Uniform product expansion of Reed–Solomon codes on coprime-degree subfield grids

Shi Jie Samuel Tan (University of Maryland and IBM) Guanyu Zhu (IBM)

November 2026

Abstract

Product expansion is the local robustness property of tuples of linear codes that underlies the recent constructions of good quantum locally testable codes and of private PCPs. We study it for Reed–Solomon codes whose evaluation sets are arbitrary equal-size subsets of three subfields $\mathbb{F}_{P^{m_i}}$ of pairwise coprime extension degrees, with constants depending only on P and the rate gap: this is the local hypothesis of the companion construction of quantum LDPC codes with near-linear distance and $N^{1-\varepsilon}$ addressable transversal CCZ gates. The new ingredient is a family of Frobenius automorphisms that act as the identity on one of the subfields and as $x \mapsto x^P$ on the others. They give, first, an elementary and field-independent bound of $(P+1)ab$ on the number of grid points of an irreducible curve of bidegree (a, b); substituted for the Corvaja–Zannier input of Bafna–Vyas, it yields a complete proof of two-direction product expansion with constant $\nu^2/(8(P+5)^2)$ for every rate gap ν and every prime power P. Second, they give a derivative-isolation lemma that replaces the only step of the inner-generation argument of Chen–Huang–Liu–Tang that uses the norm-one structure of their evaluation sets. With it, that argument yields product expansion in every fixed number of directions on coprime-degree subfield grids, with explicit constants ($\rho = \frac{1}{3}(\nu/K_3(P))^3$, $K_3(P) = 144(33P+97)$, for three directions), modulo a single imported statement, the cylinder-gluing theorem of Chen–Huang–Liu–Tang in three directions. Every other step is proved here; we prove the gluing theorem for two directions and for hyperplane cylinders in any dimension, and reduce its three-dimensional case to the configuration of complete lines in three directions, which is therefore the sole external dependency. The three new algebraic lemmas are formalized and checked in Lean 4/Mathlib.

Contents

1 Introduction **2**
- 1.1 Product expansion and the hypothesis . . . 3
- 1.2 Related work . . . 3
- 1.3 Main results . . . 4
- 1.4 Techniques . . . 5
- 1.5 Organization . . . 5

2 The point-count lemma **6**

3 Two directions **7**

4 All directions: transporting the inner-generation framework **9**
- 4.1 The framework . . . 9
- 4.2 Where the norm-one structure enters, and its replacement . . . 9

4.3 The inner-generation theorem on coprime-degree grids . . . 11
4.4 The imported statements, with exact hypotheses . . . 11
4.5 The transported induction . . . 15
4.6 From inner generation to product expansion; proof of Theorem 1.4 . . . 17
4.7 What is imported . . . 19

5 Discussion **19**
5.1 Application to the companion construction . . . 19
5.2 Scope and open problems . . . 19

A Machine-checked components **20**
A.1 Dictionary . . . 20
A.2 The main declarations . . . 21
A.3 Verification record . . . 22
A.4 Scope . . . 23

1 Introduction

Let $C_1, \dots, C_r$ be linear codes over a field F with coordinate sets $S_1, \dots, S_r$, and consider arrays on the grid $\prod_i S_i$ that are sums of *line codewords*: an array A_i all of whose direction-i lines are codewords of C_i, summed over i. Such an array may have many different decompositions, and some of them may involve far more nonzero lines than its weight suggests. The tuple is *product expanding* if every such array admits a decomposition whose total weighted number of nonzero lines is bounded by a constant times its weight. For two codes this is the robust (or agreement) testability of the tensor code $C_1 \otimes C_2$ under the row–column test, introduced by Polishchuk and Spielman [12]; for more codes it is strictly stronger than robust testability and coincides with the coboundary expansion of the tensor complex in its top nontrivial degree [9, 10]. In this form it has become the local ingredient of the recent constructions of asymptotically good quantum locally testable codes [6, 10, 4, 7, 1] and of private PCPs [2]: in each case a global expansion property is obtained from a product-expansion hypothesis on the local codes, with constants that must not depend on the code length.

Which Reed–Solomon tuples are product expanding, uniformly in the length, is a question of arithmetic geometry about the evaluation sets. Bafna and Vyas [2] prove two-direction product expansion for Reed–Solomon codes on multiplicative subgroups of pairwise coprime orders of a prime field, and conjecture the higher-dimensional statement; Chen, Huang, Liu and Tang [4] and Gay and Jeronimo [7] prove it in every fixed number of directions for Reed–Solomon codes on norm-one subgroups $\mu_{q_i+1} \subset \mathbb{F}_{q_i^2}$ of distinct sizes. The companion construction [8] of quantum LDPC codes with near-linear distance and $N^{1-\varepsilon}$ individually addressable transversal CCZ gates needs a third family: Reed–Solomon codes of equal length on arbitrary subsets of three subfields $\mathbb{F}_{P^{m_1}}, \mathbb{F}_{P^{m_2}}, \mathbb{F}_{P^{m_3}}$ of pairwise coprime extension degrees, with all directional subtuples, all dual choices and all diagonal rescalings, over every finite scalar field containing the subfields, and with a constant depending only on P and the rate gap. There the coprime-degree subfield structure is what makes a large space of global characters restrict to low-degree polynomials in every direction; it is stated as Assumption 2.1 of [8] and reproduced below as Hypothesis PE.

This paper proves Hypothesis PE. For two directions the proof is complete and elementary. For three directions it follows the inner-generation strategy of [4], whose one set-dependent step we replace, and imports exactly one statement from that work, the cylinder-gluing theorem in three

directions; we state the imported theorem with its hypotheses, prove it in the cases that elementary methods reach, and isolate precisely what remains.

1.1 Product expansion and the hypothesis

Let F be a finite field. For codes $C_i \subseteq F^{S_i}$ ($i \in J$, J a finite index set) put $G = \prod_{i\in J} S_i$ and let $Q_i \subseteq F^G$ be the space of arrays all of whose direction-i lines (fix all coordinates but the ith) lie in C_i. For $A_i \in Q_i$ let $|A_i|_i$ be the number of direction-i lines on which A_i is nonzero. The tuple $(C_i)_{i\in J}$ is *ρ-product expanding* if every $A \in \sum_i Q_i$ admits a decomposition $A = \sum_i A_i$, $A_i \in Q_i$, with

$$\sum_{i\in J} |S_i|\,|A_i|_i \;\le\; \rho^{-1}|A|. \tag{1}$$

This is definition (2) of [8]; it coincides with [9, Def. 1], [6, Def. 5.12], [4, Def. 5.1] and [7, Def. 1.1.1] ("weighted" form). Note $\sum_i Q_i = (\bigotimes_i C_i^{\perp})^{\perp}$. Coordinate permutations and nonzero diagonal rescalings in each direction preserve (1) (they biject points and lines).

For $S \subseteq F$ and $1 \le k \le |S|$, $\mathrm{RS}(S,k) = \{(f(c))_{c\in S} : \deg f < k\}$. Its dual is $\mathrm{diag}(v)\mathrm{RS}(S, |S|-k)$ with $v(a) = \prod_{b\in S\setminus\{a\}}(a-b)^{-1}$; thus the dual of a diagonally rescaled RS code of dimension k is a diagonally rescaled RS code of dimension $|S|-k$.

Hypothesis PE (Uniform subfield product expansion; [8, Assumption 2.1])**.** Fix a power P of two and $0 < \nu < 1/2$. There is $\rho = \rho(P,\nu) > 0$ with the following property. Let m_1, m_2, m_3 be pairwise coprime positive integers, let $S_i \subseteq \mathbb{F}_{P^{m_i}}$ have the same size n, and let F be any finite field containing these subfields. For arbitrary invertible diagonal matrices L_i set $C_i = L_i\mathrm{RS}(S_i, k_i)$ with $\nu n \le k_i \le (1-\nu)n$. Every nonempty directional subtuple, with each member independently chosen as C_i or $C_i^{\perp}$, is ρ-product expanding. The constant is independent of n, the extension degrees, the sets, the multipliers and the containing scalar field.

By the duality remark, every code that can occur in the hypothesis is a diagonally rescaled $\mathrm{RS}(S_i,k)$ with $\nu n \le k \le (1-\nu)n$, i.e. with *redundancy* $h = n-k \ge \nu n$ *and* dimension $\ge \nu n$. So the hypothesis is equivalent to:

> *every nonempty subtuple of* $(L_i\mathrm{RS}(S_i,k_i))_{i\le 3}$ *with* $\nu n \le k_i \le (1-\nu)n$ *is* $\rho(P,\nu)$*-product expanding over every finite field* $F \supseteq \mathbb{F}_{P^{m_1m_2m_3}}$.

One-element subtuples are the RS distance bound ($|A| \ge (n-k+1)|A|_i \ge \nu n|A|_i$). The content is in the pairs and in the full triple.

1.2 Related work

Bafna–Vyas [2, Thm. 4.11] prove the two-direction case for RS codes on multiplicative subgroups of *pairwise coprime orders* of $\mathbb{F}_q^{\times}$, q prime, with both rates bounded away from one, by the Polishchuk–Spielman argument plus a bivariate divisibility lemma whose only arithmetic input is an upper bound on the number of grid points on an irreducible curve, obtained from the Corvaja–Zannier gcd estimate. They conjecture the higher-dimensional statement [2, Conj. 4.2]. Chen–Huang–Liu–Tang [4, Thm. 5.4] and Gay–Jeronimo [7, Thm. 11.1.4] prove uniform product expansion in *every* fixed number of directions, including all subtuples, duals and rescalings, for RS codes on norm-one sets $\mu_{q_i+1} \subset \mathbb{F}_{q_i^2}$, $q_i = 2^{a_i}$ (CHLT: $a_i = 2(A+i)$; GJ: pairwise distinct a_i of bounded ratio). Both proofs use the norm-one structure through the single identity $z^{q_i} = z^{-1}$, which lets a Frobenius power act on the grid as a low-degree monomial map. None of these statements covers Hypothesis PE (arbitrary equal-size subsets of coprime-degree subfields).

1.3 Main results

Throughout, p is a prime, $P = p^f$, $K_m := \mathbb{F}_{P^m} \subset \overline{\mathbb{F}}_p$, and $\varphi\colon x \mapsto x^P$ is the P-Frobenius, an automorphism of $\overline{\mathbb{F}}_p$ whose restriction generates $\mathrm{Gal}(K/\mathbb{F}_P)$ for every finite $K \supseteq \mathbb{F}_P$.

Lemma 1.1 (Frobenius selectors)**.** *Let $m_1, \dots, m_r$ be pairwise coprime and let $(w_i)_{i\le r}$ be integers. There is $s \ge 0$ with $s \equiv w_i \pmod{m_i}$ for all i, and $\tau := \varphi^s \in \mathrm{Aut}(\overline{\mathbb{F}}_p)$ satisfies $\tau|_{K_{m_i}} = \varphi^{w_i}|_{K_{m_i}}$ for every i. In particular, for each j there is τ_j acting as the identity on K_{m_j} and as φ on every K_{m_i}, $i \ne j$.*

Proof. Chinese remainder theorem; $\varphi^s|_{K_{m_i}}$ depends only on $s \bmod m_i$ because φ^{m_i} is the identity on K_{m_i}. □

Theorem 1.2 (Point count on coprime-degree grids)**.** *Let $\gcd(m_1, m_2) = 1$ and let $Q \in \overline{\mathbb{F}}_p[X, Y]$ be irreducible of bidegree (a, b) with $a, b \ge 1$. Then Q has at most $(P+1)ab$ zeros on $K_{m_1} \times K_{m_2}$. More precisely, with Γ_Q the branch-weighted count (4) below, $\Gamma_Q \le (P+1)ab$.*

Theorem 1.3 (Two directions)**.** *Let $\gcd(m_1, m_2) = 1$, let $S_i \subseteq K_{m_i}$ with $|S_i| = n$, let $F \subset \overline{\mathbb{F}}_p$ be a finite field containing $S_1 \cup S_2$, let $0 < \varepsilon < 1$, $1 \le k_i \le (1-\varepsilon)n$, and let $C_i = D_i \mathrm{RS}(S_i, k_i) \subseteq F^{S_i}$ with D_i invertible diagonal. Then (C_1, C_2) is ρ-product expanding with*

$$\rho = \frac{\varepsilon^2}{8(P+5)^2}.$$

Consequently all two-element subtuples in Hypothesis PE are $\nu^2/(8(P+5)^2)$-product expanding, for every P (any prime power) and every scalar field.

The higher-dimensional statement depends on one imported result, which we name once and for all. For an integer $m \ge 1$ let

> (CG_m): *the cylinder-gluing theorem [4, Thm. B.6], restated with its exact hypotheses as Theorem 4.9 below, holds for grids with m directions and positive-dimensional cylinders (the only case used here).*

(CG_m) is [4, Thm. B.6], which is stated there under the standing hypothesis of that appendix that the S_i are subsets of norm-one sets, but whose proof does not use the form of the S_i (we checked this clause by clause; see the status paragraph after Theorem 4.9). We reproduce its statement for arbitrary finite sets, describe its proof and the checks we made, and prove it ourselves for $m \le 2$ and for unions of hyperplane cylinders in any dimension (Proposition 4.11). For $m = 3$ we reduce it to the configuration of complete lines in three directions (Proposition 4.11(b)). Everything else below is proved in this paper.

