

NP-Hardness of Approximating the Closest Vector Problem within a Polynomial Factor

Abstract

We prove that there is an absolute constant $c' > 0$ (one may take $c' = 1.8 \times 10^{-5}$) such that the promise problem $\text{GapCVP}_{n^{c'}}$ is NP-hard under deterministic polynomial-time Karp reductions: given a basis $B \in \mathbb{Q}^{n \times n}$ of a full-rank lattice $L \subset \mathbb{R}^n$ and a target $t \in \mathbb{Q}^n$, it is NP-hard to distinguish $\text{dist}_2(t, L) \leq 1$ from $\text{dist}_2(t, L) > n^{c'}$. The proof is a direct algebraic reduction from 3SAT through a Reed–Muller consistency lattice. All lemmas are stated and proved in full; external citations are only to: the Cook–Levin theorem, Bertrand’s postulate, the Delsarte–Goethals–MacWilliams duality for generalized Reed–Muller codes, the explicit Lang–Weil bounds of Cafure–Matera, and polynomial-time Hermite normal form computation.

Theorem. *With $c' := 1.8 \times 10^{-5}$, the promise problem $\text{GapCVP}_{n^{c'}}$ is NP-hard under deterministic polynomial-time Karp reductions.*

1 Definitions, conventions, parameters

1.1 Lattices and the promise problem

A *lattice* $L \subset \mathbb{R}^n$ is the set of integer combinations of a basis $B = (b_1, \dots, b_n)$ of $\mathbb{R}^n$; we write $\text{dist}_2(t, L) := \min_{v \in L} \|t - v\|_2$ (the minimum is attained). For a function $\gamma = \gamma(n) \geq 1$, the promise problem GapCVP_γ has instances (B, t) with $B \in \mathbb{Q}^{n \times n}$ nonsingular and $t \in \mathbb{Q}^n$; YES instances satisfy $\text{dist}_2(t, L(B)) \leq 1$, NO instances satisfy $\text{dist}_2(t, L(B)) > \gamma(n)$. A promise problem Π is *NP-hard under deterministic Karp reductions* if for every $L \in \text{NP}$ there is a deterministic polynomial-time computable map taking instances of L to instances of Π , mapping members to YES instances and non-members to NO instances. By the Cook–Levin theorem it suffices to reduce from 3SAT.

Theorem 1.1 (Main). *With $c' := 1.8 \times 10^{-5}$, $\text{GapCVP}_{n^{c'}}$ is NP-hard under deterministic polynomial-time Karp reductions.*

1.2 Measures, tables, codes, lattices of encodings

Fix a prime q . For a finite set Σ , $\mathbb{Z}[\Sigma]$ denotes the free abelian group with basis $(e_v)_{v \in \Sigma}$; its elements are called *integer measures* on Σ . For $\mu = \sum_v \mu_v e_v$ we write $\text{aug } \mu := \sum_v \mu_v$, $\|\mu\|_2^2 := \sum_v \mu_v^2$ and $\|\mu\|_1 := \sum_v |\mu_v|$. A map $\phi : \Sigma \rightarrow \Sigma'$ induces the pushforward $\phi_* : \mathbb{Z}[\Sigma] \rightarrow \mathbb{Z}[\Sigma']$, $e_v \mapsto e_{\phi(v)}$. For $\Sigma = \mathbb{F}_q^J$, marg_J denotes the pushforward along $\mathbf{v} \mapsto v_J$. We write $\bar{\mu} := \mu \bmod q$ and use the convention $0^0 := 1$.

A *table* on a finite domain X with J slots is a map $F : X \rightarrow \mathbb{Z}[\mathbb{F}_q^J]$; its coordinates are $F(x)_\mathbf{v} \in \mathbb{Z}$. A *code* $C \subseteq (\mathbb{F}_q^J)^X$ is an $\mathbb{F}_q$ -linear space of J -tuples of functions. For $c \in C$, $\text{Enc}(c)$ is the table $\text{Enc}(c)(x) := e_{c(x)}$, and

$$\mathcal{L}(C) := \mathbb{Z}\text{-span}\{\text{Enc}(c) : c \in C\} \subseteq \mathbb{Z}^{X \times \mathbb{F}_q^J}.$$

With $P := q^{2000}$, we say that a table F is C -structured if $F \in \mathcal{L}(C) + P\mathbb{Z}^{X \times \mathbb{F}_q^J}$.

