hexagon:2611.00246v1

SECOND MOMENTS OF PATTERN COUNTS IN DUAL MELAS CODEWORDS

DAVID NIEDBALA GIRAUDIN

Abstract. Let α be a primitive element of $\mathbb{F}_{2^k}$ and, for $c \in \mathbb{F}_{2^k}^*$, let $S_c = (\mathrm{Tr}(\alpha^i + c\alpha^{-i}))_{0 \le i \le 2^k-2}$ be the corresponding codeword of the dual Melas code. Let $X_{k,c}(w)$ be the number of occurrences of a uniformly random pattern $w \in \mathbb{F}_2^k$ in S_c. Sac Himelfarb and Schwartz conjectured that X_{k,c_k} converges to the Poisson law $\mathcal{P}(1)$ for every choice of $c_k \in \mathbb{F}_{2^k}^*$; they proved that the second factorial moment satisfies $\limsup M_2 \le 2$, and $M_2 \to 1$ for almost every sequence (c_k). We prove that $|M_2^{(k,c)} - 1| \le 2^{-(1/22+o(1))k}$ uniformly in $c \in \mathbb{F}_{2^k}^*$ and in the primitive element α. Thus the second factorial moment converges to 1 for every sequence (c_k). The proof expresses M_2 through a norm form of the quadratic extension $\mathbb{F}_2(x)/\mathbb{F}_2(x + x^{-1})$, which turns it into a bilinear Kloosterman sum of full length, and bounds the latter in characteristic two. We also show that the counts $N_w(S_c)$, as functions of (w, c), are the fibre sizes of a family of quadratic maps, and deduce that for almost every sequence of patterns w_k the first two factorial moments of $c \mapsto N_{w_k}(S_c)$ converge to 1, as they would under the Poisson law conjectured by Sac Himelfarb and Schwartz for fixed patterns.

1. Statement

Let $k \ge 3$, $F = \mathbb{F}_{2^k}$, $n = 2^k - 1$, $\chi(z) = (-1)^{\mathrm{Tr}(z)}$ where $\mathrm{Tr} = \mathrm{Tr}_{F/\mathbb{F}_2}$, and let $\alpha \in F$ be primitive. For $c \in F^*$ put $S_c(i) = \mathrm{Tr}(\alpha^i + c\alpha^{-i})$, $i \in \mathbb{Z}/n$. As in [5], for $w \in \mathbb{F}_2^k$ let N_w be the number of $i \in \mathbb{Z}/n$ with $(S_c(i), \dots, S_c(i+k-1)) = w$ (indices mod n), let $X_{k,c}(w) = N_w$ on $\mathbb{F}_2^k$ with the uniform measure, and

$$M_2^{(k,c)} = \mathbb{E}\big[X_{k,c}(X_{k,c} - 1)\big] = 2^{-k} \sum_{w \in \mathbb{F}_2^k} N_w(N_w - 1).$$

For $N \ge 2$ let τ_N denote the maximal number of monic divisors of a nonzero polynomial of degree $\le N$ in $\mathbb{F}_2[s]$.

Theorem 1. *For all $k \ge 3$, all primitive $\alpha \in \mathbb{F}_{2^k}$ and all $c \in \mathbb{F}_{2^k}^*$,*

$$\big|M_2^{(k,c)} - 1\big| \;\le\; 2^{-k}\Big(1 + k^3\, C_k\, 2^{21k/22}\Big), \qquad C_k = 8 + 2\,(12\,\tau_{3k})^{1/4},$$

and $\tau_N \le (N+1)^{2\sqrt{N}}\, 2^{2N/\log_2 N} = 2^{o(N)}$. In particular $\max_{c \in F^*} |M_2^{(k,c)} - 1| \le 2^{-(1/22+o(1))k}$, and $M_2^{(k,c_k)} \to 1$ for every sequence $c_k \in \mathbb{F}_{2^k}^*$.

Conjecture 35 of [5] asserts convergence in distribution to $\mathcal{P}(1)$, and [5] proposes to prove it through the convergence of all factorial moments; Theorem 1 establishes the second of these steps uniformly in c. Compare [5, Theorem 37], which gives $\limsup_k M_2^{(k,c_k)} \le 2$ for every sequence and $M_2^{(k,c_k)} \to 1$ for almost every sequence. Since $M_1^{(k,c)} = 1 - 2^{-k}$, Theorem 1 also gives $\mathrm{Var}(X_{k,c}) \to 1$ uniformly in c. The exponent $1/22$ is not optimised.

Throughout, $P_\ell \subset \mathbb{F}_2[x]$ (or $\mathbb{F}_2[s]$) denotes the set of polynomials of degree $< \ell$ (including 0).

Date: 9 November 2026.
ORCID 0009-0009-1526-1178.

