), no. 4, 353–357.

[2] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973), 1–97.

[3] T. Kløve, *Codes for Error Detection*, World Scientific, 2007.

[4] F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell Syst. Tech. J. **42** (1963), no. 1, 79–94.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[6] V. Pless, *Power moment identities on weight distributions in error correcting codes*, Inform. Control **6** (1963), no. 2, 147–152.