$\text{RM}(m_0, e)$ denotes the space of polynomials in $\mathbb{F}_q[x_1, \dots, x_{m_0}]$ of total degree $\leq e$ (identified with their evaluation tables on $\mathbb{F}_q^{m_0}$ when convenient). A code on $X = \mathbb{F}_q^{m_0}$ has *coordinate degree* $\leq \bar{d}$ if every slot function of every codeword is the evaluation of a polynomial of total degree $\leq \bar{d}$.

Two standard facts will be used throughout.

Lemma 1.2 (Schwartz–Zippel and reduced evaluation). *(i) A nonzero $P \in \mathbb{F}_q[x_1, \dots, x_{m_0}]$ of total degree D has at most Dq^{m_0-1} zeros in $\mathbb{F}_q^{m_0}$.*

(ii) A nonzero polynomial all of whose individual degrees are $\leq q-1$ (in particular, any nonzero polynomial of total degree $< q$) does not vanish identically on $\mathbb{F}_q^{m_0}$; consequently two polynomials of total degree $< q$ defining the same function are equal.

Proof. (i) Induction on m_0 via the leading variable. (ii) The evaluation map is injective on the span of the monomials with individual degrees $\leq q-1$ (dimension count q^{m_0} against q^{m_0} points, triangularity via interpolation; alternatively, induction on m_0). $\square$

1.3 Parameters

The input is a 3CNF formula φ with N variables and at least one clause (clauses are ordered triples of literals; formulas with no clause, or with $N < N_0$ below, are handled trivially in §2.6). We fix:

- $m := 8$, $m' := 3m + 3 = 27$; $h := \lceil N^{1/m} \rceil$; $d := 60h$;
- $q :=$ the least prime $\geq d^{40}$; by Bertrand’s postulate $d^{40} \leq q < 2d^{40}$, so $h \leq q^{1/40}$ and $q \geq h^{40} \geq N^5$;
- $N_0 := 2^{2 \cdot 10^4}$, so that $N \geq N_0$ implies $q \geq N^5 \geq 2^{10^5}$; in particular *every explicit constant $\leq 2^{100}$ appearing below is $\leq q^{0.001}$* (the “absorption rule”, used silently in the ledger of §12.1);
- $H := \{0, 1, 2, \dots, h-1\} \subset \mathbb{F}_q$ (residues; $\{0, 1\} \subseteq H$, $|H| = h \geq 2$);
- $c := 10^{-3}$, $c_3 := 10^{-2}$; $g^2 := 16q^{2c}$;
- witness degrees $d_3 := m'h + 3(d+1) + d = 267h + 3$ and $d_6 := 2d + mh = 128h$;
- penalty weight $W := q^{1000}$, padding scale $P := q^{2000}$;
- windows $L_1 := \lceil q^{0.15} \rceil$, $L_2 := \lfloor q^{0.3} \rfloor$.

The variables of φ are identified with distinct points of H^m via a fixed injection ι_{var} (base- h digits; $h^m \geq N$). A clause $\mathcal{C} = (\ell_1, \ell_2, \ell_3)$ with $\ell_\iota = (v_\iota, b_\iota)$ ($b_\iota = 1$ iff the literal is negated) is encoded as

$$w(\mathcal{C}) := (\iota_{\text{var}}(v_1), \iota_{\text{var}}(v_2), \iota_{\text{var}}(v_3), 1 - b_1, 1 - b_2, 1 - b_3) \in H^{m'}.$$