Theorem 1.4 (All directions)**.** *Let $p = 2$, $P = 2^f$, $r \ge 2$, $m_1, \dots, m_r$ pairwise coprime, $\emptyset \ne S_i \subseteq K_{m_i}$ with $|S_i| = n_i$ and $\max_i n_i \le R_0 \min_i n_i$, and let $F \subset \overline{\mathbb{F}}_2$ be a finite field containing all S_i. Let $0 < \beta \le 1$, $\beta n_i \le h_i \le n_i$, and $C_i = D_i \mathrm{RS}(S_i, n_i - h_i) \subseteq F^{S_i}$. Assume ($\mathrm{CG}_m$) for $3 \le m \le r$ (no assumption if $r = 2$). Then every nonempty subtuple of $(C_i)_{i\le r}$ is ϱ-product expanding with*

$$\varrho = \frac{1}{r}\Big(\frac{\beta}{K_r(P) R_0}\Big)^r, \qquad K_r(P) = K'_r, \quad K'_1 = 2, \quad K'_m = m^2 2^{m+1}\big(K'_{m-1} + P + 1\big).$$

Corollary 1.5 (Hypothesis PE)**.** *Assume (CG_3); by Proposition 4.11(b) it suffices to assume it for unions of complete lines in three directions. Then Hypothesis PE holds with*

$$\rho(P, \nu) = \frac{1}{3}\Big(\frac{\nu}{K_3(P)}\Big)^3, \qquad K_3(P) = 144\,(33P + 97).$$

For the specialization used in [8] ($\nu = 1/8$) and $P = 2$ this is $\rho \approx 5 \cdot 10^{-17}$; only positivity and uniformity are needed there.

Logical status. The two-direction part of Hypothesis PE is a theorem (Section 3; no external input beyond classical curve theory). The full hypothesis is a theorem modulo (CG_3), a statement proved in [4] (for norm-one sets, by an argument that does not use their form) by sheaf-cohomological means that we have inspected (§4.4) but not independently re-derived. No other step of the argument is imported; Section 4.7 lists precisely what is.

1.4 Techniques

All new arguments rest on one observation. If $m_1, \dots, m_r$ are pairwise coprime, the Chinese remainder theorem produces powers τ of the P-Frobenius $\varphi\colon x \mapsto x^P$ that act as the identity on $K_{m_j} = \mathbb{F}_{P^{m_j}}$ and as φ on every other K_{m_i} (Lemma 1.1, *Frobenius selectors*). Such a τ preserves the grid $\prod_i K_{m_i}$ while acting on polynomials as a substitution $X_i \mapsto X_i^P$ in the directions $i \neq j$.

For two directions this gives a *grid-preserving transform* $Q \mapsto \mathcal{T}Q = Q^\sigma(X, Y^P)$ on bivariate polynomials, with the same zeros as Q on $K_{m_1} \times K_{m_2}$. An irreducible Q of bidegree (a, b) with $a, b \geq 1$ never divides $\mathcal{T}Q$ (Lemma 2.1, a unique-factorization argument), so $\mathcal{T}Q$ restricts to a nonzero rational function on the curve $Q = 0$ that vanishes at every grid point of the curve; a pole count then bounds the number of grid points by $(P{+}1)ab$ (Theorem 1.2). This bound is independent of the extension degrees and of the coefficient field, and it replaces the Corvaja–Zannier estimate in the bivariate divisibility lemma of [2]; the Polishchuk–Spielman decomposition argument then gives Theorem 1.3, with a divisibility threshold that is linear in the redundancy rather than cubic.

For more directions we use the framework of [4]: product expansion follows from the *inner generation* of polynomial zero sets (every sum of line codewords supported on the zero set of a low-degree polynomial is a sum of line codewords on lines inside the zero set), via polynomial hulls and a descent to the scalar field. Their proof of inner generation uses the norm-one structure of their evaluation sets in exactly one place, a lemma that isolates one partial derivative of a polynomial at a time. Frobenius selectors give a direct replacement on coprime-degree subfield grids (Lemma 4.1), with no restriction on the evaluation sets and no monomial prefactors. We then write out their induction in full in our setting (Proposition 4.13), with every imported statement restated with its exact hypotheses (§4.4); the only one that we do not re-prove is their cylinder-gluing theorem, a statement about unions of coordinate cylinders proved by sheaf cohomology on $(\mathbb{P}^1)^m$. We prove it by an elementary Boolean-sum interpolation for $m \leq 2$ and for unions of hyperplane cylinders in any dimension, and reduce its three-dimensional case to unions of complete lines in three directions (Proposition 4.11).

Finally, the three new algebraic lemmas (Lemmas 1.1, 2.1 and 4.1) have been formalized and checked in the Lean 4 proof assistant with the Mathlib library; Appendix A records what was checked and how.

1.5 Organization

Section 2 proves the point-count theorem, Section 3 the two-direction case, and Section 4 the general case: the framework (§4.1), the derivative-isolation lemma (§4.2), the imported statements (§4.4), the induction (§4.5), the passage to product expansion (§4.6) and a summary of what is imported (§4.7). Section 5 discusses the application to [8], the scope of the result and open problems. Appendix A describes the machine-checked components.

2 The point-count lemma

Fix $\gcd(m_1, m_2) = 1$ and let $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}}_p)$ be the selector of Lemma 1.1 with $\sigma|_{K_{m_1}} = \mathrm{id}$, $\sigma|_{K_{m_2}} = \varphi$. For $Q = \sum q_{ij} X^i Y^j$ write $Q^\sigma = \sum \sigma(q_{ij}) X^i Y^j$ and

$$\mathcal{T}Q(X, Y) := Q^\sigma(X, Y^P).$$

The point of $\mathcal{T}$ is that it preserves the grid: for $(\alpha, \beta) \in K_{m_1} \times K_{m_2}$,

$$\mathcal{T}Q(\alpha, \beta) = Q^\sigma(\sigma\alpha, \sigma\beta) = \sigma\big(Q(\alpha, \beta)\big), \tag{2}$$

so Q and $\mathcal{T}Q$ have the same zeros on $K_{m_1} \times K_{m_2}$, while $\mathcal{T}$ multiplies the Y-degree by P and keeps the X-degree.

Lemma 2.1. *If $Q \in \overline{\mathbb{F}}_p[X, Y]$ is irreducible of bidegree (a, b) with $a, b \geq 1$, then $Q \nmid \mathcal{T}Q$.*

Proof. Let $\theta = \varphi^{-1}$ and $H := Q^{\theta\sigma}(X', Y) \in \overline{\mathbb{F}}_p[X', Y]$, where X' is a new variable. Since $\theta\sigma$ is a field automorphism, H is irreducible in $R' := \overline{\mathbb{F}}_p[X', Y]$, and in R' we have $H^P = \sum \sigma(q_{ij}) X'^{Pi} Y^{Pj} = \mathcal{T}Q(X'^P, Y)$. Identify $R := \overline{\mathbb{F}}_p[X, Y]$ with the subring $\overline{\mathbb{F}}_p[X'^P, Y] \subset R'$ via $X = X'^P$. If $Q \mid \mathcal{T}Q$ in R, then $Q(X'^P, Y) \mid H^P$ in R', so by unique factorization every irreducible factor of $Q(X'^P, Y)$ in R' is an associate of H, i.e. $Q(X'^P, Y) = cH^e$ for some $c \in \overline{\mathbb{F}}_p^\times$, $e \geq 1$. Comparing Y-degrees gives $b = eb$, so $e = 1$; comparing X'-degrees then gives $Pa = a$, so $a = 0$, a contradiction. □

Curve-theoretic set-up (as in [2, §4.4.1]). Let Q be irreducible of bidegree (a, b), $a, b \geq 1$, and let X_Q be the normalization of the closure of $\{Q = 0\}$ in $\mathbb{P}^1 \times \mathbb{P}^1$; it is a smooth projective curve over $\overline{\mathbb{F}}_p$ with coordinate functions $x, y \in \overline{\mathbb{F}}_p(X_Q)$ of degrees $\deg x = b$, $\deg y = a$. For a point $\nu \in X_Q$ and $f \neq 0$, $\mathrm{ord}_\nu f$ is the order of vanishing. A polynomial $H(X, Y)$ of bidegree at most (D_X, D_Y) that does not vanish identically on X_Q gives a rational function $H(x, y)$ whose poles lie over the poles of x and y, with total pole order at most $D_X \deg x + D_Y \deg y = D_X b + D_Y a$; hence

$$\#\{\text{zeros of } H(x, y) \text{ on } X_Q, \text{ with multiplicity}\} \leq D_X b + D_Y a. \tag{3}$$

For a finite set $T_1 \times T_2 \subseteq K_{m_1} \times K_{m_2}$ define the branch-weighted count

$$\Gamma_Q(T_1 \times T_2) := \sum_{\substack{\nu \in X_Q \\ x(\nu) \in T_1,\ y(\nu) \in T_2}} \min\big\{\mathrm{ord}_\nu(x - x(\nu)),\, \mathrm{ord}_\nu(y - y(\nu))\big\}, \qquad \Gamma_Q := \Gamma_Q(K_{m_1} \times K_{m_2}). \tag{4}$$

Every grid point on the curve has at least one branch above it, contributing at least 1; so $\#(\{Q = 0\} \cap T_1 \times T_2) \leq \Gamma_Q(T_1 \times T_2) \leq \Gamma_Q$.

Proof of Theorem 1.2. Put $G := \mathcal{T}Q(x, y) = Q^\sigma(x, y^P) \in \overline{\mathbb{F}}_p(X_Q)$. By Lemma 2.1, $\mathcal{T}Q$ is not divisible by Q, hence does not vanish identically on the irreducible curve, so $G \neq 0$. Since $\mathcal{T}Q$ has bidegree (a, Pb), (3) gives at most $ab + Pab = (P + 1)ab$ zeros of G counted with multiplicity.

Now let $\nu \in X_Q$ lie over a grid point $(\alpha, \beta) \in K_{m_1} \times K_{m_2}$. Expand the polynomial Q^σ around (α, β^P): $Q^\sigma(\alpha + U, \beta^P + V) = \sum_{i,j} c_{ij} U^i V^j$ with $c_{00} = Q^\sigma(\alpha, \beta^P) = \sigma(Q(\alpha, \beta)) = 0$ by (2). Substituting $U = x - \alpha$ and $V = y^P - \beta^P = (y - \beta)^P$,

$$G = \sum_{(i,j) \neq (0,0)} c_{ij}\, (x - \alpha)^i (y - \beta)^{Pj},$$

so that

$$\mathrm{ord}_\nu G \;\geq\; \min\{\mathrm{ord}_\nu(x - \alpha),\, P\,\mathrm{ord}_\nu(y - \beta)\} \;\geq\; \min\{\mathrm{ord}_\nu(x - \alpha), \mathrm{ord}_\nu(y - \beta)\}.$$

Summing over all branches above grid points, $\Gamma_Q \leq \sum_\nu \mathrm{ord}_\nu G \leq (P + 1)ab$. □

Remark 2.2. (i) The bound is attained for $(a,b)=(1,1)$: with $P=2$, $\mathbb{F}_{64}=\mathbb{F}_2(g)$, $g^6+g^4+g^3+g+1=0$, $\mathbb{F}_4=\mathbb{F}_2(g^{21})$ and $\mathbb{F}_8=\mathbb{F}_2(g^9)$, the bilinear curve $XY+g(X+Y)=0$ contains the three grid points $(0,0)$, (g^{21},g^{27}), (g^{42},g^{18}) of $\mathbb{F}_4\times\mathbb{F}_8$ (a direct check), and $3=P+1$. (ii) Compare [2, Thm. 4.12]: $\Gamma_F\le C\,(N^{1/3}(ab)^{2/3}+ab)$ for coprime subgroups of orders n_1,n_2, $N=n_1n_2<q$, q prime. Theorem 1.2 has no dependence on n or on the field, no primality restriction, and an elementary proof. This is what makes the divisibility threshold below *linear* in h instead of h^3/N. (iii) The dependence on P is necessary, and it is exactly the size of the intersection field that matters: for $\mathbb{F}_{16}\subset\mathbb{F}_{256}$ the trace curve $XY+Y^2+1=0$ (bidegree $(1,2)$) has 31 points on $\mathbb{F}_{16}\times\mathbb{F}_{256}$ and 17 on $\mathbb{F}_{16}\times\mu_{17}$, and $X-Y$ has 16 points on $\mathbb{F}_{16}\times\mathbb{F}_{16}$. Read as instances with base field $\mathbb{F}_{16}$ (degrees $(1,2)$ and $(1,1)$, $P=16$) these respect the bounds 34 and 17, but a bound growing with the intersection field is useless for product expansion: these three configurations are precisely the known witnesses (the reflected Polishchuk–Spielman corner $2\nu_1+\nu_2>2$ and the rate-sum-one barrier). In Hypothesis PE the intersection field is the fixed $\mathbb{F}_P$, which is what makes the bound uniform in n. (iv) If $\gcd(m_1,m_2)=g>1$ the same proof works with $\sigma|_{K_{m_2}}=\varphi^g$ and gives $(P^g+1)ab$: the effective base field is $K_{m_1}\cap K_{m_2}=\mathbb{F}_{P^g}$.

3 Two directions

Lemma 3.1 (Bivariate divisibility on a coprime-degree subfield grid)**.** *Let* $\gcd(m_1,m_2)=1$, $S_i\subseteq K_{m_i}$ *with* $|S_i|=n_i$, *integers* $0\le k_i<n_i$, *and* $h:=\min\{n_1-k_1,n_2-k_2\}$. *Let* $E,\Phi\in\overline{\mathbb{F}}_p[X,Y]$ *with* $E\neq0$, $e_X=\deg_X E$, $e_Y=\deg_Y E$, $t=\max\{e_X,e_Y\}$, *and suppose*

$$t<\frac{2h}{P+5},\qquad \deg_X\Phi<k_1+e_X,\qquad \deg_Y\Phi<k_2+e_Y,$$

and that for every $\alpha\in S_1$ *and* $\beta\in S_2$ *there are polynomials* R_α,C_β *with* $\Phi(\alpha,Y)=E(\alpha,Y)R_\alpha(Y)$ *and* $\Phi(X,\beta)=E(X,\beta)C_\beta(X)$. *Then* $E\mid\Phi$; *hence* $\Phi=EQ$ *with* $\deg_X Q<k_1$ *and* $\deg_Y Q<k_2$.

Proof. This is [2, Lemma 4.13] with the Corvaja–Zannier input replaced by Theorem 1.2; we give the full argument. If $\Phi=0$ there is nothing to prove.