2. Zero windows and the norm $h(\alpha)h(\alpha^{-1})$

Let m_α, $m_{\alpha^{-1}}$ be the minimal polynomials of α, α^{-1} over $\mathbb{F}_2$. They are distinct: otherwise $\alpha^{-1} = \alpha^{2^j}$ with $0 \le j < k$, so $n \mid 2^j + 1 \le 2^{k-1} + 1 < n$. Put $M = m_\alpha m_{\alpha^{-1}}$ (degree $2k$), $R = \mathbb{F}_2[x]/(M)$, and identify $R \cong F \times F$ by $h \mapsto (h(\alpha), h(\alpha^{-1}))$. For $h \in R$ put $\mathrm{Nm}(h) = h(\alpha)h(\alpha^{-1}) \in F$. Every $h \in P_k \setminus \{0\}$ satisfies $h(\alpha) \ne 0 \ne h(\alpha^{-1})$, since $\deg h < k$.

Lemma 2 (cf. [5, Theorems 12–13])**.** *There is $\kappa \in F^*$, depending only on α, with the following property. For $P, Q \in F^*$ let $s_i = \mathrm{Tr}(P\alpha^i + Q\alpha^{-i})$ and let $Z(P,Q)$ be the number of $i \in \mathbb{Z}/n$ with $s_i = s_{i+1} = \cdots = s_{i+k-1} = 0$. Then*

$$Z(P,Q) = \rho(\kappa PQ), \qquad \rho(v) = \#\{h \in P_k \setminus \{0\} : \ \mathrm{Nm}(h) = v\}.$$

Proof. Let $\tau : R \to \mathbb{F}_2$ send z to the coefficient of x^{2k-1} of its representative of degree $< 2k$. The pairing $(z, w) \mapsto \tau(zw)$ is nondegenerate: on the basis $x^0, \dots, x^{2k-1}$ its Gram matrix $(\tau(x^{a+b}))$ vanishes for $a + b < 2k - 1$ and equals 1 for $a + b = 2k - 1$. Hence every $\mathbb{F}_2$-linear form on R is $\tau(\varphi\,\cdot)$ for a unique $\varphi \in R$. Every linear form on $F \times F$ is $(z_1, z_2) \mapsto \mathrm{Tr}(Az_1 + Bz_2)$; write $\tau(z) = \mathrm{Tr}(A_0 z(\alpha) + B_0 z(\alpha^{-1}))$. If $A_0 = 0$, then $\tau(zw) = 0$ for $z = (1, 0)$ and all w, contradicting nondegeneracy; so $A_0 \ne 0$, and likewise $B_0 \ne 0$. Put $\kappa = (A_0 B_0)^{-1}$.

Let $\Lambda(z) = \mathrm{Tr}(Pz(\alpha) + Qz(\alpha^{-1}))$, so $s_i = \Lambda(x^i)$, and let $\varphi \in R$ with $\Lambda = \tau(\varphi\,\cdot)$. Comparing the two expressions of Λ gives $P = A_0\varphi(\alpha)$ and $Q = B_0\varphi(\alpha^{-1})$, so $\varphi \in R^*$ and $\mathrm{Nm}(\varphi) = \kappa PQ$. Now $s_{i+j} = \tau(x^i\varphi \cdot x^j)$. The annihilator $\mathcal{A} = \{w \in R : \tau(wx^j) = 0,\ 0 \le j < k\}$ of the k-dimensional space P_k has dimension k, and it contains P_k, because for $\deg w < k$ and $j < k$ the product wx^j has degree $\le 2k - 2$. Hence $\mathcal{A} = P_k$, and the window at i is zero if and only if $h_i := x^i\varphi \in P_k$.

Since x has order n in R^* (its image is (α, α^{-1})), the elements h_i, $i \in \mathbb{Z}/n$, are distinct, and $\mathrm{Nm}(h_i) = \mathrm{Nm}(\varphi)$. Conversely, let $h \in P_k \setminus \{0\}$ with $\mathrm{Nm}(h) = \mathrm{Nm}(\varphi)$. Then $h(\alpha)/\varphi(\alpha) = \alpha^i$ for a unique $i \in \mathbb{Z}/n$, and $h(\alpha^{-1}) = \mathrm{Nm}(\varphi)/h(\alpha) = \varphi(\alpha^{-1})\alpha^{-i}$, so $h = h_i$ in R. Thus $Z(P,Q) = \rho(\mathrm{Nm}\,\varphi) = \rho(\kappa PQ)$. □

Proposition 3. *With κ as in Lemma 2, for every $c \in F^*$,*

$$M_2^{(k,c)} = 1 - 2^{-k} + 2^{-k}\,W(c), \qquad W(c) = \sum_{h \in P_k \setminus \{0\}} \chi\Big(\frac{\kappa c}{\mathrm{Nm}(h)}\Big).$$