We write points of $\mathbb{F}_q^{m'}$ as $w = (y_1, y_2, y_3, s)$ with $y_\iota \in \mathbb{F}_q^m$, $s = (s_1, s_2, s_3) \in \mathbb{F}_q^3$, and put $\pi_\iota(w) := y_\iota$. For a Boolean assignment α , the literal ℓ_ι of $\mathcal{C}$ is true iff $\alpha(v_\iota) = s_\iota$, where $s_\iota = 1 - b_\iota$ is the ι -th s -coordinate of $w(\mathcal{C})$. Let $\hat{\phi} : H^{m'} \rightarrow \{0, 1\}$ be the indicator of $\{w(\mathcal{C}) : \mathcal{C} \in \varphi\}$ and let $\hat{\Phi} \in \mathbb{F}_q[w]$ be its unique extension with all individual degrees $< h$ (Lemma 3.1); then $\hat{\Phi} \neq 0$ and $\deg \hat{\Phi} \leq m'(h - 1)$. Finally we set $Z_\kappa(w) := \prod_{\eta \in H} (w_\kappa - \eta)$ (degree h , vanishing on $\{w_\kappa \in H\}$); on $\mathbb{F}_q^m$ we use the same notation $Z_\kappa(x)$, $\kappa \leq m$.

2 The construction

2.1 Layers

A *layer* is a quadruple $\tau = (X_\tau, J_\tau, C_\tau, \sigma_\tau)$ consisting of a domain, a slot number, a code and an integer scaling. We use exactly four layers (the indices are legacy labels):

τ	X_τ	J_τ	C_τ	$\bar{d}_\tau$	σ_τ
1 (A -layer)	$\mathbb{F}_q^m$	1	$\{A : A \in \text{RM}(m, d)\}$	d	q^{26}
2 (triple)	$\mathbb{F}_q^{m'}$	3	$\{(A\pi_1, A\pi_2, A\pi_3) : A \in \text{RM}(m, d)\}$	d	$[q^{33/2}]$
3 (clause witness)	$\mathbb{F}_q^{m'}$	m'	$\{(B_1, \dots, B_{m'}) : B_\kappa \in \text{RM}(m', d_3)\}$	d_3	$[q^{33/2}]$
6 (Bool. witness)	$\mathbb{F}_q^m$	m	$\{(B_1, \dots, B_m) : B_\kappa \in \text{RM}(m, d_6)\}$	d_6	q^{26}

Here $\bar{d}_\tau$ is the coordinate degree of C_τ . With $\dim_\tau := \dim X_\tau$ we have $\sigma_\tau^2 q^{\dim_\tau} \in [q^{60}, 4q^{60}]$ for each τ , hence

$$\Delta_\varphi^2 := \sum_\tau \sigma_\tau^2 q^{\dim_\tau} \in [4q^{60}, 16q^{60}], \quad \Delta_\varphi \leq 4q^{30}. \quad (2.1)$$

2.2 Penalties

Each penalty is a $\mathbb{Z}$ -linear form ℓ_ρ on the joint table vector (F_1, F_2, F_3, F_6) with coefficients in $\{0, \pm 1\}$, together with a target value $\beta_\rho \in \{0, 1\}$. The rows are:

(P0) for each τ and each $x \in X_\tau$: $\text{aug } F_\tau(x) = 1$.

(P1) for each $w \in \mathbb{F}_q^{m'}$, $\iota \in \{1, 2, 3\}$ and $u \in \mathbb{F}_q$: $(\text{marg}_\iota F_2(w))_u - (F_1(\pi_\iota w))_u = 0$, i.e. the measure equality $\text{marg}_\iota F_2(w) = F_1(\pi_\iota w)$.

(P4) for each w and $u \in \mathbb{F}_q$: $((\Theta_w)_* F_2(w))_u - ((\Xi_w)_* F_3(w))_u = 0$, where

$$\Theta_w(\mathbf{v}) := \hat{\Phi}(w) \prod_{\iota=1}^3 (v_\iota - s_\iota), \quad \Xi_w(\mathbf{u}) := \sum_{\kappa=1}^{m'} Z_\kappa(w) u_\kappa.$$

(P6) for each $x \in \mathbb{F}_q^m$ and $u \in \mathbb{F}_q$: $(\theta_* F_1(x))_u - ((\Xi_x^m)_* F_6(x))_u = 0$, where $\theta(v) := v^2 - v$ and $\Xi_x^m(\mathbf{u}) := \sum_{\kappa=1}^m Z_\kappa(x) u_\kappa$.