Mixed factors. Let F be an irreducible factor of E with $a=\deg_X F\ge1$ and $b=\deg_Y F\ge1$, and suppose $F\nmid\Phi$. Then $\Phi(x,y)\neq0$ in $\overline{\mathbb{F}}_p(X_F)$. For $\alpha\in S_1$ we have $F(\alpha,Y)\neq0$ (otherwise $X-\alpha$ would divide the irreducible F, forcing $b=0$), and $F(\alpha,Y)\mid\Phi(\alpha,Y)$: if $E(\alpha,Y)\neq0$ this follows from $F(\alpha,Y)\mid E(\alpha,Y)\mid\Phi(\alpha,Y)$, and if $E(\alpha,Y)=0$ the hypothesis gives $\Phi(\alpha,Y)=0$. Writing $\Phi(\alpha,Y)=F(\alpha,Y)R'_\alpha(Y)$ we get $\Phi(X,Y)=F(X,Y)R'_\alpha(Y)+(X-\alpha)K_\alpha(X,Y)$, so on X_F, $\Phi(x,y)=(x-\alpha)K_\alpha(x,y)$ and therefore $\operatorname{ord}_\nu\Phi(x,y)\ge\operatorname{ord}_\nu(x-\alpha)$ at every ν with $x(\nu)=\alpha$ and $y(\nu)\neq\infty$. Symmetrically for $\beta\in S_2$. Set $A_\nu=\operatorname{ord}_\nu(x-\alpha)$ if $x(\nu)=\alpha\in S_1$ and $y(\nu)\neq\infty$, and $A_\nu=0$ otherwise; define B_ν symmetrically. Then $\operatorname{ord}_\nu\Phi\ge\max\{A_\nu,B_\nu\}=A_\nu+B_\nu-\min\{A_\nu,B_\nu\}$ wherever $A_\nu+B_\nu>0$. The zero divisor of $\prod_{\alpha\in S_1}(x-\alpha)$ has degree n_1b; the part of it lying over $y=\infty$ has degree at most ab (at most a such points, each with $\operatorname{ord}_\nu(x-\alpha)\le\deg(x)=b$ for the unique relevant α). Hence $\sum_\nu A_\nu\ge n_1b-ab$, and likewise $\sum_\nu B_\nu\ge n_2a-ab$, while $\sum_\nu\min\{A_\nu,B_\nu\}=\Gamma_F(S_1\times S_2)\le(P+1)ab$ by Theorem 1.2. Thus $\Phi(x,y)$ has at least $n_1b+n_2a-(P+3)ab$ zeros. By (3) it has at most $(k_1+e_X-1)b+(k_2+e_Y-1)a$. Therefore

$$(h-t+1)(a+b)\ \le\ (n_1-k_1-e_X+1)b+(n_2-k_2-e_Y+1)a\ \le\ (P+3)ab\ \le\ \tfrac12(P+3)\,t\,(a+b),$$

using $a,b\le t$ in the last step. This gives $t\ge2(h+1)/(P+5)>2h/(P+5)$, contradicting the hypothesis. Hence $F\mid\Phi$.

Write $E=FE_1$, $\Phi=F\Phi_1$. The pair (E_1,Φ_1) satisfies the same hypotheses: the degree bounds drop by (a,b) on both sides; for $\alpha\in S_1$, if $E(\alpha,Y)\neq0$ then cancelling the nonzero $F(\alpha,Y)$

gives $E_1(\alpha, Y) \mid \Phi_1(\alpha, Y)$, and if $E(\alpha, Y) = 0$ then $E_1(\alpha, Y) = 0 = \Phi_1(\alpha, Y)$; t does not increase. Iterating removes all mixed factors with their multiplicities.

Factors in one variable. It remains to treat $E_0 = U(X)V(Y)$ with quotient Φ_0 (normalize V to be monic by moving a constant into U). Divide Φ_0 by V in $\overline{\mathbb{F}}_p[X][Y]$: $\Phi_0 = VQ_0 + R$ with $\deg_Y R < \deg V$. For $\alpha \in S_1$ with $U(\alpha) \neq 0$, $V \mid \Phi_0(\alpha, Y)$ forces $R(\alpha, Y) = 0$; for $U(\alpha) = 0$ we have $\Phi_0(\alpha, Y) = 0$ and again $R(\alpha, Y) = 0$. Each coefficient of R is a polynomial in X of degree $\leq \deg_X \Phi_0 < k_1 + \deg U \leq k_1 + t < k_1 + h \leq n_1$ vanishing on the n_1 points of S_1, hence zero. So $V \mid \Phi_0$, symmetrically $U \mid \Phi_0$, and since U, V are coprime, $UV \mid \Phi_0$. The degree bounds for $Q = \Phi/E$ follow by subtraction. □

Proof of Theorem 1.3. This is the Polishchuk–Spielman argument in the form of [2, Thm. 4.11]. Rescaling: if $A \in Q_1 + Q_2$ for $(D_1\mathrm{RS}, D_2\mathrm{RS})$, then the array $A'(x, y) = A(x, y)/(d_1(x)d_2(y))$ lies in $Q_1 + Q_2$ for $(\mathrm{RS}(S_1, k_1), \mathrm{RS}(S_2, k_2))$, with the same support and the same nonzero lines in every decomposition; so assume $D_i = I$. Write $n_1 = n_2 = n$, $h = \min_i(n - k_i) \geq \varepsilon n$, $N = n^2$, and

$$\tau := \frac{h}{P+5} \left(\leq \frac{h}{4}\right), \qquad \rho := \min\left\{\frac{h}{4n}, \frac{\tau^2}{8N}\right\} = \frac{h^2}{8(P+5)^2 n^2} \;\geq\; \frac{\varepsilon^2}{8(P+5)^2}.$$

Let $M = A + B \in Q_1 + Q_2$ with $A \in Q_1$ (direction-1 lines, i.e. $Y = \beta$ fixed, are codewords of C_1), $B \in Q_2$, and $w = |M|$. If $w = 0$ use the zero decomposition.

Large weight, $w \geq \tau^2/4$. Keep $M = A + B$: $n|A|_1 + n|B|_2 \leq 2N \leq (8N/\tau^2)\, w \leq \rho^{-1} w$.

Small weight, $0 < w < \tau^2/4$. Let $t = \lfloor \sqrt{w} \rfloor < \tau/2$. Since $(t+1)^2 > w$, there is a nonzero $E \in F[X, Y]$ of bidegree $\leq (t, t)$ vanishing on $\operatorname{supp} M$ (a homogeneous linear system over F with more unknowns than equations). Let $A(X, Y)$ be the unique polynomial with $\deg_X < k_1$, $\deg_Y < n$ agreeing with the array A on the grid (each line $Y = \beta$ is a polynomial of degree $< k_1$ in X; interpolate the coefficients in Y across S_2), and similarly $B(X, Y)$ with $\deg_Y < k_2$, $\deg_X < n$. Since $EM = 0$ on the grid, the arrays EA and $-EB$ coincide there. Reducing EA modulo $\prod_{\beta \in S_2}(Y - \beta)$ in the variable Y and $-EB$ modulo $\prod_{\alpha \in S_1}(X - \alpha)$ in X gives two polynomials of individual degrees $< (n, n)$ with the same grid values, hence equal; call it Φ. Thus $\deg_X \Phi < k_1 + e_X \leq n$ and $\deg_Y \Phi < k_2 + e_Y \leq n$. On each line $Y = \beta$ the polynomials $\Phi(X, \beta)$ and $E(X, \beta)A(X, \beta)$ have degree $< n$ and agree on S_1, so they are equal; similarly $\Phi(\alpha, Y) = -E(\alpha, Y)B(\alpha, Y)$. Since $t < \tau/2 < 2h/(P+5)$, Lemma 3.1 gives $\Phi = EQ$ with $\deg_X Q < k_1$, $\deg_Y Q < k_2$ (and $Q \in F[X, Y]$, as the quotient of polynomials over F). The array of Q lies in $Q_1 \cap Q_2$, so $M = (A - Q) + (B + Q)$ is again a decomposition. Let J be the set of nonzero lines $Y = \beta$ of $A - Q$ and I the set of nonzero lines $X = \alpha$ of $B + Q$. For $\beta \in J$, $E(X, \beta)(A - Q)(X, \beta) = \Phi(X, \beta) - E(X, \beta)Q(X, \beta) = 0$ forces $E(X, \beta) \equiv 0$, i.e. $(Y - \beta) \mid E$; so $|J| \leq e_Y \leq t$, and likewise $|I| \leq t$. Each nonzero line of $A - Q$ is a codeword of $\mathrm{RS}(S_1, k_1)$, of weight $\geq h + 1$; outside the lines of I the array $B + Q$ vanishes, so $M = A - Q$ there, and the line contributes at least $h + 1 - |I|$ points to $\operatorname{supp} M$. Hence $w \geq |J|(h + 1 - |I|)$ and $w \geq |I|(h + 1 - |J|)$; with $|I|, |J| \leq t < h/4$ this gives $|I|, |J| \leq 2w/h$, so

$$n|J| + n|I| \leq \frac{4n}{h}\, w \leq \rho^{-1} w.$$ □

Remark 3.2. (i) Nothing in §2–§3 uses characteristic two or equal lengths; for $n_1 \neq n_2$ one gets $\rho = \min\{h/(2(n_1+n_2)),\, h^2/(8(P+5)^2 n_1 n_2)\}$. (ii) The theorem is not comparable to [2, Thm. 4.11]: the independence mechanism there is coprime *subgroup orders* inside one prime field (in our notation $m_1 = m_2 = 1$, $P = q$, where Theorem 1.3 degenerates), here it is coprime *extension degrees* with the intersection field fixed. Within its own setting Theorem 1.3 allows arbitrary subsets and any finite field and has the polynomial constant $\varepsilon^2/(8(P+5)^2)$; the proof structure is identical to [2], with Theorem 1.2 playing the role of the Corvaja–Zannier estimate. (iii) By the Kalachev–Panteleev

equivalence [9, Lemma 1], Theorem 1.3 is also the robust/agreement testability of $C_1 \otimes C_2$ for all these pairs; by the robustness-composition results for tensor codes [3, 13] it should also give robust testability of the triple tensor codes $C_1 \otimes C_2 \otimes C_3$ under the axis-parallel line test, although we have not checked the parameters. The latter is *weaker* than three-direction product expansion [10, §1], which is what the Dinur–Lin–Vidick local-to-global argument of the distance-transfer argument of [8, Thm. 7.4, Lemma 7.6] consumes; this is why Section 4 is needed.

4 All directions: transporting the inner-generation framework

4.1 The framework

We recall [4, §5 and App. B] in our notation. Let $\overline{\mathbb{F}} = \overline{\mathbb{F}}_2$, let S_i ($i \in J$, $|J| = m$) be finite nonempty subsets of $\overline{\mathbb{F}}$, $n_i = |S_i|$, redundancies $1 \le h_i \le n_i$, $H = \min_i h_i$, $C_i = \mathrm{RS}(S_i, n_i - h_i)$ over $\overline{\mathbb{F}}$, and

$$\mathcal{B}_h := \sum_{\ell} C_\ell = \Big(\bigotimes_{i \in J} C_i^{\perp}\Big)^{\perp} \subseteq \overline{\mathbb{F}}^G, \qquad G = \prod_{i \in J} S_i,$$

the span of all coordinate-line codewords (C_ℓ is C_i placed on the direction-i line ℓ). A scalar subscript $\mathcal{B}_w$ means $h_i = w$ for all i; since $\mathrm{RS}(S_i, n_i - h_i)$ shrinks as h_i grows, $\mathcal{B}_{h'} \subseteq \mathcal{B}_h$ whenever $h' \ge h$ componentwise. For a sub-grid in the directions $I \subseteq J$ the same notation is used with J replaced by I. A set $Z \subseteq G$ is *inner-generated* (for $\mathcal{B}_h$) if every element of $\mathcal{B}_h$ supported in Z is a sum of line codewords on lines contained in Z. For $U \subseteq G$ and $d \ge 0$ the *degree-d hull* is $\mathrm{hull}_d(U) = \{z \in G : \ f(z) = 0 \ \forall f \in \mathcal{P}_d \text{ with } f|_U = 0\}$, where $\mathcal{P}_d$ are the polynomials of degree $\le d$ in each variable. For a polynomial E, Z_E is its zero set on G and U_E the union of all coordinate lines of G contained in Z_E. The three generic facts are:

- [4, Lemma 5.3] (= Lemma 4.14 below): if the support of every nonzero $x \in \mathcal{B}$ lies in an inner-generated Z with $|Z| \le K|\operatorname{supp} x|$, then $(C_i)_{i \in J}$ is $\frac{1}{|J|K}$-product expanding.
- [4, Lemma 5.6] (= Lemma 4.15 below): hulls are unchanged by field extension; if $d + 1 \le n_i$ for all i then $|\mathrm{hull}_d(U)| \le |U| \prod_i \frac{n_i}{d+1}$; and if $Z = \mathrm{hull}_d(U) \ne G$ there is a nonzero $E \in \mathcal{P}_d(\overline{\mathbb{F}})$ whose grid zero set is exactly Z.
- [4, Thm. 5.7 = Thm. B.1] (inner generation of polynomial zero sets): *there is $K_r \ge 2$ such that if $E \ne 0$ has coordinate degrees $\le d \ge 1$ and $H \ge K_r d$, then Z_E is inner-generated.* This is the only place where the evaluation sets matter; its transported version is Theorem 4.3.

Given these, [4, proof of Thm. 5.4] proceeds: for $x \in \mathcal{B}_J \setminus 0$ put $U = \operatorname{supp} x$, $d = \lfloor H/K_r \rfloor$, $Z = \mathrm{hull}_d(U)$; then $d + 1 \le n_i$, $|Z| \le |U| \prod_i n_i/(d+1) \le |U|(K_r R_0/\beta)^{|J|}$ because $n_i/(d+1) < K_r n_i/H \le K_r R_0/\beta$; Z is inner-generated over $\overline{\mathbb{F}}$ (trivially if $Z = G$, by Thm. 5.7 otherwise); inner generation descends to F by rank invariance (Lemma 4.16); Lemma 5.3 concludes. The proof of Theorem 1.4 in §4.6 follows this scheme line by line.