Proof. $2^k M_2^{(k,c)}$ is the number of ordered pairs $i \ne i'$ in $\mathbb{Z}/n$ with equal windows. Writing $i' = i + d$, $d \not\equiv 0$, the windows at i and $i + d$ coincide if and only if the sequence $S_c(i) + S_c(i+d) = \mathrm{Tr}\left((1 + \alpha^d)\alpha^i + c(1 + \alpha^{-d})\alpha^{-i}\right)$ has a zero window at i. By Lemma 2, with $t = \alpha^d \ne 1$ and $(1 + t)(1 + t^{-1}) = t + t^{-1}$,

$$2^k M_2^{(k,c)} = \sum_{t \in F^* \setminus \{1\}} \rho\big(\kappa c\,(t + t^{-1})\big).$$

For $v \in F^*$, the equation $t + t^{-1} = v$, i.e. $(t/v)^2 + (t/v) = v^{-2}$, has $1 + \chi(v^{-1})$ solutions t, all different from 0 and 1; and $t + t^{-1} \ne 0$ for $t \ne 1$. Hence $2^k M_2^{(k,c)} = \sum_{v \in F^*}(1 + \chi(v^{-1}))\rho(\kappa cv)$. The first part equals $\sum_{u \in F^*} \rho(u) = 2^k - 1$. In the second part put $u = \kappa cv = \mathrm{Nm}(h)$, so that $v^{-1} = \kappa c/\mathrm{Nm}(h)$; it equals $W(c)$. □

Remark 4. Proposition 3 gives another expression for the quantity in formula (8) of [5].

3. The norm form of $\mathbb{F}_2(x)/\mathbb{F}_2(s)$, $s = x + x^{-1}$

Let $A = \mathbb{F}_2[s]$ and $O = \mathbb{F}_2[x, x^{-1}] = A[x]$, where $x^2 + sx + 1 = 0$. The involution $x \mapsto x^{-1}$ fixes s, so for $h \in \mathbb{F}_2[x]$ there is a unique $N(h) \in A$ with $h(x)h(x^{-1}) = N(h)(x + x^{-1})$. Put $\beta = \alpha + \alpha^{-1}$; then $\mathrm{Nm}(h) = N(h)(\beta)$.

The field $\mathbb{F}_2(\beta)$ is all of F: otherwise $k = 2j$, $\beta \in \mathbb{F}_{2^j}$, and α, α^{-1} are the two roots of $X^2 + \beta X + 1$ over $\mathbb{F}_{2^j}$, so $\alpha^{2^j} = \alpha^{-1}$ and $n \mid 2^j + 1$, which is impossible. Let $m_\beta \in A$ be the minimal polynomial of β (irreducible, of degree k). Then $y \mapsto y(\beta)$ is a bijection from $P_k \subset A$ onto F, and from P_ℓ onto an $\mathbb{F}_2$-subspace U_ℓ of dimension ℓ, for $\ell \le k$.

Define $\chi_0 : A \to \{0, \pm 1\}$ by $\chi_0(D) = 0$ if $s \mid D$, and $\chi_0(D) = (-1)^{D_1}$ if $D = 1 + D_1 s + \dots$. It is completely multiplicative.

Proposition 5. *For $P \in A \setminus \{0\}$ with $\deg P < k$,*

$$r(P) := \#\{h \in P_k : \ N(h) = P\} = (k - \deg P) \sum_{D \mid P} \chi_0(D).$$

Moreover $N(h) \neq 0$ and $\deg N(h) < k$ for every $h \in P_k \setminus \{0\}$.

Proof. Write $h = x^a h_0$ with $h_0(0) = 1$ and $e = \deg h_0$. Then $N(h) = N(h_0)$, and the Laurent polynomial $h_0(x)h_0(x^{-1})$ has extreme terms $x^{\pm e}$, so $N(h_0)$ has degree exactly $e \le \deg h < k$.