Each row touches at most $2q^{m'}$ table entries (with coefficients ± 1). The number of rows is $2q^8 + 2q^{27}$ (P0) + $3q^{28}$ (P1) + q^{28} (P4) + q^9 (P6).

2.3 Coordinates, lattice, target

The coordinate set is $\mathcal{I} = \mathcal{I}_{\text{mass}} \sqcup \mathcal{I}_{\text{pen}}$: one *mass coordinate* per triple $(\tau, x, \mathbf{v})$ and one *penalty coordinate* per row ρ . In total,

$$D_{\text{tot}} = \underbrace{q^9 + q^{30} + q^{54} + q^{16}}_{\text{mass}} + \underbrace{2q^8 + 2q^{27} + 3q^{28} + q^{28} + q^9}_{\text{penalty}} \leq 2q^{54} \leq q^{55}. \quad (2.2)$$

For a table u supported on layer τ define the vector $\Gamma_\tau(u) \in \mathbb{Z}^{\mathcal{I}}$: the mass coordinates of layer τ carry $\sigma_\tau u$, the other mass coordinates carry 0, and penalty coordinate ρ carries $W\ell_\rho(u)$. The lattice L is generated by:

1. $\Gamma_\tau(b)$ for every vector b in the basis of $\mathcal{L}(C_\tau)$ provided by Lemma 2.1, for each τ ;
2. padding: $\sigma_{\tau(i)} P e_i$ for every mass coordinate i (of layer $\tau(i)$), and $P e_\rho$ for every penalty coordinate ρ .

The target $t^* \in \mathbb{Z}^{\mathcal{I}}$ is 0 on all mass coordinates and $W\beta_\rho$ on penalty coordinate ρ (so W on P0 rows and 0 on P1/P4/P6 rows). By the padding, L has full rank $n = D_{\text{tot}}$.

Every $v \in L$ has the form

$$v = \sum_{\tau} \Gamma_\tau(u_\tau) + P \cdot (\text{padding part}), \quad u_\tau \in \mathcal{L}(C_\tau), \quad (2.3)$$

and its mass coordinates read $\sigma_\tau F_\tau(x)_{\mathbf{v}}$ with $F_\tau := u_\tau + P\mu^{(\tau)}$ for integer tables $\mu^{(\tau)}$, while penalty coordinate ρ reads $W\ell_\rho(F) + P\nu_\rho$ for some $\nu_\rho \in \mathbb{Z}$ (one absorbs $W P \ell_\rho(\mu^{(\cdot)})$ into $P\nu_\rho$; note $P \mid WP$). In particular, **each F_τ is C_τ -structured**.

Lemma 2.1 (Explicit bases). *Given an $\mathbb{F}_q$ -basis $c_1, \dots, c_k$ of a code C on X (q prime), a $\mathbb{Z}$ -basis of $\mathcal{L}(C)$, with entries of bit-size polynomial in $|X|q^J$, is computable in time polynomial in $|X|q^J k$.*

Proof. For $0 \leq i \leq k$ let $C^{(i)} := \text{span}(c_1, \dots, c_i)$. Let σ_i^j ($0 \leq j \leq q-1$) be the coordinate permutation of $\mathbb{Z}^{X \times \mathbb{F}_q^J}$ given by $(\sigma_i^j u)_{x, \mathbf{v}} := u_{x, \mathbf{v} - j c_i(x)}$; then $\sigma_i^j \text{Enc}(c) = \text{Enc}(c + j c_i)$. Since q is prime, every $c' \in C^{(i)}$ equals $c + j c_i$ with $c \in C^{(i-1)}$ and $j \in \{0, \dots, q-1\}$; conversely all such elements lie in $C^{(i)}$. Hence