4.2 Where the norm-one structure enters, and its replacement

The proof of [4, Thm. B.1] uses: the parity test (their (25)); interpolation bounds (Def. B.2, Lemma B.3); two gradient lemmas (Lemma B.4 "isolating a derivative", Lemma B.5 "Jacobian"); the cylinder-gluing Theorem B.6; and the induction of §B.4. Of these, only Lemma B.4 uses the sets in an essential way (the induction of §B.4 also invokes "all grid coordinates are nonzero" once, which is dispensable; see step (II) of Proposition 4.13): "*The following lemma relies on our choice*

of Σ_i as a norm-one set. It uses the identity $x_i^{2^{a_i}} = x_i^{-1}$ on $S_i \subseteq \Sigma_i$ to isolate one partial derivative at a time". Its role: given F depending on X_j, produce R_j with the same grid zero set, coordinate degrees $\le K_r'' \deg_i F$, $\partial_i R_j \equiv 0$ for $i \neq j$, and $\partial_j R_j(x) \neq 0$ exactly where a nonzero polynomial b_j of smaller total degree is nonzero. On coprime-degree subfield grids the Frobenius selectors do this directly, with constant P and without the monomial prefactors of [4] (so grid coordinates equal to 0 are allowed). All other ingredients are restated with their exact hypotheses, and proved, in §4.4, with the single exception of Theorem 4.9.

Lemma 4.1 (Isolating a derivative; replacement for [4, Lemma B.4])**.** *Let $P = 2^f$, let m_i $(i \in J)$ be pairwise coprime and $S_i \subseteq K_{m_i}$. Let $0 \neq F \in \overline{\mathbb{F}}_2[X_i : i \in J]$ depend on X_j. For each i let $u_i \ge 0$ be maximal with 2^{u_i} dividing every exponent of X_i occurring in F ($u_i = 0$ if X_i is absent), and let G be defined by $F = G\big((X_i^{2^{u_i}})_i\big)$. Put $b_j := (\partial_j G)\big((X_i^{2^{u_i}})_i\big)$. Then $b_j \neq 0$, b_j has smaller total degree than F and no larger coordinate degrees, and there is $R_j \in \overline{\mathbb{F}}_2[X_i : i \in J]$ and an automorphism σ of $\overline{\mathbb{F}}_2$ such that*

(a) $R_j(x) = \sigma(F(x))$ for every $x \in \prod_i K_{m_i}$; in particular R_j and F have the same zero set on $\prod_i S_i$;

(b) $\partial_i R_j \equiv 0$ for every $i \neq j$;

(c) $\partial_j R_j(x) = \sigma(b_j(x))$ for every $x \in \prod_i K_{m_i}$;

(d) $\deg_i R_j \le P \deg_i F$ for $i \neq j$ and $\deg_j R_j \le \deg_j F$.

Proof. By maximality of u_j some exponent of X_j in G is odd, so $\partial_j G \neq 0$ in characteristic two and $b_j \neq 0$. A monomial X^γ of G corresponds to the monomial of F with exponents $2^{u_i}\gamma_i$; the monomials of $\partial_j G$ are $X^{\gamma - e_j}$ with γ_j odd, so b_j's monomials have total degree $\sum_i 2^{u_i}\gamma_i - 2^{u_j}$, smaller than the corresponding monomial of F, and coordinate degrees $\le$ those of F.

Choose $v_j = 0$ and, for $i \neq j$, $v_i \in \{1, \dots, f\}$ with $v_i \equiv u_i - u_j \pmod f$. Then $u_i - v_i \equiv u_j \pmod f$ for all i. Consider the congruences $e \equiv u_i - v_i \pmod{fm_i}$, $i \in J$. Since $\gcd(fm_i, fm_k) = f$ for $i \neq k$ and the right-hand sides are pairwise congruent modulo f, the system is solvable; fix a solution $e \ge 0$ (generalized Chinese remainder theorem). Let $\sigma := \mathrm{Frob}_2^{-e}$ $(c \mapsto c^{2^{-e}})$ and

$$R_j := G^\sigma\big((X_i^{2^{v_i}})_i\big),$$

where G^σ applies σ to the coefficients. For $x_i \in K_{m_i} = \mathbb{F}_{2^{fm_i}}$ we have $x_i^{2^{fm_i}} = x_i$, hence $x_i^{2^{v_i+e}} = x_i^{2^{u_i}}$ because $v_i + e \equiv u_i \pmod{fm_i}$. Therefore, for $x \in \prod_i K_{m_i}$,

$$R_j(x) = \sigma\Big(G\big((\sigma^{-1}(x_i^{2^{v_i}}))_i\big)\Big) = \sigma\Big(G\big((x_i^{2^{v_i+e}})_i\big)\Big) = \sigma\Big(G\big((x_i^{2^{u_i}})_i\big)\Big) = \sigma(F(x)),$$

which is (a). For $i \neq j$ every exponent of X_i in R_j is a multiple of 2^{v_i} with $v_i \ge 1$, so $\partial_i R_j \equiv 0$ in characteristic two, which is (b). Since $v_j = 0$, $\partial_j R_j = (\partial_j G)^\sigma\big((X_i^{2^{v_i}})_i\big)$, and the computation of (a) applied to $\partial_j G$ gives (c). Finally $\deg_i R_j = 2^{v_i} \deg_i G \le 2^f \deg_i G \le P \deg_i F$ for $i \neq j$ and $\deg_j R_j = \deg_j G \le \deg_j F$, which is (d). □

Remark 4.2. (i) For $f = 1$ $(P = 2)$ the choice is forced: $v_i = 1$ for $i \neq j$ and $e \equiv u_i - 1 \pmod{m_i}$ $(i \neq j)$, $e \equiv u_j \pmod{m_j}$. (ii) With pairwise $\gcd(m_i, m_k) \le g$ the same proof works with $v_i \in \{1, \dots, fL\}$, $L =$ lcm of the pairwise gcds, and constant P^L in (d). (iii) $R_j \neq 0$: indeed $G^\sigma \neq 0$ and the substitution $X_i \mapsto X_i^{2^{v_i}}$ is injective on monomials. (iv) Lemma 4.1 is machine-checked (Appendix A).

4.3 The inner-generation theorem on coprime-degree grids

Theorem 4.3 (Inner generation; [4, Thm. 5.7] transported)**.** *Let $P = 2^f$, $r \geq 2$, $m_1, \ldots, m_r$ pairwise coprime, $\emptyset \neq J \subseteq [r]$, $\emptyset \neq S_i \subseteq K_{m_i}$, $1 \leq h_i \leq n_i = |S_i|$, $C_i = \mathrm{RS}(S_i, n_i - h_i)$ over $\overline{\mathbb{F}}_2$, and $0 \neq E \in \overline{\mathbb{F}}_2[X_i : i \in J]$ of coordinate degrees $\leq d \geq 1$. Assume (CG_m) for $3 \leq m \leq |J|$. If $h_i \geq K_r(P)\, d$ for all $i \in J$, with $K_r(P)$ as in Theorem 1.4, then every codeword of $\mathcal{B}_h$ supported on Z_E is a sum of line codewords on coordinate lines contained in Z_E.*

The proof is Proposition 4.13 in §4.5; it uses the statements collected next.

4.4 The imported statements, with exact hypotheses

Throughout this subsection $\overline{\mathbb{F}}$ is an algebraically closed field of characteristic two, $S_i \subset \overline{\mathbb{F}}$ ($i \in J$, $|J| = m$) are finite nonempty, $n_i = |S_i|$, $1 \leq h_i \leq n_i$, $H = \min_i h_i$, $C_i = \mathrm{RS}(S_i, n_i - h_i)$, $v_i(a) = \prod_{b \in S_i \setminus \{a\}} (a-b)^{-1}$ and $v(x) = \prod_{i \in J} v_i(x_i)$. Nothing here uses the special form of the sets S_i (the only such ingredient is Lemma 4.1).

Lemma 4.4 (Parity test; [4, (25)])**.** *$C_i^{\perp} = \mathrm{diag}(v_i)\mathrm{RS}(S_i, h_i)$, and consequently*

$$M \in \mathcal{B}_h \quad \Longleftrightarrow \quad \sum_{x \in G} M(x) f(x) v(x) = 0 \ \text{ for every polynomial } f \text{ with } \deg_i f < h_i \ (i \in J). \tag{5}$$

In particular, if $M \in \mathcal{B}_h$ and g is a polynomial with $\deg_i g \leq e_i < h_i$, then $gM \in \mathcal{B}_{h-e}$.

Proof. For f with $\deg f < n_i$, the coefficient of $X^{n_i - 1}$ in its Lagrange interpolant on S_i is $\sum_{a \in S_i} f(a) v_i(a)$; hence $\sum_a f(a) g(a) v_i(a) = 0$ whenever $\deg f < n_i - h_i$ and $\deg g < h_i$, which gives $\mathrm{diag}(v_i)\mathrm{RS}(S_i, h_i) \subseteq C_i^{\perp}$, and the dimensions agree. Then $\mathcal{B}_h^{\perp} = \bigcap_\ell C_\ell^{\perp} = \bigotimes_i C_i^{\perp} = \{v \cdot f|_G : \deg_i f < h_i\}$, which is (5). For the last claim apply (5) to gM and test functions f with $\deg_i f < h_i - e_i$: fg has $\deg_i(fg) < h_i$. □

Definition 4.5 (Interpolation with a bound; [4, Def. B.2])**.** Let $W \subseteq G$ and $w \geq 1$. *W admits interpolation with bound w* if every function $W \to \overline{\mathbb{F}}$ is the restriction of a polynomial f with $\deg_i f < w$ for all $i \in J$; equivalently, if for every $a \in W$ there is a *delta interpolant* L_a with these degree bounds and $L_a(b) = \mathbf{1}_{a=b}$ for $b \in W$. The empty set admits interpolation with every bound, and we then take $w = 0$ in sums of bounds.

Lemma 4.6 (Interpolation, inner generation and $\mathcal{B}$)**.** *Let $W \subseteq G$ and $1 \leq w \leq \min_i n_i$.*

(i) Interpolation with bound w passes to subsets of W.

(ii) W admits interpolation with bound w if and only if $\mathcal{B}_w \cap \overline{\mathbb{F}}^W = 0$, where $\mathcal{B}_w$ is taken for the codes $\mathrm{RS}(S_i, n_i - w)$ and $\overline{\mathbb{F}}^W$ denotes the arrays supported in W.

(iii) If $Z \subseteq G$ is inner-generated for $\mathcal{B}_w$ and U is the union of the coordinate lines of G contained in Z, then $Z \setminus U$ admits interpolation with bound w.

(iv) In one variable ($m = 1$), $W \subseteq S_1$ admits interpolation with bound w if and only if $|W| \leq w$.

Proof. (i) Restrict delta interpolants. (ii) Let $V_w = \{f : \deg_i f < w\}$; since $w \leq n_i$, evaluation $V_w \to \overline{\mathbb{F}}^G$ is injective, and by Lemma 4.4 $\mathcal{B}_w^{\perp} = \{v \cdot f|_G : f \in V_w\}$. W admits interpolation with bound w iff $V_w \to \overline{\mathbb{F}}^W$ is onto iff no nonzero $\phi \in \overline{\mathbb{F}}^W$ satisfies $\sum_{x \in W} \phi(x) f(x) = 0$ for all $f \in V_w$ iff (writing $\phi = vM$ with $M \in \overline{\mathbb{F}}^W$, v nowhere zero) no nonzero $M \in \overline{\mathbb{F}}^W$ is orthogonal to $\mathcal{B}_w^{\perp}$ iff

$\mathcal{B}_w \cap \overline{\mathbb{F}}^W = 0$. (iii) If $M \in \mathcal{B}_w$ is supported in $Z \setminus U$, inner generation writes M as a sum of line codewords on lines contained in Z, hence in U; so $\operatorname{supp} M \subseteq U \cap (Z \setminus U) = \emptyset$ and $M = 0$. Apply (ii). (iv) Lagrange interpolation, and a dimension count for the converse. □

Lemma 4.7 (Unions and separation; [4, Lemma B.3])**.** *(a) If $W \subseteq G$ admits interpolation with bound w and $z \in G \setminus W$, there is a polynomial of coordinate degrees $\le w$ vanishing on W and not at z. (b) If $W_1, \dots, W_s \subseteq G$ admit interpolation with bounds $w_1, \dots, w_s$, then $\bigcup_\nu W_\nu$ admits interpolation with bound $\sum_\nu w_\nu$.*

Proof. (a) Let L_a ($a \in W$) be delta interpolants. The polynomials $1 - \sum_{a \in W} L_a$ and $(X_i - a_i)L_a$ ($a \in W$, $i \in J$) have coordinate degrees $\le w$ and vanish on W. If all of them vanished at z, then $\sum_a L_a(z) = 1$ would give some $L_a(z) \neq 0$, and $(z_i - a_i)L_a(z) = 0$ for all i would give $z = a \in W$. (b) For a in the union put $\Lambda_a := \prod_{\nu:\, a \in W_\nu} L_a^{(\nu)} \cdot \prod_{\nu:\, a \notin W_\nu} D_a^{(\nu)} / D_a^{(\nu)}(a)$, where $D_a^{(\nu)}$ is a separating polynomial for W_ν and a from (a). Then $\Lambda_a(a) = 1$; if $b \neq a$ lies in the union, pick ν with $b \in W_\nu$: the factor $L_a^{(\nu)}$ (if $a \in W_\nu$) or $D_a^{(\nu)}$ (if $a \notin W_\nu$) vanishes at b. The coordinate degrees of Λ_a are at most $\sum_{\nu: a \in W_\nu}(w_\nu - 1) + \sum_{\nu: a \notin W_\nu} w_\nu < \sum_\nu w_\nu$, because at least one ν has $a \in W_\nu$. □

Lemma 4.8 (Jacobian; [4, Lemma B.5])**.** *Let $M \in \mathcal{B}_h$ on the m-dimensional grid G and $S = \operatorname{supp} M$. If $H \ge mB$, then no m polynomials of coordinate degrees $\le B$ vanishing on S have linearly independent gradients at a point of S.*