O is a localisation of $\mathbb{F}_2[x]$, hence a principal ideal domain, integral over A; it is the integral closure of A in $\mathbb{F}_2(x)$, and N is the norm of the quadratic extension $\mathbb{F}_2(x)/\mathbb{F}_2(s)$. The units of O are the monomials x^j, so each nonzero ideal of O has a unique generator $h_0 \in \mathbb{F}_2[x]$ with $h_0(0) = 1$, and its norm is $N(h_0)A$. Hence $\#\{h_0 : h_0(0) = 1, \ N(h_0) = P\}$ is the number $a(P)$ of ideals of O of norm PA. Since $O = A[x]$, the decomposition of a prime Q of A in O follows that of $X^2 + \bar{s}X + 1$ over A/Q. For $Q = s$ this is $(X + 1)^2$ (ramified). For $Q \neq s$ put $\theta = \bar{s} \neq 0$; the polynomial is separable, and it has a root if and only if $Y^2 + Y = \theta^{-2}$ does, i.e. iff $\mathrm{Tr}_{(A/Q)/\mathbb{F}_2}(\theta^{-1}) = 0$. This trace is the sum of the inverses of the roots of $Q = 1 + q_1 s + \dots$, namely q_1. Thus Q splits iff $\chi_0(Q) = 1$ and is inert iff $\chi_0(Q) = -1$, and the standard count gives $a = 1 * \chi_0$. Finally $h = x^a h_0$ with $\deg h < k$ allows $a \in \{0, \dots, k - 1 - e\}$, which is $k - \deg P$ choices. □

Corollary 6. *Put $\lambda = \kappa c$ and $\bar{y} = y(\beta)^{-1}$ for $y \in A \setminus \{0\}$ of degree $< k$. Then*

$$W(c) = \sum_{\substack{D, E \in A \setminus \{0\} \\ \deg D + \deg E \le k-1}} (k - \deg D - \deg E)\, \chi_0(D)\, \chi(\lambda \bar{D} \bar{E}).$$

Proof. By Propositions 3 and 5, $W(c) = \sum_P r(P) \chi(\lambda / P(\beta))$, and $r(P) = (k - \deg P) \sum_{DE = P} \chi_0(D)$. □

4. Estimates in characteristic two

Lemma 7 (Weil [6])**.** *For $a, b \in F^*$, $\left| \sum_{z \in F^*} \chi(az + b/z) \right| \le 2 \cdot 2^{k/2}$; and $\sum_{z \in F^*} \chi(b/z) = -1$.*

Lemma 8. *Let $0 \le \ell \le k - 1$ and $\mu \in F^*$. Then*

$$\Big| \sum_{\deg y = \ell} \chi(\mu \bar{y}) \Big| \le 2^{k/2+3}, \qquad \Big| \sum_{\deg y = \ell} \chi_0(y) \chi(\mu \bar{y}) \Big| \le 2^{k/2+3}.$$

Proof. For $\ell' \le k$ and $\eta \in F$, write $\mathbf{1}_{U_{\ell'}}(z) = 2^{\ell' - k} \sum_{\xi \in U_{\ell'}^\perp} \chi(\xi z)$, where $U^\perp$ is the annihilator for $(z, \xi) \mapsto \mathrm{Tr}(z\xi)$, of size $2^{k - \ell'}$. Then $\sum_{z \in U_{\ell'} \setminus \{0\}} \chi(\mu z^{-1} + \eta z) = 2^{\ell' - k} \sum_\xi \sum_{z \in F^*} \chi(\mu z^{-1} + (\eta + \xi) z)$, which by Lemma 7 has absolute value $\le 2 \cdot 2^{k/2} + 1$. The polynomials of exact degree ℓ are $P_{\ell+1} \setminus P_\ell$, giving the first bound with $\eta = 0$. For the second, $\chi_0(y) = \frac{1}{2}\big((-1)^{y_1} - (-1)^{y_0 + y_1}\big)$ for all y, and $y \mapsto y_1$, $y \mapsto y_0 + y_1$ are linear forms on $P_k \cong F$, i.e. of the shape $z \mapsto \mathrm{Tr}(\eta z)$; this gives four sums of the previous type with weight $\frac{1}{2}$. □

Lemma 9 (divisor bound)**.** *For $N \ge 2$, $\tau_N \le (N + 1)^{2\sqrt{N}} 2^{2N / \log_2 N}$.*

Proof. Let $f = \prod Q^{e_Q}$, $\deg f \le N$, and $L = \lceil (\log_2 N)/2 \rceil \ge 1$. There are at most $2^L \le 2\sqrt{N}$ primes of degree $< L$, each contributing a factor $e_Q + 1 \le N+1$. Primes of degree $\ge L$ contribute $\prod (e_Q+1) \le 2^{\sum e_Q} \le 2^{N/L} \le 2^{2N/\log_2 N}$. □

The next lemma is Bagshaw's Lemma 5.3 [1], whose proof uses no hypothesis on q and no exponential sums; we give it with explicit constants for $q = 2$ and irreducible modulus.