$$\mathcal{L}(C^{(i)}) = \sum_{j=0}^{q-1} \sigma_i^j \mathcal{L}(C^{(i-1)}).$$

Starting from the basis $\{\text{Enc}(0)\}$ of $\mathcal{L}(C^{(0)})$, iterate: given a basis B_{i-1} (of size $\leq |X|q^J$), the set $\{\sigma_i^j b : b \in B_{i-1}, 0 \leq j < q\}$ ($q|B_{i-1}|$ vectors) generates $\mathcal{L}(C^{(i)})$; compute the Hermite normal form of the stacked matrix to obtain B_i . Polynomial running time and bit-sizes follow from polynomial-time HNF algorithms (Kannan–Bachem). For the bit-size bound: each $\mathcal{L}(C^{(i)})$ is generated over $\mathbb{Z}$ by the 0–1 vectors $\{\text{Enc}(c) : c \in C^{(i)}\}$, so by Hadamard’s inequality every full-rank subdeterminant of this generating set has absolute value at most $N^{N/2}$ where $N := |X|q^J$; since the reduced Hermite normal form of a lattice is unique and has entries bounded by the largest such subdeterminant, each B_i has entries of bit-size $O(N \log N)$, independently of how B_{i-1} was computed, so no accumulation occurs across the $k \leq N$ iterations. $\square$

Lemma 2.2 (Restrictions; plane membership is automatic). *Let $Y \subseteq X$ and let $C|_Y$ denote the restricted code. Restriction of tables maps $\mathcal{L}(C)$ into $\mathcal{L}(C|_Y)$ and $P\mathbb{Z}^{X \times \cdot}$ into $P\mathbb{Z}^{Y \times \cdot}$. Hence a C -structured table restricts, on every affine plane $\Pi \subset X = \mathbb{F}_q^{m_0}$, to a $C|_\Pi$ -structured table. Likewise, any pushforward applied pointwise (marginals, ϕ_* with ϕ depending on the point) maps $\text{Enc}(c)$ to Enc of the image codeword and hence maps structured tables to structured tables for the image code. The same holds for domain-extended families of pointwise pushforwards: if $(\phi_z)_{z \in Z}$ is a family of maps $\mathbb{F}_q^J \rightarrow \mathbb{F}_q^{J'}$ and F is C -structured on X , then $\tilde{F}(x, z) := (\phi_z)_* F(x)$ is $\tilde{C}$ -structured on $X \times Z$ for $\tilde{C} := \{(x, z) \mapsto \phi_z(c(x)) : c \in C\}$ (an $\mathbb{F}_q$ -linear code whenever each ϕ_z is linear on values).*

Proof. Immediate from $\text{Enc}(c)|_Y = \text{Enc}(c|_Y)$ and $(\phi_z)_* \text{Enc}(c)(x) = e_{\phi_z(c(x))}$ (so the family map sends $\text{Enc}(c)$ to Enc of the image codeword on $X \times Z$), together with the $\mathbb{Z}$ -linearity of all maps involved (the $P\mathbb{Z}$ parts are preserved since pushforwards have integer matrices). $\square$

2.4 Output instance

The reduction computes all generators and the target exactly (evaluating $\hat{\Phi}$ by Lagrange interpolation over H), stacks the generators, computes a basis B_0 of L by HNF, computes the integer Δ_φ^2 and a rational R with $\Delta_\varphi \leq R \leq (1 + q^{-10})\Delta_\varphi$ (via the integer square root of $q^{20}\Delta_\varphi^2$), and outputs $(B_0/R, t^*/R)$.

2.5 Sizes and time

We have $q \leq 2(60(N^{1/8} + 1))^{40} = O(N^5)$ and $n \leq 2q^{54} = O(N^{271})$. All entries have bit-size $O(\log q) \cdot 2100 = \text{poly}(N)$ before HNF and polynomial bit-size after. The prime q is found by trial division in time $O(d^{80})$. Code dimensions are at most $m' \binom{d_3 + m'}{m'} \leq q$. The total running time is polynomial in N (of large but fixed degree), and the reduction is deterministic.