Proof. Suppose $F_1, \dots, F_m$ vanish on S, have coordinate degrees $\le B$, and have independent gradients at $z \in S$. Telescoping,

$$F_j(X) = F_j(X) - F_j(z) = \sum_{i=1}^{m} (X_i - z_i) A_{ji}(X), \qquad A_{ji} := \frac{F_j(z_{<i}, X_i, X_{>i}) - F_j(z_{<i}, z_i, X_{>i})}{X_i - z_i},$$

with $z_{<i} = (z_1, \dots, z_{i-1})$ and $X_{>i} = (X_{i+1}, \dots, X_m)$, where A_{ji} has degree $\le B - 1$ in X_i and $\le B$ in the other variables, and $A_{ji}(z) = \partial_i F_j(z)$ (the value at z_i of a univariate difference quotient is the formal derivative). Hence $D := \det(A_{ji})$ satisfies $\deg_i D \le (B-1) + (m-1)B = mB - 1 < h_i$ for all i, $D(z) = \det(\partial_i F_j(z)) \neq 0$, and $D(x) = 0$ for $x \in S \setminus \{z\}$, because $A(x)(x - z) = (F_j(x))_j = 0$ with $x - z \neq 0$. The parity test (5) with $f = D$ gives $0 = \sum_x M(x)D(x)v(x) = M(z)D(z)v(z) \neq 0$, a contradiction. □

Theorem 4.9 (Cylinder unions; [4, Thm. B.6]; its positive-dimensional case is (CG_m))**.** *Let $m \ge 1$ and $J = [m]$. For each nonempty $I \subseteq [m]$ let $W_I \subseteq S_I := \prod_{i \in I} S_i$ be a set admitting interpolation with bound w_I on the grid S_I (Definition 4.5; empty W_I are omitted). Put*

$$Z = \bigcup_I \Big(W_I \times \prod_{j \notin I} S_j \Big), \qquad R = \max\Big\{ 2,\ \sum_I w_I \Big\}.$$

If $H \ge 2mR$, then every $M \in \mathcal{B}_h$ with $\operatorname{supp} M \subseteq Z$ is a sum of line codewords on the free-direction lines of the cylinders*: the direction-j lines, $j \notin I$, contained in $\{a\} \times \prod_{j \notin I} S_j$ for some I and $a \in W_I$. In particular Z is inner-generated for $\mathcal{B}_h$. (Point cylinders, $I = [m]$, are allowed in [4]; this paper only uses the statement for positive-dimensional cylinders, $\emptyset \neq I \subsetneq [m]$, which is what ($\mathrm{CG}_m$) denotes.)*

Status of Theorem 4.9. The statement is [4, Thm. B.6] with one change: the standing hypothesis of their Appendix B, that each S_i is a subset of the norm-one set $\Sigma_i = \{x : x^{q_i+1} = 1\}$, is replaced by "arbitrary finite nonempty $S_i \subset \overline{\mathbb{F}}$" ($\overline{\mathbb{F}}$ algebraically closed of characteristic two). This replacement is our claim, not theirs; it is legitimate because no step of their proof refers to the sets beyond finiteness and $h_i \le |S_i|$, which we checked clause by clause. Their proof (about one page, plus Lemmas C.1–C.3 of their Appendix C) has the following structure, which we have read and whose arithmetic we have checked, but whose sheaf-theoretic steps we have not independently re-derived:

1. The cylinder union is modelled by the closed subscheme $Y = \bigcup_I W_I \times (\mathbb{P}^1)^{[m]\setminus I}$ of $X = (\mathbb{P}^1)^m$ with ideal sheaf $\mathcal{I}$.

2. For each $z \in X$ the ideal $\mathcal{J}_z$ of the union of the cylinder components through z is generated by square-free monomials in local coordinates; the Taylor resolution and the vanishing $H^q(X, \mathcal{O}_X(t-\epsilon)) = 0$ ($q > 0$, $t_i \ge 0$, $\epsilon \in \{0,1\}^m$) give $H^q(X, \mathcal{J}_z(t)) = 0$ for $q > 0$, $t_i \ge 0$.

3. Lemma 4.7 produces, for each z, a section s_z of $\mathcal{O}_X(R\mathbf{1})$ nonzero at z and vanishing on every component not through z; multiplication by s_z on $\mathcal{I}(t)$ factors through $\mathcal{J}_z(t)$, hence is zero on higher cohomology for $t_i \ge 0$.

4. The s_z have no common zero; $m+1$ of them give a Koszul complex that stays exact after tensoring with $\mathcal{I}(t)$; a descending induction on $q = m, \dots, 1$ shows $H^q(X, \mathcal{I}(t)) = 0$ whenever $t_i \ge a_q := (2(m-q)+1)R$. (We checked the two numerical steps: with $p = q+j-1$, $a_q - jR = a_p + (j-2)R \ge a_p$ for $j \ge 2$, and $a_1 = (2m-1)R \le 2mR - 1$.) Hence $H^1(X, \mathcal{I}(t)) = 0$ for $t_i \ge 2mR - 1$ and every section of $\mathcal{O}_Y(t)$ extends to X.

5. By (5), a functional on $\overline{\mathbb{F}}^Z$ annihilating the free-direction line codes is, on each cylinder grid, the evaluation of a polynomial of degree $< h_j$ in each free variable x_j; these polynomials are glued to a section of $\mathcal{O}_Y(h-\mathbf{1})$ (Chinese remainder theorem for the distributive family of local component ideals), extended to X by step 4 since $h_i - 1 \ge 2mR - 1$, and the extension is a polynomial with $\deg_i < h_i$ which, by (5) again, annihilates $\mathcal{B}_h$. Linear duality (Lemma 4.10 below) finishes the proof.

Nothing in this proof refers to the sets S_i beyond finiteness and $h_i \le |S_i|$; step 4 uses that the ground field is infinite. Steps 1–5, except for the final duality step (which is Lemma 4.10), are the only part of the present note that is neither classical nor re-derived here.

Lemma 4.10 (Extension form of Theorem 4.9)**.** *Let S_i, h_i, C_i be as above, let $W_I \subseteq S_I$ ($\emptyset \ne I \subseteq [m]$) be arbitrary sets and $Z = \bigcup_I W_I \times \prod_{j \notin I} S_j$ (no interpolation bounds and no lower bound on H are assumed). Then the conclusion of Theorem 4.9 for this configuration is equivalent to the following statement. Let $\psi\colon Z \to \overline{\mathbb{F}}$ be a function such that for every I and $a \in W_I$ the restriction of ψ to $\{a\} \times \prod_{j \notin I} S_j$ is the evaluation of a polynomial $g_{I,a}(X_{[m]\setminus I})$ with $\deg_j g_{I,a} < h_j$ for all $j \notin I$ ("cylinder data"). Then there is $g \in \overline{\mathbb{F}}[X_1, \dots, X_m]$ with $\deg_i g < h_i$ for all i and $g|_Z = \psi$.*

Proof. Let $L \subseteq \mathcal{B}_h \cap \overline{\mathbb{F}}^Z$ be the span of the free-direction line codewords. By linear algebra, $L = \mathcal{B}_h \cap \overline{\mathbb{F}}^Z$ iff every functional on $\overline{\mathbb{F}}^Z$ annihilating L is the restriction of a functional annihilating $\mathcal{B}_h$, i.e. (Lemma 4.4) of a function $v \cdot g|_G$ with $\deg_i g < h_i$. A function $\phi\colon Z \to \overline{\mathbb{F}}$ annihilates L iff on every free-direction line ℓ (direction j) of every cylinder, $\phi|_\ell \in C_j^\perp = \mathrm{diag}(v_j)\mathrm{RS}(S_j, h_j)$, iff $\psi := \phi/v$ restricted to ℓ is a polynomial of degree $< h_j$ in x_j (the other factors of v are constant on ℓ). Since a function on the grid $\prod_{j \notin I} S_j$ lying in $\mathrm{RS}(S_j, h_j)$ along every direction-j line, for all

$j \notin I$, lies in $\bigotimes_{j\notin I} \mathrm{RS}(S_j, h_j)$ (the intersection of the subspaces $\bigotimes_{k\neq j} \overline{\mathbb{F}}^{S_k} \otimes \mathrm{RS}(S_j, h_j)$ is the tensor product), this says exactly that ψ is cylinder data. The claim follows. □

Proposition 4.11 (Elementary cases of Theorem 4.9)**.** *(a) Suppose every cylinder is a coordinate hyperplane, i.e. $W_I = \emptyset$ unless $|I| = 1$; write $W_i := W_{\{i\}} \subseteq S_i$ and $w_i := w_{\{i\}}$. Then the conclusion of Theorem 4.9 holds under the weaker hypothesis $h_i \geq w_i$ for all i. In particular* (CG_1) *and* (CG_2) *hold.*

(b) (CG_3) *follows from its special case in which every cylinder is a line ($W_I = \emptyset$ unless $|I| = 2$).*

Proof. We use the extension form (Lemma 4.10).

(a) By Lemma 4.6(iv), $|W_i| \leq w_i \leq h_i$. Let $\lambda_a^{(i)}(X_i)$, $a \in W_i$, be the Lagrange polynomials of W_i (degree $< |W_i|$). For nonempty $T \subseteq [m]$ and $a_T \in \prod_{i\in T} W_i$, the sub-grid $\{a_T\} \times \prod_{j\notin T} S_j$ lies in the cylinder of every $i \in T$, and the restriction of ψ to it is the evaluation of a unique polynomial $\psi_{a_T}(X_{[m]\setminus T})$ with $\deg_j < h_j$ (restrict $g_{\{i\},a_i}$; uniqueness because $h_j \leq n_j$; for $T = [m]$, ψ_{a_T} is the constant $\psi(a_T)$). Put

$$g := \sum_{\emptyset\neq T\subseteq[m]} (-1)^{|T|+1} \sum_{a_T\in\prod_{i\in T} W_i} \psi_{a_T}(X_{[m]\setminus T}) \prod_{i\in T} \lambda_{a_i}^{(i)}(X_i)$$

(the Boolean sum of the interpolation projectors in the single variables). Each term has degree $< h_j$ in X_j for $j \notin T$ and $< |W_j| \leq h_j$ for $j \in T$, so $\deg_j g < h_j$. Fix $i = 1$ (say) and $a \in W_1$. At $X_1 = a$ the term $T = \{1\}$ equals $g_{\{1\},a}$; for $\emptyset \neq T' \subseteq \{2, \ldots, m\}$ the terms $T = T'$ and $T = T' \cup \{1\}$ cancel, because $\lambda_{a'}^{(1)}(a) = \mathbf{1}_{a'=a}$ and the restriction of $\psi_{a_{T'}}$ to $X_1 = a$ is $\psi_{(a,a_{T'})}$ (both are polynomials with $\deg_j < h_j$ agreeing with ψ on $\{(a, a_{T'})\} \times \prod_{j\notin T'\cup\{1\}} S_j$). Hence $g(a, X_2, \ldots, X_m) = g_{\{1\},a}$, and likewise in every direction. For $m \leq 2$ all positive-dimensional cylinders are hyperplanes and $2mR \geq w_i$, so (a) gives (CG_1), (CG_2). Point cylinders ($I = [m]$, base $W_{[m]}$ with bound $w_{[m]}$ and delta interpolants L_a of coordinate degrees $< w_{[m]}$) can be added: discard the points lying on hyperplanes of the configuration, put $\omega_i := \prod_{c\in W_i}(X_i - c)$, and replace g by $g + \prod_i \omega_i \cdot \sum_{a\in W_{[m]}} \frac{\psi(a)-g(a)}{\prod_i \omega_i(a_i)} L_a$, whose coordinate degrees are $< \max\{h_i, |W_i| + w_{[m]}\}$; so for $m \leq 2$ Theorem 4.9 holds in full under $h_i \geq w_i + w_{[m]}$.

(b) Let $m = 3$, with plane bases $W_i \subseteq S_i$ ($|W_i| \leq w_i$) and line bases $W_{ij} := W_{\{i,j\}} \subseteq S_i \times S_j$ with bounds w_{ij}, and $H \geq 6R$, $R \geq \sum_i w_i + \sum_{i<j} w_{ij}$. Let ψ be cylinder data on Z. *Step 1.* Remove from W_{12} every (a, b) with $a \in W_1$ or $b \in W_2$, and similarly for W_{13}, W_{23}: the removed lines lie in planes of the configuration, so Z and the cylinder data are unchanged, and interpolation bounds pass to subsets (Lemma 4.6(i)). *Step 2.* Let g_0 be the polynomial of part (a) for the plane data alone ($|W_i| \leq w_i \leq H \leq h_i$), so $\deg_i g_0 < h_i$ and $g_0 = \psi$ on the planes. *Step 3.* Put $\omega_i := \prod_{c\in W_i}(X_i - c)$ and $\psi_1 := \psi - g_0|_Z$, which vanishes on the planes. For $(a, b) \in W_{12}$ the function ψ_1 on the line $\{(a, b)\} \times S_3$ is the evaluation of $q_{ab}(X_3) := g_{\{1,2\},(a,b)} - g_0(a, b, X_3)$, of degree $< h_3$, and $q_{ab}(c) = \psi_1(a, b, c) = 0$ for $c \in W_3$ because (a, b, c) lies on the plane $X_3 = c$. So $q_{ab} = \omega_3 \tilde{q}_{ab}$ with $\deg \tilde{q}_{ab} < h_3' := h_3 - |W_3|$. Define $\tilde{\psi}$ on the union Z' of the lines by $\tilde{\psi}(a, b, x_3) := \tilde{q}_{ab}(x_3)/(\omega_1(a)\omega_2(b))$ (the denominator is nonzero by Step 1), and symmetrically for the other two directions. If a point $x = (a, b, c)$ lies on two lines, say over $(a, b) \in W_{12}$ and $(b, c) \in W_{23}$, then $a \notin W_1$, $b \notin W_2$, $c \notin W_3$ by Step 1, and both definitions give $\psi_1(x)/(\omega_1(a)\omega_2(b)\omega_3(c))$; so $\tilde{\psi}$ is well defined, and it is cylinder data for the lines-only configuration (W_{12}, W_{13}, W_{23}) with redundancies $h_i' := h_i - |W_i|$. *Step 4.* If $\sum_{i<j} w_{ij} \leq 1$ there is at most one line, say over $(a, b) \in W_{12}$, and $\tilde{g} := \tilde{q}_{ab}(X_3)/(\omega_1(a)\omega_2(b))$ extends $\tilde{\psi}$. Otherwise $R' := \max\{2, \sum_{i<j} w_{ij}\} \leq R - \max_i w_i$, hence $H' := \min_i h_i' \geq H - \max_i w_i \geq 6R - \max_i w_i \geq 6R'$, and the lines-only case of (CG_3) gives $\tilde{g}$ with $\deg_i \tilde{g} < h_i'$ and $\tilde{g}|_{Z'} = \tilde{\psi}$. *Step 5.* $g := g_0 + \omega_1\omega_2\omega_3\, \tilde{g}$

has $\deg_i g < h_i' + |W_i| = h_i$; on a plane $X_i = c \in W_i$ it equals $g_0 = \psi$; on the line over $(a,b) \in W_{12}$ it equals $g_0(a,b,X_3) + \omega_3(X_3)\tilde{q}_{ab}(X_3) = g_0(a,b,X_3) + q_{ab} = g_{\{1,2\},(a,b)}$, and likewise in the other directions. So $g|_Z = \psi$. □

Remark 4.12. The Boolean-sum argument of (a) needs commuting interpolation projectors, which is why it stops at hyperplane cylinders; for lines in three directions the projectors onto W_{12} and onto W_{23} do not commute, and the statement becomes a regularity bound for a reducible curve (a union of lines in $(\mathbb{P}^1)^3$ meeting in a prescribed pattern), which is what the cohomological argument of [4] supplies. We did not find an elementary substitute. In the application (§4.5, step (III)) the line bases are of the form $Z_F \setminus U_F$ for a bivariate polynomial F of coordinate degrees $\le d$, with interpolation bound $K_2' d$; a direct proof for this special class would also suffice.