Lemma 10. *Let $1 \le \ell \le k$, $a \in F^*$, and $I(a) = \#\{(y_1, y_2) \in (P_\ell \setminus \{0\})^2 : \bar{y}_1 + \bar{y}_2 = a\}$. Then $I(a) \le \tau_{3k}\big(1 + 2^{(3\ell-k)/2}\big)$.*

Proof. Let $\tilde{a} \in P_k$ with $\tilde{a}(\beta) = a$, and $k_0 = \lceil (k+\ell)/2 \rceil - 1 \in [1, k-1]$. The linear map sending $u \in P_{k_0+1}$ to the coefficients of $s^{k-k_0}, \dots, s^{k-1}$ of $\tilde{a}u \bmod m_\beta$ goes from dimension k_0+1 to dimension k_0, so there is $u \ne 0$, $\deg u \le k_0$, with $v := \tilde{a}u \bmod m_\beta$ of degree $\le k - k_0 - 1$. Also $v \ne 0$, as $m_\beta \nmid \tilde{a}$ and $m_\beta \nmid u$. For a solution, $u(y_1+y_2) \equiv v y_1 y_2 \pmod{m_\beta}$, so $G := u(y_1+y_2) + v y_1 y_2 = t\, m_\beta$ with $t \in A$, and $\deg G \le \max(k_0 + \ell - 1,\ k - k_0 - 1 + 2\ell - 2)$. With $(k+\ell)/2 - 1 \le k_0 \le (k+\ell-1)/2$, this gives $\deg t \le (3\ell - k - 3)/2$, hence at most $1 + 2^{(3\ell-k)/2}$ possible t (the term 1 accounts for $t = 0$). For fixed t,

$$(v y_1 + u)(v y_2 + u) = u^2 + v t\, m_\beta =: N_t,$$

and $N_t \ne 0$, since otherwise $m_\beta \mid u$. The divisor $v y_1 + u$ of N_t determines y_1 and then y_2, and $\deg N_t \le 3k$. So each t accounts for at most τ_{3k} solutions. □

Lemma 11 (energy)**.** *For $1 \le \ell \le k$ and $Y \subseteq P_\ell \setminus \{0\}$, the additive energy $E(Y) = \#\{(y_1, \dots, y_4) \in Y^4 : \bar{y}_1 + \bar{y}_2 = \bar{y}_3 + \bar{y}_4\}$ satisfies $E(Y) \le 2^{2\ell}\big(1 + \tau_{3k}(1 + 2^{(3\ell-k)/2})\big)$.*

Proof. $E(Y) \le E(P_\ell \setminus \{0\}) = \sum_{a \in F} I(a)^2$ with $I(0) = 2^\ell - 1$ (in characteristic two $\bar{y}_1 = \bar{y}_2$ iff $y_1 = y_2$), and $\sum_{a \ne 0} I(a)^2 \le \max_{a \ne 0} I(a) \sum_a I(a) \le \max_{a \ne 0} I(a)\, 2^{2\ell}$. Apply Lemma 10. □

Lemma 12 (bilinear bound)**.** *Let $X, Y \subseteq P_k \setminus \{0\}$, $|\alpha_x| \le 1$, and $\lambda \in F^*$. Then $S = \sum_{x \in X} \sum_{y \in Y} \alpha_x \chi(\lambda \bar{x} \bar{y})$ satisfies $|S|^4 \le |X|^3\, 2^k\, E(Y)$.*

Proof. By Cauchy–Schwarz, $|S|^2 \le |X| \sum_{x \in X} |\sum_y \chi(\lambda \bar{x} \bar{y})|^2 = |X| \sum_{z \in F} \nu(z) \sum_{x \in X} \chi(\lambda \bar{x} z)$, where $\nu(z) = \#\{(y_1, y_2) \in Y^2 : \bar{y}_1 + \bar{y}_2 = z\}$. By Cauchy–Schwarz again and orthogonality, $|S|^2 \le |X| \big(\sum_z \nu(z)^2\big)^{1/2} \big(\sum_{z \in F} |\sum_{x \in X} \chi(\lambda \bar{x} z)|^2\big)^{1/2} = |X|\, E(Y)^{1/2} (2^k |X|)^{1/2}$. □

5. Proof of Theorem 1

By Corollary 6, $W(c) = \sum_{d+e \le k-1} (k-d-e) S_{d,e}$ with $S_{d,e} = \sum_{\deg D = d} \sum_{\deg E = e} \chi_0(D) \chi(\lambda \bar{D} \bar{E})$, $d, e \ge 0$. There are at most $k(k+1)/2$ pairs and the weights are $\le k$, so $|W(c)| \le k^3 \max_{d,e} |S_{d,e}|$. Each $S_{d,e}$ satisfies:

(i) $|S_{d,e}| \le 2^{d+e}$;
(ii) $|S_{d,e}| \le 2^d \cdot 2^{k/2+3}$ and $|S_{d,e}| \le 2^e \cdot 2^{k/2+3}$ (fix one variable, Lemma 8);
(iii) $|S_{d,e}|^4 \le 2^{3d+k} E(Y_e) \le 12\, \tau_{3k}\, 2^{3d+2e+k} \max\big(1, 2^{(3e+3-k)/2}\big)$ (Lemmas 12 and 11, with Y_e the polynomials of degree e, $Y_e \subseteq P_{e+1}$, and $1 + \tau(1+z) \le 3\tau \max(1, z)$).