2.6 Degenerate inputs

If φ has no clause, output a fixed YES instance ($B = (1)$, $t = 0$, $n = 1$: distance $0 \leq 1$). If $N < N_0$, decide φ by brute force (constant time) and output either the fixed YES instance above or the fixed NO instance $B = (3)$, $t = 3/2$, $n = 1$ (distance $3/2 > 1 = n^{c'}$).

3 Completeness

Lemma 3.1 (Low-degree extension). *Every $f : H^M \rightarrow \mathbb{F}_q$ has a unique extension $F \in \mathbb{F}_q[w_1, \dots, w_M]$ with all individual degrees $< h$; and a polynomial with individual degrees $< h$ vanishing on H^M is 0.*

Proof. Existence: Lagrange interpolation, $F = \sum_{z \in H^M} f(z) \prod_\kappa \prod_{\eta \neq z_\kappa} \frac{w_\kappa - \eta}{z_\kappa - \eta}$. Vanishing: induction on M ; write $R = \sum_{j < h} R_j(w') w_M^j$; for each $w' \in H^{M-1}$ the univariate polynomial of degree $< h$ vanishes on h points, so all R_j vanish on H^{M-1} ; now induct. Uniqueness follows. $\square$

Lemma 3.2 (Division). *If $P \in \mathbb{F}_q[w_1, \dots, w_M]$ vanishes identically on H^M , then $P = \sum_{\kappa=1}^M Z_\kappa B_\kappa$ with $\deg B_\kappa \leq \deg P - h$.*

Proof. Divide P by the monic univariate $Z_1(w_1)$: since $Z_1 - w_1^h$ has degree $\leq h - 1$, each cancellation step replaces a term of total degree $\leq \deg P$ by terms of strictly smaller w_1 -degree and total degree $\leq \deg P$; hence $P = Z_1 B_1 + R_1$ with $\deg B_1 \leq \deg P - h$, $\deg R_1 \leq \deg P$ and $\deg_{w_1} R_1 < h$. Divide R_1 by Z_2 (this does not increase w_1 -degrees), and so on. The final remainder R has all individual degrees $< h$ and vanishes on H^M , hence $R = 0$ by Lemma 3.1. $\square$

Proposition 3.3 (Completeness). *If φ is satisfiable then $\text{dist}_2(t^*, L) \leq \Delta_\varphi$.*

Proof. Let α be a satisfying assignment, extended by 0 to all of H^m , and let $A \in \mathbb{F}_q[x_1, \dots, x_m]$ be its individual-degree- $< h$ extension; then $\deg A \leq m(h - 1) \leq 8h \leq d$, so $A \in \text{RM}(m, d)$. Set $F_1 := \text{Enc}(A)$ and $F_2 := \text{Enc}((A\pi_1, A\pi_2, A\pi_3))$.

Clause witness. The polynomial $P_\alpha := \hat{\Phi} \prod_\iota (A(y_\iota) - s_\iota)$ vanishes on $H^{m'}$: at $w \in H^{m'}$, either $\hat{\phi}(w) = 0 = \hat{\Phi}(w)$, or $w = w(\mathcal{C})$ for a clause $\mathcal{C}$ satisfied by α , so that some literal is true, i.e. $A(y_\iota) = s_\iota$ for some ι . By Lemma 3.2, $P_\alpha = \sum_\kappa Z_\kappa B_\kappa$ with $\deg B_\kappa \leq \deg P_\alpha - h \leq 27(h - 1) + 3 \cdot 8(h - 1) - h \leq 50h \leq d_3$. Set $F_3 := \text{Enc}((B_1, \dots, B_{m'}))$.

Booleanity witness. Since α is Boolean, $A^2 - A$ vanishes on H^m , so $A^2 - A = \sum_{\kappa \leq m} Z_\kappa B_\kappa^{(6)}$ with $\deg B_\kappa^{(6)} \leq 2m(h - 1) - h \leq 15h \leq d_6$. Set $F_6 := \text{Enc}(\mathbf{B}^{(6)})$.