4.5 The transported induction

We now give, in full, the argument of [4, §B.4] with Lemma 4.1 in place of their Lemma B.4, in the setting of Theorem 4.3: $P = 2^f$, $r \ge 2$, $m_1, \dots, m_r$ pairwise coprime, and for every $i \in [r]$ a nonempty $S_i \subseteq K_{m_i}$. For $\emptyset \ne J \subseteq [r]$ write $S_J = \prod_{i \in J} S_i$; for $I \subseteq J$ and a polynomial F in the variables X_J, we use the following notions on the grid S_J: a *flat with fixed set* I is a set $\{a\} \times S_{J \setminus I}$ with $a \in S_I$ (a point if $I = J$, a line if $|I| = |J| - 1$); it is *maximal in* Z_F if it is contained in Z_F and no flat with fixed set $I \setminus \{i\}$, $i \in I$, containing it is; $W_I(F) \subseteq S_I$ denotes the set of bases a of the maximal flats with fixed set I. Set

$$K_1' := 2, \qquad K_m' := m^2 2^{m+1}(K_{m-1}' + P + 1) \quad (m \ge 2),$$

an increasing sequence. For $m \ge 2$ and $H \ge K_m' d$ we shall use the inequalities

$$\begin{aligned} &\text{(A) } H - 2(m-1)d \ge 2^m K_{m-1}' d, \qquad \text{(B) } H - (m-1)d \ge m(P+m-1)d, \\ &\text{(C) } H \ge 2m\, 2^m K_{m-1}' d, \end{aligned} \tag{6}$$

which hold because $K_m' \ge 2^m K_{m-1}' + 2(m-1)$, $K_m' \ge m(P+m-1) + (m-1)$ and $K_m' \ge m 2^{m+1} K_{m-1}'$, all immediate from the recursion ($m^2 2^{m+1}(P+1) \ge 8m^2(P+1) \ge m(P+m-1) + (m-1)$). Note also that (C) gives $2^m K_{m-1}' d \le H \le n_i$ and (A) gives $(m-1)d + td < h_i$ for $t \le m-1$.

Proposition 4.13 (Transported induction)**.** *Let $m \ge 1$ and assume* ($\mathrm{CG}_{m'}$) *for $3 \le m' \le m$. Then for every $J \subseteq [r]$ with $|J| = m$, every choice of redundancies $1 \le h_i \le n_i$ $(i \in J)$ with $H = \min_{i \in J} h_i \ge K_m' d$, and every nonzero $E \in \overline{\mathbb{F}}_2[X_J]$ with coordinate degrees $\le d$, $d \ge 1$: every $M \in \mathcal{B}_h$ on S_J with $\operatorname{supp} M \subseteq Z_E$ is a sum of line codewords on coordinate lines contained in Z_E.*

Theorem 4.3 follows, since $K_r(P) = K_r' \ge K_{|J|}'$.

Proof. Induction on m, simultaneously for all J of size m and all redundancies (the sets S_i are fixed throughout; the induction hypothesis is applied to sub-grids S_I, $I \subsetneq J$, with the same sets and with redundancies of our choosing). Throughout, $|S_i| = n_i \ge h_i \ge H \ge K_m' d > d$ for $i \in J$.

Base case $m = 1$. Z_E is the set of roots of E in S_i, of size $\le d < h_i + 1$. A nonzero codeword of $C_i = \mathrm{RS}(S_i, n_i - h_i)$ has weight $\ge h_i + 1$, so $M = 0$, the empty sum.

Inductive step. Let $m \ge 2$ and assume the proposition for all $m' < m$ (with the constants $K_{m'}' \le K_{m-1}'$). Fix J, h, E, M as in the statement and enumerate $J = \{j_1, \dots, j_m\}$.

(I) Interpolation on bases. Let $F \ne 0$ be a polynomial in X_J with coordinate degrees $\le d$ and let $\emptyset \ne I \subseteq J$. Write $F = \sum_\beta f_\beta(X_I) X_{J \setminus I}^\beta$. Since $n_j > d$ for $j \in J \setminus I$, the flat $\{a\} \times S_{J \setminus I}$ lies in Z_F iff $F(a, X_{J \setminus I})$ vanishes on $S_{J \setminus I}$ iff $f_\beta(a) = 0$ for all β. As $\overline{\mathbb{F}}_2$ is infinite, there is a linear

combination $F_I = \sum_\beta \lambda_\beta f_\beta$ whose zero set on S_I is exactly the common zero set of the f_β (for each $a \in S_I$ outside the common zero set, the λ with $\sum_\beta \lambda_\beta f_\beta(a) = 0$ form a hyperplane; avoid these finitely many hyperplanes). F_I is a nonzero polynomial in X_I with coordinate degrees $\le d$ (nonzero because F does not vanish on S_J, so some flat is not in Z_F). A base $a \in Z_{F_I}$ is non-maximal iff for some $i \in I$ the flat with fixed set $I \setminus \{i\}$ through it lies in Z_F iff the direction-i line of S_I through a lies in Z_{F_I}; hence

$$W_I(F) = Z_{F_I} \setminus U_{F_I} \quad \text{(computed on the grid } S_I\text{)}, \qquad Z_F = \bigcup_{\emptyset \neq I \subseteq J} W_I(F) \times S_{J\setminus I},$$

the second identity because every point of Z_F lies in a maximal flat (free coordinates one at a time while staying inside Z_F). If $|I| < m$, the induction hypothesis applied to F_I on S_I with all redundancies equal to $w := K'_{m-1}d$ (legitimate: $w \le n_i$ by (6)(C), and $w \ge K'_{|I|}d$) shows that Z_{F_I} is inner-generated for $\mathcal{B}_w$ on S_I, so by Lemma 4.6(iii)

$$W_I(F) \text{ admits interpolation with bound } K'_{m-1}d \qquad (\emptyset \neq I \subsetneq J). \tag{7}$$

(I′) Few variables force interpolation. Let $F \neq 0$ have coordinate degrees $\le d$ and depend on fewer than m variables, and let $T \subseteq Z_E \setminus U_E$ with $F|_T = 0$. Then T admits interpolation with bound $2^m K'_{m-1}d$. Indeed, if F is constant then $T = \emptyset$. Otherwise let $\emptyset \neq I_0 \subsetneq J$ be the set of variables of F and apply (I) to F: since F does not involve the variables outside I_0, every flat inside Z_F can be freed in those directions, so $W_I(F) = \emptyset$ unless $I \subseteq I_0$, and $Z_F = \bigcup_{\emptyset \neq I \subseteq I_0} W_I \times S_{J\setminus I}$ with each $W_I = W_I(F)$ admitting interpolation with bound $K'_{m-1}d$ by (7) (as $I \subseteq I_0 \subsetneq J$), say with delta interpolants $L_a(X_I)$. Fix I and $a \in W_I$, and let $T_a := \{y \in S_{J\setminus I} : (a, y) \in T\}$. If $E(a, X_{J\setminus I}) \equiv 0$, the flat $\{a\} \times S_{J\setminus I}$ is a positive-dimensional flat inside Z_E, hence contained in U_E, so $T_a = \emptyset$. Otherwise $E_a := E(a, X_{J\setminus I})$ is a nonzero polynomial in $|J \setminus I| < m$ variables with coordinate degrees $\le d$, and $T_a \subseteq Z_{E_a} \setminus U_{E_a}$ (a complete line of $S_{J\setminus I}$ inside Z_{E_a} through y would give a complete line of S_J inside Z_E through $(a, y) \in T$, contradicting $T \cap U_E = \emptyset$). By the induction hypothesis at redundancy $K'_{m-1}d$ and Lemma 4.6(iii),(i), T_a admits interpolation with bound $K'_{m-1}d$, say with delta interpolants $L'_{a,b}(X_{J\setminus I})$, $b \in T_a$. The products $L_a(X_I)L'_{a,b}(X_{J\setminus I})$ are delta interpolants on $T \cap (W_I \times S_{J\setminus I})$ with coordinate degrees $< K'_{m-1}d$ (disjoint variable sets). These fewer than 2^m sets cover T, so Lemma 4.7(b) gives the claim.

(II) Restricting the support to U_E. For each $i \in J$ write $E = \sum_\beta e_{i,\beta}(X_{J\setminus\{i\}})X_i^\beta$ and choose, as in (I), a linear combination p_i of the $e_{i,\beta}$ whose zero set on $S_{J\setminus\{i\}}$ is exactly the set of bases of the direction-i lines contained in Z_E. Then $P_0 := \prod_{i\in J} p_i$ is a nonzero polynomial with coordinate degrees $\le (m-1)d$ whose zero set on S_J is exactly U_E. Put $N := P_0 M$. By Lemma 4.4 and (6)(A), $N \in \mathcal{B}_{h-(m-1)d\mathbf{1}} \subseteq \mathcal{B}_{H-(m-1)d}$, and $\operatorname{supp} N \subseteq Z_E \setminus U_E$. We claim $N = 0$; this gives $\operatorname{supp} M \subseteq U_E$.

Suppose $N \neq 0$. We construct recursively, for $t = 0, \dots, m-1$, polynomials Q_t with coordinate degrees $\le td$ and $\operatorname{supp}(Q_t N) \neq \emptyset$, starting with $Q_0 = 1$, together with $R_{t+1}, b_{t+1}, A_{t+1}$. Given Q_t, let F_t be a polynomial of minimal total degree in the nonempty set

$$\{G \neq 0 : \ G|_{\operatorname{supp}(Q_t N)} = 0, \ \deg_i G \le d \ \forall i \in J\} \ni E.$$

F_t depends on all m variables: otherwise (I′), applied to F_t and $T := \operatorname{supp}(Q_t N) \subseteq Z_E \setminus U_E$, shows that T admits interpolation with bound $2^m K'_{m-1}d \le \min n_i$, so $\mathcal{B}_{2^m K'_{m-1}d} \cap \overline{\mathbb{F}}^T = 0$ by Lemma 4.6(ii); but $Q_t N \in \mathcal{B}_{H-(m-1+t)d} \subseteq \mathcal{B}_{2^m K'_{m-1}d}$ by Lemma 4.4 and (6)(A) (as $t \le m-1$), and $Q_t N$ is a nonzero array supported in T, a contradiction. Now apply Lemma 4.1 to F_t in the direction $j := j_{t+1}$ and set $R_{t+1} := R_j$, $b_{t+1} := b_j$. By Lemma 4.1 and Remark 4.2(iii):

- $R_{t+1} \neq 0$ has coordinate degrees $\le Pd$ and vanishes on $\operatorname{supp}(Q_t N) \subseteq Z_{F_t}$ (by (a));

- $b_{t+1} \neq 0$ has coordinate degrees $\leq d$ and total degree smaller than that of F_t;
- for $x \in \operatorname{supp}(Q_t N)$: $\partial_i R_{t+1}(x) = 0$ for $i \neq j_{t+1}$ (by (b)), and $\partial_{j_{t+1}} R_{t+1}(x) \neq 0$ iff $b_{t+1}(x) \neq 0$ (by (c)).

Put $Q_{t+1} := Q_t b_{t+1}$ (coordinate degrees $\leq (t+1)d$). Minimality of F_t forbids b_{t+1} to vanish on all of $\operatorname{supp}(Q_t N)$, so $\operatorname{supp}(Q_{t+1}N) = \operatorname{supp}(Q_t N) \setminus Z_{b_{t+1}} \neq \emptyset$. Put $A_{t+1} := Q_t R_{t+1}$. Then: A_{t+1} has coordinate degrees $\leq (P+t)d \leq (P+m-1)d$; A_{t+1} vanishes on $\operatorname{supp} N$ (on $\operatorname{supp}(Q_t N)$ because R_{t+1} does, and on $\operatorname{supp} N \setminus \operatorname{supp}(Q_t N)$ because Q_t does); and at every $x \in \operatorname{supp}(Q_{t+1}N) \subseteq \operatorname{supp}(Q_t N)$ we have $Q_t(x) \neq 0$, $b_{t+1}(x) \neq 0$, $R_{t+1}(x) = 0$, hence $\nabla A_{t+1}(x) = Q_t(x) \nabla R_{t+1}(x)$ is a nonzero multiple of the coordinate vector $e_{j_{t+1}}$.