Let $\eta = 1/22$. If $\min(d, e) \le (1/2 - \eta)k$, (ii) gives $|S_{d,e}| \le 8 \cdot 2^{(1-\eta)k}$. If $d + e \le (1-\eta)k$, (i) gives $|S_{d,e}| \le 2^{(1-\eta)k}$. Otherwise $\min(d, e) > (1/2 - \eta)k$ and $d + e \le k - 1$, so $\max(d, e) < (1/2 + \eta)k$, and (iii) gives

$$\frac{|S_{d,e}|^4}{2^{4(d+e)}} \le 12 \tau_{3k} \max\big(2^{k-d-2e},\, 2^{(k+3)/2-d-e/2}\big) \le 12 \tau_{3k}\, 2^{3/2}\, 2^{(-1/4+3\eta/2)k},$$

because $k - d - 2e < (-1/2 + 3\eta)k$ and $(k+3)/2 - d - e/2 < (-1/4 + 3\eta/2)k + 3/2$. As $-\frac{1}{16} + \frac{3\eta}{8} = -\frac{1}{22}$ and $d + e < k$, we get $|S_{d,e}| \le (12\tau_{3k})^{1/4} 2^{3/8}\, 2^{21k/22}$. Hence $|W(c)| \le k^3 C_k 2^{21k/22}$, and Proposition 3 gives the theorem, with Lemma 9 for τ_{3k}. □

6. Fixed pattern, random codeword

For $w \in \mathbb{F}_2^k$ let X_w be the random variable $c \mapsto N_w(S_c)$ on F^* with the uniform measure. It is conjectured in [5, §V-D] that $X_{w_k} \to \mathcal{P}(1)$ for almost every $(w_k) \in \prod_k \mathbb{F}_2^k$ (product of uniform measures); this fails for $w_k = 0^k$.

Let $\psi : F \to F$ be the $\mathbb{F}_2$-linear bijection $g(\alpha) \mapsto g(\alpha^{-1})$ ($g \in P_k$), and for $\delta \in F$ put $\Phi_\delta(y) = y\psi(y) + \delta y$.

Proposition 13 (cf. [5, Theorem 13])**.** *There is an $\mathbb{F}_2$-linear bijection $w \mapsto \delta_w$ from $\mathbb{F}_2^k$ onto F, with $\delta_0 = 0$, such that for all w and all $c \in F^*$*

$$N_w(S_c) = \#\{y \in F : \ \Phi_{\delta_w}(y) = \kappa c\}.$$

Proof. Keep the notation of the proof of Lemma 2, with $P = 1$, $Q = c$. Let $A_w = \{z \in R : \tau(zx^j) = w_j,\ 0 \le j < k\}$. By nondegeneracy A_w is a coset $z_w + P_k$ of the annihilator P_k, and z_w may be chosen $\mathbb{F}_2$-linear in w. The window of S_c at i equals w iff $x^i\varphi \in A_w$. As in Lemma 2, the units $h \in A_w$ with $\mathrm{Nm}(h) = \mathrm{Nm}(\varphi) = \kappa c$ are exactly the elements $x^i\varphi \in A_w$, one for each such i. Write $(z_w(\alpha), z_w(\alpha^{-1})) = (p, q)$; for $g \in P_k$ with $g(\alpha) = y$, $\mathrm{Nm}(z_w + g) = (p+y)(q+\psi(y)) = y'(\psi(y') + \delta_w)$ with $y' = y + p$ and $\delta_w = \psi(p) + q$, which does not depend on the choice of z_w in its coset. Every solution of $y'(\psi(y') + \delta_w) = \kappa c \neq 0$ gives a unit. The map $w \mapsto \delta_w$ is linear, and $\delta_w = 0$ iff (p, q) lies in the image of P_k, i.e. iff $A_w = P_k$, i.e. iff $w = 0$. Hence it is bijective. □

Thus the matrix $(N_w(S_c))_{w,c}$ is the matrix of fibre sizes $\#\Phi_\delta^{-1}(\lambda)$, $\delta \in F$, $\lambda \in F^*$: its rows (c fixed) are the objects of Conjecture 35 of [5], its columns (w fixed) those of [5, §V-D].