After m steps, $A_1, \ldots, A_m$ vanish on $\operatorname{supp} N$, have coordinate degrees $\leq B := (P+m-1)d$, and at any $z \in \operatorname{supp}(Q_m N) \neq \emptyset$ (which lies in $\operatorname{supp}(Q_s N)$ for every $s \leq m$) their gradients are nonzero multiples of the distinct vectors $e_{j_1}, \ldots, e_{j_m}$, hence linearly independent. Since $N \in \mathcal{B}_{H-(m-1)d}$ and $H - (m-1)d \geq mB$ by (6)(B), this contradicts Lemma 4.8. Hence $N = 0$.

(III) Gluing the lines. By (II), $\operatorname{supp} M \subseteq U_E = \bigcup_{\emptyset \neq I \subsetneq J} W_I(E) \times S_{J \setminus I}$ (a complete line in Z_E lies in a maximal flat with $|I| \leq m-1$, and each such flat is a union of complete lines). By (7), each $W_I(E)$, $\emptyset \neq I \subsetneq J$, admits interpolation with bound $K'_{m-1}d$. Apply Theorem 4.9 in the m directions of J to these fewer than 2^m families: $R = \max\{2, \sum_I w_I\} \leq 2^m K'_{m-1} d$ and $H \geq 2mR$ by (6)(C). (For $m = 2$ this is Proposition 4.11(a); for $m \geq 3$ it is the hypothesis (CG_m).) It writes M as a sum of line codewords on free-direction lines of the cylinders, which are complete coordinate lines contained in $U_E \subseteq Z_E$. This completes the induction. □

Step of Proposition 4.13	statement used	hypothesis it needs / where discharged
base case	RS distance	$d < h_i + 1$
(I): flats $\leftrightarrow$ coefficients	–	$n_j > d$ (from $H \geq K'_m d$)
(I): existence of F_I, p_i	infinite field	–
(I): bound (7)	induction hypothesis at redundancy $K'_{m-1}d$; Lemma 4.6(iii)	$K'_{\lvert I\rvert}d \leq K'_{m-1}d \leq n_i$ (C)
(I′)	(I), induction hypothesis, Lemma 4.6(i),(iii), Lemma 4.7(b)	fewer than 2^m pieces; $K'_{m-1}d \leq n_i$
(II): N, $Q_t N \in \mathcal{B}$.	Lemma 4.4	$(m-1+t)d < h_i$ (A)
(II): F_t uses all variables	(I′), Lemma 4.6(ii)	$H - 2(m-1)d \geq 2^m K'_{m-1}d$ (A); $2^m K'_{m-1}d \leq n_i$ (C)
(II): R_{t+1}, b_{t+1}	Lemma 4.1 (replaces [4, B.4])	$S_i \subseteq K_{m_i}$, m_i pairwise coprime; $K'' = P$
(II): contradiction	Lemma 4.8	$H - (m-1)d \geq m(P+m-1)d$ (B)
(III)	Theorem 4.9 = (CG_m); Prop. 4.11(a) if $m = 2$	bounds (7); $H \geq 2m\,2^m K'_{m-1}d$ (C)

4.6 From inner generation to product expansion; proof of Theorem 1.4

The three generic facts of §4.1, with proofs.

Lemma 4.14 ([4, Lemma 5.3])**.** *Let $K \geq 1$. If the support of every nonzero $x \in \mathcal{B}_h$ is contained in a set Z that is inner-generated for $\mathcal{B}_h$ and satisfies $|Z| \leq K |\operatorname{supp} x|$, then $(C_i)_{i \in J}$ is $\frac{1}{|J|K}$-product expanding.*

Proof. Write $x = \sum_{\ell \subseteq Z} a_\ell$, $a_\ell \in C_\ell$. Lines of a fixed direction are pairwise disjoint, so their total length inside Z is at most $|Z|$; summing over directions, $\sum_{\ell : a_\ell \neq 0} |\ell| \leq |J||Z| \leq |J|K|x|$, which is (1) with $A_i = \sum_{\ell \text{ in direction } i} a_\ell$. □

Lemma 4.15 ([4, Lemma 5.6])**.** *Let $F' \subseteq \overline{\mathbb{F}}$ be a subfield containing all S_i, $U \subseteq G$ and $Z = \mathrm{hull}_d(U)$ computed with $\mathcal{P}_d(F')$. (i) Z is unchanged if F' is replaced by any extension field. (ii) If $d+1 \leq n_i$ for all i, then $|Z| \leq |U| \prod_{i \in J} \frac{n_i}{d+1}$. (iii) If $Z \neq G$, there is a nonzero $E \in \mathcal{P}_d(\overline{\mathbb{F}})$ with $Z_E = Z$.*

Proof. Let $\mathrm{ev}_z \in \mathcal{P}_d(F')^*$ be evaluation at z and $W = \mathrm{span}\{\mathrm{ev}_u : u \in U\}$. Then $z \in Z$ iff ev_z vanishes on $\bigcap_{u \in U} \ker \mathrm{ev}_u$ iff $\mathrm{ev}_z \in W$ (finite dimension), i.e. iff adding the row of z to the evaluation matrix of U (monomial basis) does not increase its rank; ranks of matrices over F' are unchanged by field extension, which is (i). For (ii), choose $T_i \subseteq S_i$ of size $d+1$ uniformly and independently and let $T = \prod_i T_i$. Products of univariate Lagrange polynomials on the T_i form a basis of $\mathcal{P}_d$ dual to the evaluations at T; so the evaluations at $T \cap Z$ are linearly independent elements of W and $|T \cap Z| \leq \dim W \leq |U|$. Taking expectations, $|Z| \prod_i \frac{d+1}{n_i} = \mathbb{E}|T \cap Z| \leq |U|$. For (iii), let $V = \{f \in \mathcal{P}_d(\overline{\mathbb{F}}) : f|_U = 0\}$; by (i), each $z \in G \setminus Z$ defines a proper subspace $\{f \in V : f(z) = 0\}$, and a vector space over an infinite field is not a finite union of proper subspaces; any $E \in V$ outside their union works. □

Lemma 4.16 (Descent)**.** *Let $F' \subseteq \overline{\mathbb{F}}$ be a subfield containing all S_i, let $C_i = \mathrm{RS}(S_i, n_i - h_i)$ be defined over F', and let $Z \subseteq G$. If Z is inner-generated for $\mathcal{B}_h$ over $\overline{\mathbb{F}}$, then it is inner-generated for $\mathcal{B}_h$ over F'.*

Proof. Over either field consider $L = \sum_{\ell \subseteq Z} C_\ell \subseteq V = \{y \in \mathcal{B}_h : \mathrm{supp}\, y \subseteq Z\}$. L is the span of generators with entries in F'; V is the kernel of a matrix over F' (parity checks of $\mathcal{B}_h$, together with the coordinate projections outside Z). Ranks are unchanged by field extension, so $\dim_{F'} L = \dim_{\overline{\mathbb{F}}} L$ and $\dim_{F'} V = \dim_{\overline{\mathbb{F}}} V$; equality $L = V$ over $\overline{\mathbb{F}}$ gives $L = V$ over F'. □

Proof of Theorem 1.4 and Corollary 1.5. Rescalings are removed as in Theorem 1.3. Fix a nonempty $J \subseteq [r]$ and $0 \neq x \in \mathcal{B}_J$ over F. With $U = \mathrm{supp}\, x$, $H = \min_{i \in J} h_i \geq \beta \min_i n_i$, $d = \lfloor H/K_r(P) \rfloor$ and $Z = \mathrm{hull}_d(U)$ (over F, equivalently over $\overline{\mathbb{F}}_2$ by Lemma 4.15(i)): $d \leq H/2 \leq n_i/2$, so $d+1 \leq n_i$, and Lemma 4.15(ii) gives $|Z| \leq |U| \prod_{i \in J} n_i/(d+1) < |U|(K_r(P)R_0/\beta)^{|J|}$, because $n_i/(d+1) < K_r(P)n_i/H \leq K_r(P)R_0/\beta$. Z is inner-generated over $\overline{\mathbb{F}}_2$: if $Z = G_J$ this holds by definition (this includes $d = 0$, since the only constant vanishing on $U \neq \emptyset$ is 0); otherwise $d \geq 1$, Lemma 4.15(iii) gives $E \in \mathcal{P}_d(\overline{\mathbb{F}}_2) \setminus 0$ with $Z_E = Z$, and Theorem 4.3 applies since $h_i \geq H \geq K_r(P)d$. By Lemma 4.16, Z is inner-generated over F, and Lemma 4.14 gives product expansion of the subtuple J with constant $1/(|J|K) \geq \frac{1}{r}(\beta/(K_r(P)R_0))^r$, $K = (K_r(P)R_0/\beta)^{|J|}$. Nothing depends on F beyond $F \supseteq \bigcup S_i$.

For the corollary take $r = 3$, $R_0 = 1$, $\beta = \nu$: by §1.1 every code occurring in Hypothesis PE is a rescaled $\mathrm{RS}(S_i, k)$ with redundancy $n - k \geq \nu n$ (dimension $\geq \nu n$ for the duals), so Theorem 1.4 covers all 2^3 sign patterns and all subtuples; the only hypothesis is (CG_3), reduced to its lines-only case by Proposition 4.11(b). The recursion gives $K_2' = 32(P+3)$ and $K_3' = 144(33P+97)$. □

4.7 What is imported

Item in [4, §5, App. B]	uses the evaluation sets?	status here
Def. 5.1 (PE), Lemma 5.3	no	proved (Lemma 4.14)
Lemma 5.6 (hull size, field extension, defining E)	no	proved (Lemma 4.15)
Parity test (25), Def. B.2, Lemma B.3	no	proved (Lemmas 4.4, 4.6, 4.7)
Lemma B.4 (isolating a derivative)	**yes** (norm-one identity, CRT on the exponents a_i)	**replaced by Lemma 4.1** (machine-checked, Appendix A)
Lemma B.5 (Jacobian)	no	proved (Lemma 4.8)
Theorem B.6 (cylinder gluing on $(\mathbb{P}^1)^m$)	no (stated for norm-one subsets, proof set-independent)	stated exactly (Theorem 4.9); proved for $m \le 2$ and for hyperplane cylinders; *imported for* $m \ge 3$ (for Hypothesis PE: $m = 3$, where only the lines-only case is needed, Prop. 4.11)
§B.4 induction and constants	only via Lemma B.4 and "all grid coordinates are nonzero"	written out in full (Prop. 4.13); the latter hypothesis is not needed
Thm. 5.4 (hull ⇒ PE), descent to F	only through the size ratio 4^{r-1}	proved with ratio R_0 (Lemma 4.16, §4.6)

5 Discussion

5.1 Application to the companion construction

Hypothesis PE is [8, Assumption 2.1], which is the only unproved input of the main theorem of [8]. Corollary 1.5 establishes it under (CG_3), with the uniformity under extension of the scalar field that [8, Lemma 2.2] requires built into the statement: the constant depends only on P and ν. In [8] the hypothesis enters through the distance-transfer theorem [8, Thm. 7.4], where product expansion of all directional tuples at a vertex gives, by the local-to-global argument of Dinur–Lin–Vidick [6], a uniform robustness constant $\kappa(\rho)$ [8, Lemma 7.6] and hence the spectral target [8, (136)]. Only positivity and uniformity of ρ matter there: the constants of Corollary 1.5 are tiny ($\rho(2, 1/8) \approx 5 \cdot 10^{-17}$), which affects how large the extension degree r must be chosen in [8, §8] but not the asymptotic statement. Independently of [4], Theorem 1.3 settles all two-direction tuples of Hypothesis PE with the explicit constant $\nu^2/(8(P+5)^2)$, for any prime power P; in the local-to-global argument these are the inputs below the top degree, while the top degree needs the full triple, Theorem 1.4. The hypotheses of Theorems 1.3 and 1.4 are weaker than those of Hypothesis PE in three respects that cost nothing: unequal lengths with bounded ratio R_0, evaluation sets containing 0, and extension degrees with bounded pairwise gcd (constants with P replaced by P^g, resp. P^L, Remarks 2.2(iv) and 4.2(ii)). The specialization used in [8] (r odd, degrees $(r, r+1, r+2)$, $n = d_0\lfloor P^r/d_0 \rfloor$, $k = \lfloor n/7 \rfloor$) needs none of these. We stress that this paper proves the hypothesis and does not re-examine its use in [8].

5.2 Scope and open problems

The imported statement. Theorem 1.4 for $r = 3$ inherits any error in the proof of [4, Thm. B.6] for $m = 3$ (Theorem 4.9). All other components of the chain are proved here; the induction of [4, §B.4] is written out in full as Proposition 4.13 and its three inequalities are verified in (6). By Proposition 4.11, the dependency is on the lines-only case of Theorem 4.9 in three directions: given

three families of complete lines in a three-dimensional grid whose bases admit interpolation with bounds w_{12}, w_{13}, w_{23}, every element of $\mathcal{B}_h$ supported on their union is a sum of line codewords on these lines as soon as $H \geq 6\max\{2, \sum w\}$. An elementary proof of this statement, even for bases of the special form $Z_F \setminus U_F$ with F bivariate of coordinate degrees $\leq d$ that occur in Proposition 4.13, would make Hypothesis PE unconditional; we were not able to find one, and the Boolean-sum method of Proposition 4.11 does not apply because the interpolation projectors onto the three base sets do not commute.

Constants. The constants in Theorem 1.4 follow the bookkeeping of [4] with $K_r'' = P$ and are not optimized; the two-direction constant of Theorem 1.3 is polynomial in P and ν.

An alternative route. The construction of [8] could also be run on norm-one colour sets $S_i \subseteq \mu_{P^{m_i}+1} \subset \mathbb{F}_{P^{2m_i}}$ with the same degrees $m_i = r + i - 1$, for which product expansion is a theorem as stated in [4, Thm. 5.4] (for $P = 4$, where $q_i = 4^{m_i} = 2^{2(A+i)}$ with $A = r - 1$) and, by an independent method, in [7, Thm. 11.1.4] (any P; exponents fm_i with ratio bound P^2), for the full sets of sizes $P^{m_i} + 1$. This would remove the conditional status at the price of unequal local lengths (or of subsets, which are covered by [4, Thm. 5.7] but not by [7] as stated), a different character-cancellation lemma, and a Laurent-polynomial version of the Frobenius digit argument of [8, §4.5]. Conversely, the one-lemma substitution of this paper should also apply to the route of [7, Thm. 10.1.3], whose only set-dependent step is the grid-preserving "anisotropic transform" built from $z^{q_i} = z^{-1}$: the transform $F \mapsto F^{\tau_i}(X_1, \dots, X_i^P, \dots, X_r)$ of Lemma 1.1 has the same two properties (it preserves the grid $\prod_i K_{m_i}$ by (2), and it fixes no irreducible hypersurface that depends on X_i and on another variable, by the argument of Lemma 2.1). We have not checked their induction in detail and do not rely on it; a second, independent proof of Hypothesis PE along these lines would be valuable.

A Machine-checked components

The three new algebraic statements of this paper, Lemmas 1.1, 2.1 and 4.1, are formalized and machine-checked in Lean 4 [5] with Mathlib [11]. The formalization is attached to this paper as supplementary material, consisting of the Lean source file `CoprimeFrobenius.lean` (667 lines, 41 declarations, a single `import Mathlib`, no `sorry`), a `README.md` with the dictionary below and the build instructions, and the verification log `verification_log_2026-10-27.txt`. This appendix records what exactly is formalized, how the check was performed and what it does and does not establish; the paper's mathematics does not depend on it. The source file is organized in eight parts (A: the substitution $X_i \mapsto X_i^{w_i}$; B: derivatives of twisted polynomials in characteristic two; C: Frobenius selectors and grid exponent identities; D: the twist lemma, core form; E: choice of the exponents v, e; F: the polynomial b_j; G: Lemma 4.1 assembled; H: $Q \nmid \mathcal{T}Q$), followed by the verification hooks quoted in §A.3. Its header docstring refers to an earlier working version of this paper; the numbering of Lemmas 1.1, 2.1, 4.1 is the same there and here.

A.1 Dictionary

The grid in the Lean statements is the full product $\prod_i K_{m_i}$ of the subfields, as in Lemma 4.1(a),(c); the coefficient field is any perfect field of characteristic two, so $\overline{\mathbb{F}}_2$ is a special case.

in this paper	in `CoprimeFrobenius.lean`
polynomials in the variables X_i, $i \in J$	`MvPolynomial I F`, with `I` a finite type with decidable equality
coefficient field $\overline{\mathbb{F}}_2$	any `F` with `[Field F] [CharP F 2] [PerfectRing F 2]`
the grid $\prod_i K_{m_i}$, $P = 2^f$	`x : I -> F` with `x i ^ 2 ^ (f * m i) = x i` for all `i`
pairwise coprime m_i	`Pairwise (fun i k => Nat.Coprime (m i) (m k))`
substitution $X_i \mapsto X_i^{w_i}$	`scaleSub w`, the algebra endomorphism `bind₁ (fun i => X i ^ w i)`
$F = G((X_i^{2^{u_i}})_i)$	`scaleSub (fun i => 2 ^ u i) G`
$\sigma(c) = c^{2^{-e}}$	`invFrob e`, the ring homomorphism `(iterateFrobeniusEquiv F 2 e).symm`
$R_j = G^\sigma((X_i^{2^{v_i}})_i)$	`twist v e G`, defined as `scaleSub (fun i => 2 ^ v i) (map (invFrob e) G)`
b_j	`scaleSub (fun i => 2 ^ u i) (pderiv j G)`
∂_i, $\deg_i$, total degree	`pderiv i`, `degreeOf i`, `totalDegree`
$\mathcal{T}Q = Q^\sigma(X, Y^P)$ (§2)	`tw sigma P Q`, defined as `scaleSub ![1, P] (map sigma Q)` on `MvPolynomial (Fin 2) K`

A.2 The main declarations

Lemma 1.1. `exists_selector` is the Chinese remainder statement (for pairwise coprime `m` and any `w` there is `s` with `s ≡ w i [MOD m i]` for all `i`); `exists_selector_mul` is the generalized form with the common factor `f` (residues that agree modulo `f` are realized simultaneously modulo `f * m i`); and `pow_pow_congr` states that if $x^{q^m} = x$ and $a \equiv b \pmod m$ then $x^{q^a} = x^{q^b}$, which is the statement that $\varphi^s|_{K_m}$ depends only on s mod m.

Lemma 2.1. `not_dvd_tw` is stated for any field `K` that is perfect of characteristic `p` (`[Fact p.Prime] [CharP K p] [PerfectRing K p]`), any ring automorphism `sigma` of `K`, any `f ≥ 1`, and any irreducible `Q` with positive degree in both variables; it concludes that `Q` does not divide `tw sigma (p ^ f) Q`. Rendered in ASCII (Lean's Unicode notation replaced by its ASCII equivalents; the file itself uses the Unicode forms), the statement reads

```
theorem not_dvd_tw (sigma : RingEquiv K K) (f : Nat) (hf : 0 < f)
    (Q : MvPolynomial (Fin 2) K) (hQ : Irreducible Q)
    (h0 : 0 < degreeOf 0 Q) (h1 : 0 < degreeOf 1 Q) :
    Not (Dvd.dvd Q (tw (sigma : RingHom K K) (p ^ f) Q))
```

The proof follows Lemma 2.1: `pow_char_pow_eq_expand` identifies H^P with the expansion of the coefficientwise Frobenius image, the hypothesis $Q \mid \mathcal{T}Q$ is transported along the substitution $X \mapsto X'^P$, unique factorization (`dvd_prime_pow`) forces $Q(X'^P, Y)$ to be an associate of a power of H, and the degree comparison closes. The grid identity (2) is not stated separately in the file; it is an instance of `eval_scaleSub_map` (whose hypothesis $x_i^{w_i} = \tau(x_i^{u_i})$ is, for the selector $\sigma = \varphi^s$, the content of `pow_pow_congr`).

Lemma 4.1. `lemma_4_1` takes as input `f > 0`, pairwise coprime `m`, exponents `u`, a polynomial `G` and a direction `j` with `pderiv j G ≠ 0`, and produces `v`, `e` with `v j = 0` and `1 ≤ v i ≤ f` for `i ≠ j`, such that `twist v e G` satisfies (a)–(d) of Lemma 4.1 on every grid point, together with the three properties of b_j (nonzero, smaller total degree, no larger coordinate degrees). It is assembled from the following declarations: `twist_eval` for (a); `pderiv_twist_of_ne_zero` for (b); `pderiv_twist_of_eq_zero` for (c); `degreeOf_twist` for (d); `exists_twist_exponents` for the choice of `v` and `e`; and `totalDegree_scaleSub_pderiv_lt` together with `degreeOf_pderiv_le` for

the properties of b_j. The hypothesis `pderiv j G ≠ 0` is the maximality of u_j in Lemma 4.1 (some exponent of X_j in G is odd, so $\partial_j G \neq 0$ in characteristic two); the purely combinatorial step of extracting the maximal powers of two from the exponents of F to obtain such a pair (G, u) is not formalized. The formal statement is slightly more general than Lemma 4.1: the exponents u_i for $i \neq j$ are arbitrary, and the coefficient field need only be perfect of characteristic two. In the same ASCII rendering (with the type variable ι written `I`), the statement reads

```
theorem lemma_4_1 (f : Nat) (hf : 0 < f) (m : I -> Nat) (hm : forall i, Ne (m i) 0)
    (hcop : Pairwise (fun i k => Nat.Coprime (m i) (m k))) (u : I -> Nat)
    (G : MvPolynomial I F) (j : I) (hG : Ne (pderiv j G) 0) :
    exists v : I -> Nat, exists e : Nat,
      v j = 0 /\ (forall i, Ne i j -> 1 <= v i /\ v i <= f) /\
      (forall x : I -> F, (forall i, x i ^ 2 ^ (f * m i) = x i) ->
        eval x (twist v e G) = invFrob e (eval x (scaleSub (fun i => 2 ^ u i) G))) /\
      (forall i, Ne i j -> pderiv i (twist v e G) = 0) /\
      (forall x : I -> F, (forall i, x i ^ 2 ^ (f * m i) = x i) ->
        eval x (pderiv j (twist v e G))
          = invFrob e (eval x (scaleSub (fun i => 2 ^ u i) (pderiv j G)))) /\
      (forall i, Ne i j ->
        degreeOf i (twist v e G)
          <= 2 ^ f * degreeOf i (scaleSub (fun i => 2 ^ u i) G)) /\
      degreeOf j (twist v e G) <= degreeOf j (scaleSub (fun i => 2 ^ u i) G) /\
      Ne (scaleSub (fun i => 2 ^ u i) (pderiv j G)) 0 /\
      (scaleSub (fun i => 2 ^ u i) (pderiv j G)).totalDegree
        < (scaleSub (fun i => 2 ^ u i) G).totalDegree /\
      forall i, degreeOf i (scaleSub (fun i => 2 ^ u i) (pderiv j G))
        <= degreeOf i (scaleSub (fun i => 2 ^ u i) G)
```

in the context `{I F : Type*} [Fintype I] [DecidableEq I] [Field F] [CharP F 2] [PerfectRing F 2]`.

A.3 Verification record

The file was checked on October 27, 2026 with two independent toolchains of the Lean web editor (`live.lean-lang.org`, which runs the Lean server and kernel on the project's machines): "Latest Mathlib" with Lean `4.36.0-rc2`, and the "Stable Release" with Lean `4.35.0` and the matching Mathlib. In both runs the complete list of diagnostics consisted of three deprecation warnings (the lemmas `if_pos`/`if_neg` have been renamed in core Lean; the proofs are unaffected) and the output of the verification hooks at the end of the file:

```
'CoprimeFrobenius.lemma_4_1' depends on axioms: [propext, Classical.choice, Quot.sound]
'CoprimeFrobenius.not_dvd_tw' depends on axioms: [propext, Classical.choice, Quot.sound]
'CoprimeFrobenius.exists_selector_mul' depends on axioms: [propext, Classical.choice, Quot.sound]
"CoprimeFrobenius: all declarations checked"
```

There were no errors. The axiom lists are decisive: `#print axioms` reports every axiom a theorem ultimately depends on, and the three listed ones (propositional extensionality, the axiom of choice, and quotient soundness) are the standard foundation of classical mathematics in Lean, used throughout Mathlib. An incomplete proof would show the additional axiom `sorryAx`; the file contains no `sorry`, no `axiom` declaration, and no option affecting soundness (its only `set_option` disables an unused-variable linter). The SHA-256 digest of the checked file, recorded together with the full message lists in the attached `verification_log_2026-10-27.txt`, is

`34fbbb6e1efd1016c3bd31002147b1f5c426eabeb1c9032e8f3542b052adc0c4`.

To repeat the check, open `live.lean-lang.org`, select either of the two projects, paste the file and wait for the final message above; in a local Mathlib project, add the file and run `lake build CoprimeFrobenius`. The attached `README.md` lists the declarations and their correspondence with the statements of this paper.

A.4 Scope

The machine-checked part is exactly the algebraic novelty of this paper: Lemmas 1.1, 2.1, 4.1 and the properties of the polynomial b_j (`exists_selector`, `exists_selector_mul`, `not_dvd_tw`, `lemma_4_1`). Not formalized are the extraction of maximal powers of two preceding Lemma 4.1; the point count of Theorem 1.2, which uses the normalization of a plane curve and the pole-order bound (3); the Polishchuk–Spielman argument of §3; the inner-generation framework of §4, including the imported Theorem 4.9; and the deduction of Hypothesis PE. Accordingly the logical status of Hypothesis PE is as stated in §1.3: its two-direction case is proved, and its three-direction case is proved modulo (CG_3). What the formalization adds is that the three statements on which the reduction rests, and in particular the identities (a)–(d) of Lemma 4.1 that carry the whole dependence on the coprime-degree structure, hold exactly as stated, with no hidden hypothesis on the evaluation sets, the extension degrees, or the coefficient field beyond those displayed.

References

[1] M. Bafna, A. Li, and Q. Nguyen. Good quantum locally testable codes from product expansion. arXiv:2609.26735, 2026.

[2] M. Bafna and N. Vyas. Private PCPs from product expansion. ECCC TR26-150, 2026.

[3] E. Ben-Sasson and M. Sudan. Robust locally testable codes and products of codes. *Random Structures & Algorithms* 28(4):387–402, 2006.

[4] Y. Chen, M. M.-Y. Huang, Y. Liu, and E.-C. Tang. Cubical sheaf complexes with constant expansion with applications to asymptotically good qLTCs. arXiv:2609.28028, 2026.

[5] L. de Moura and S. Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, LNCS 12699, pp. 625–635. Springer, 2021.

[6] I. Dinur, T.-C. Lin, and T. Vidick. Expansion of high-dimensional cubical complexes with application to quantum locally testable codes. arXiv:2402.07476, 2024.

[7] W. Gay and F. G. Jeronimo. Asymptotically good quantum locally testable codes. arXiv:2609.20780, 2026.

[8] V. Guemard, S. J. S. Tan, and G. Zhu. Maximally parallelizable transversal non-Clifford gates on almost-good quantum LDPC codes and near-optimal magic state protocols. Manuscript, 2026.

[9] G. Kalachev and P. Panteleev. Two-sided robustly testable codes. arXiv:2206.09973, 2022.

[10] G. Kalachev and P. Panteleev. Maximally extendable product codes are good coboundary expanders. In *Proc. 66th IEEE Symposium on Foundations of Computer Science (FOCS 2025)*; arXiv:2501.01411.

[11] The mathlib Community. The Lean mathematical library. In *Proc. 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pp. 367–381.

[12] A. Polishchuk and D. A. Spielman. Nearly-linear size holographic proofs. In *Proc. 26th ACM Symposium on Theory of Computing (STOC 1994)*, pp. 194–203.

[13] M. Viderman. A combination of testability and decodability by tensor products. *Random Structures & Algorithms* 46(3):572–598, 2015.