Lemma 14. *Let $\Sigma_0 = \#\{(a, b) \in (F^*)^2 : a\psi(b) = b\psi(a)\}$. Then $\Sigma_0 \le 6k^2 2^k$.*

Proof. With $a = g(\alpha)$, $b = h(\alpha)$, $g, h \in P_k \setminus \{0\}$, the condition reads $B(g, h)(\beta) = 0$ with $B(g, h) = N(g + h) + N(g) + N(h) \in A$ of degree $< k$; hence $B(g, h) = 0$, i.e. $g(x)h(x^{-1}) = h(x)g(x^{-1})$. Write $g = x^a d g_1$, $h = x^b d h_1$ with d, g_1, h_1 of constant term 1 and $\gcd(g_1, h_1) = 1$. Cancelling $d(x)d(x^{-1})$ and writing $f^*(x) = x^{\deg f} f(x^{-1})$, the condition becomes $x^{2(a-b)+\deg g_1 - \deg h_1} g_1 h_1^* = g_1^* h_1$; comparing constant terms, $2(a - b) = \deg h_1 - \deg g_1$ and $g_1 h_1^* = g_1^* h_1$, whence $g_1 \mid g_1^*$, $g_1^* = g_1$ and $h_1^* = h_1$. There are at most $2^{e/2}$ palindromes of degree e with constant term 1, at most 2^δ choices of d of degree δ, and at most k choices of (a, b) once the degrees are fixed. Hence $\Sigma_0 \le k \sum_{\delta<k} 2^\delta \big(\sum_{e<k-\delta} 2^{e/2}\big)^2 \le k \sum_{\delta<k} 2^k (\sqrt{2} - 1)^{-2} \le 6k^2 2^k$. □

Remark 15. Σ_0 is the quantity computed exactly in [5, Lemma 7(1)]: $\Sigma_0 = (3k - 3)2^{k-2} + 1$ for k odd and $(3k - 4)2^{k-2} + 1$ for k even. Lemma 14 is a self-contained weaker bound; with the exact value the constant $120k^3$ in Theorem 16(ii) becomes $8k^{3/2}$. The use of the spaces E_ρ below parallels the proof of [5, Theorem 38].

Theorem 16. *(i) For every $w \neq 0$, $\mathbb{E}[X_w] = (2^k - 2)/(2^k - 1)$.*

(ii) For every $k \ge 3$ and every $\varepsilon \in (2^{2-k}, 1)$,

$$\frac{1}{2^k} \#\Big\{ w \in \mathbb{F}_2^k : \ \big|\mathbb{E}[X_w(X_w - 1)] - 1\big| > \varepsilon \Big\} \ \le \ \frac{120\, k^3\, 2^{-k/2}}{(\varepsilon - 2^{2-k})^2}.$$

Consequently, for almost every sequence $(w_k) \in \prod_k \mathbb{F}_2^k$, $\mathbb{E}[X_{w_k}] \to 1$ and $\mathbb{E}[X_{w_k}(X_{w_k} - 1)] \to 1$.

Proof. Write $\delta = \delta_w$ and $\lambda = \kappa c$, which is uniform on F^*. (i) $\sum_{\lambda \neq 0} \#\Phi_\delta^{-1}(\lambda) = 2^k - \#\Phi_\delta^{-1}(0)$ and $\Phi_\delta^{-1}(0) = \{0, \psi^{-1}(\delta)\}$, of size 2 for $\delta \neq 0$.

(ii) Let $S(\delta) = \#\{(y, y') : y \neq y',\ \Phi_\delta(y) = \Phi_\delta(y')\}$; then $n\,\mathbb{E}[X_w(X_w - 1)] = S(\delta) - 2$ for $w \neq 0$. For $a \neq 0$, $\Phi_\delta(y + a) + \Phi_\delta(y) = \ell_a(y) + a\psi(a) + \delta a$ with $\ell_a(y) = y\psi(a) + a\psi(y)$, which

is $\mathbb{F}_2$-linear in y. Let $d_a = \dim \ker \ell_a$ and $C_a = \{\delta : \delta a \in a\psi(a) + \operatorname{Im} \ell_a\}$, an affine subspace of codimension d_a with direction $D_a = a^{-1} \operatorname{Im} \ell_a$. Then $S(\delta) = \sum_{a \neq 0} 2^{d_a} \mathbf{1}_{C_a}(\delta)$, whose mean over $\delta \in F$ is $m = \sum_{a \neq 0} 1 = n$.

Put $\rho(a) = \psi(a)/a$, $E_\rho = \{y : \psi(y) = \rho y\}$ and $E_\rho^* = \{\theta : \psi^*(\theta) = \rho\theta\}$, where ψ^* is the adjoint of ψ for $(u, v) \mapsto \operatorname{Tr}(uv)$. Then $\ker \ell_a = E_{\rho(a)}$. The adjoint of ℓ_a is $z \mapsto z\psi(a) + \psi^*(za)$, so $\theta \in D_a^\perp$ iff $\ell_a^*(\theta/a) = 0$ iff $\psi^*(\theta) = \rho(a)\theta$: $D_a^\perp = E_{\rho(a)}^*$. If $\rho(a) \neq \rho(b)$ then $D_a^\perp \cap D_b^\perp = 0$, so $D_a + D_b = F$ and $|C_a \cap C_b| = 2^{k - d_a - d_b}$. Therefore

$$\sum_{\delta \in F} (S(\delta) - m)^2 = \sum_{a,b \neq 0} 2^{d_a + d_b} \big(|C_a \cap C_b| - 2^{k - d_a - d_b} \big) \leq \sum_{\rho(a) = \rho(b)} 2^{2d_a} 2^{k - d_a} = \sum_v (2^{d_v} - 1)^2 \, 2^{k + d_v},$$

where v runs over the values of ρ and $\{a : \rho(a) = v\} = E_v \setminus \{0\}$ has $2^{d_v} - 1$ elements. Here $\sum_v (2^{d_v} - 1)^2 = \Sigma_0$ and $2^{d_v} \leq 2(2^{d_v} - 1) \leq 2\Sigma_0^{1/2}$, so by Lemma 14 the sum is $\leq 2^{k+1} \Sigma_0^{3/2} \leq 30\, k^3 2^{5k/2}$. Since $|\mathbb{E}[X_w(X_w - 1)] - 1| \leq |S(\delta_w) - m|/n + 2/n$ for every w, $2/n \leq 2^{2-k}$ and $n^2 \geq 2^{2k-2}$, Chebyshev's inequality gives (ii). The bound is summable in k, and so is $\Pr(w_k = 0) = 2^{-k}$; the last statement follows from the Borel–Cantelli lemma (applied with $\varepsilon = 1/j$, $j = 1, 2, \dots$) and (i). □

7. Numerical verification

The ancillary script `VERIF_MELAS_M2.py` (pure Python) checks:

- Proposition 3 against direct pattern counting, for every $c \in F^*$ and $4 \leq k \leq 10$ (a single constant κ for all c);
- Proposition 5, for every P with $\deg P < k$, $3 \leq k \leq 9$;
- the worst case $\max_c |M_2^{(k,c)} - 1|$, for $k \leq 16$;
- Proposition 13 (equality of the multisets of columns $(N_w(S_c))_c$ and of fibre-size vectors of Φ_δ), for $k \leq 8$;
- Lemma 14, for $3 \leq k \leq 8$.

Corollary 6 was checked separately for $4 \leq k \leq 10$, on about fifty values of c for each k. Observed values of $\max_c |M_2^{(k,c)} - 1|$ (with the primitive polynomials listed in the script) are:

k	8	10	12	14	16	20
$\max_c \lvert M_2 - 1\rvert$	0.2969	0.2168	0.1245	0.0710	0.0439	0.0156

and $\max_c |W(c)|/2^{k/2} < k$ for $4 \leq k \leq 20$, consistent with square-root cancellation, which is far stronger than Theorem 1.

For the columns, the computed values of Σ_0 agree with [5, Lemma 7(1)], and the variance of $\mathbb{E}[X_w(X_w - 1)]$ over $w \neq 0$ is 0.158, 0.104, 0.063, 0.036 for $k = 6, 8, 10, 12$, while $\max_w \mathbb{E}[X_w(X_w - 1)] \approx (k + 1)/2$ in this range, so that the restriction to almost every w in Theorem 16 cannot be dropped.

Status. Theorems 1 and 16: proved. Section 7: verified by computation. The full Conjecture 35 of [5] (all factorial moments, for every sequence c_k) remains open.

Acknowledgements. The conjectures, the correspondence between windows and polynomials [5, Theorems 12–13] and the count of [5, Lemma 7] are due to Sac Himelfarb and Schwartz. The energy bound follows Bagshaw [1, 2] and Bourgain–Garaev [4]. Computations and drafting were assisted by Claude (Anthropic).

References

[1] C. Bagshaw, Bilinear forms with Kloosterman and Gauss sums in function fields, Finite Fields Appl. 94 (2024), 102356; arXiv:2304.05014.
[2] C. Bagshaw, Bilinear Kloosterman sums in function fields and the distribution of irreducible polynomials, Canad. J. Math. (2024); arXiv:2401.10399.
[3] C. Bagshaw and I. E. Shparlinski, Energy bounds, bilinear forms and their applications in function fields, Finite Fields Appl. 82 (2022), 102048.
[4] J. Bourgain and M. Z. Garaev, Kloosterman sums in residue rings, Acta Arith. 164 (2014), 43–64.
[5] G. Sac Himelfarb and M. Schwartz, On the b-symbol weight distribution of dual Melas codes and a Poisson randomness postulate, arXiv:2610.38017.
[6] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. USA 34 (1948), 204–207.

Meaux, France