All penalties hold exactly: (P0) each point carries a single unit atom; (P1) $\text{marg}_\iota e_{(A(y_1), A(y_2), A(y_3))} = e_{A(y_\iota)}$; (P4) both sides at w equal $e_{P_\alpha(w)}$; (P6) both sides at x equal $e_{(A^2 - A)(x)}$. The lattice vector $v := \sum_\tau \Gamma_\tau(F_\tau)$ (no padding) then matches t^* exactly on all penalty coordinates, and $\|v - t^*\|_2^2 = \sum_\tau \sigma_\tau^2 |X_\tau| = \Delta_\varphi^2$. $\square$

4 Soundness radius: coherent integer proofs

Definition 4.1. A *coherent integer proof* is a quadruple of tables (F_1, F_2, F_3, F_6) such that:

- (a) each F_τ is C_τ -structured;
- (b) all penalties (P0), (P1), (P4), (P6) hold exactly over $\mathbb{Z}$;
- (c) $\sum_{x \in X_\tau} \|F_\tau(x)\|_2^2 \leq g^2 q^{\dim_\tau}$ for each τ , where $g^2 = 16q^{2c}$.

Proposition 4.2. *If $\text{dist}_2(t^*, L) \leq q^c \Delta_\varphi$ then a coherent integer proof exists.*

Proof. Take $v \in L$ with $\|v - t^*\| \leq q^c \Delta_\varphi \leq q^{0.001} \cdot 4q^{30} < q^{31}$ and decompose it as in (2.3); let $F_\tau = u_\tau + P\mu^{(\tau)}$ be the integer tables read off the mass coordinates. Part (a) holds by construction. For (c): the mass part of $\|v - t^*\|^2$ is $\sum_\tau \sigma_\tau^2 \sum_x \|F_\tau(x)\|^2 \leq q^{2c} \Delta_\varphi^2$, and $\sigma_\tau^2 \geq q^{60 - \dim_\tau}$ together with $\Delta_\varphi^2 \leq 16q^{60}$ gives (c). For (b): pointwise, $|F_\tau(x)_\mathbf{v}| \leq \sqrt{g^2 q^{27.002}} \leq q^{14}$, so $|\ell_\rho(F)| \leq 2q^{27} \cdot q^{14} = 2q^{41}$ for every row. Penalty coordinate ρ of $v - t^*$ equals $W(\ell_\rho(F) - \beta_\rho) + P\nu_\rho$ with $|W(\ell_\rho(F) - \beta_\rho)| \leq q^{1000} \cdot 3q^{41} < q^{1042}$. If $\nu_\rho \neq 0$ the coordinate has absolute value $\geq P - q^{1042} > q^{31}$, a contradiction; so $\nu_\rho = 0$, and then $W|\ell_\rho(F) - \beta_\rho| < q^{31} < W$ forces $\ell_\rho(F) = \beta_\rho$. $\square$

The rest of the paper proves: *if φ is unsatisfiable, no coherent integer proof exists* (Corollary 11.3). Together with Propositions 3.3 and 4.2 this yields Theorem 1.1 (§12).

5 Moment machinery

Throughout §§5–8, “layer” means: a domain $\mathbb{F}_q^{m_0}$ ($2 \leq m_0 \leq 28$), a code C of coordinate degree $\leq \bar{d} \leq q^{0.04}$, and a C -structured table F with $\text{aug } F(x) = 1$ for all x . For $\mathbf{k} \in \mathbb{Z}_{\geq 0}^J$ define

$$\mu_{\mathbf{k}}(x) := \sum_{\mathbf{v}} \mathbf{v}^{\mathbf{k}} \bar{F}(x)_{\mathbf{v}} \in \mathbb{F}_q, \quad \text{where } \mathbf{v}^{\mathbf{k}} = \prod_j v_j^{k_j}.$$

Lemma 5.1 (Plane moment invariant). *Let $\Pi \subset \mathbb{F}_q^{m_0}$ be an affine plane ($\cong \mathbb{F}_q^2$), u a $C|_{\Pi}$ -structured table on Π , p a bivariate polynomial on Π , and suppose $\deg p + |\mathbf{k}|\bar{d} \leq 2q - 3$. Then $\sum_{s \in \Pi} p(s) \sum_{\mathbf{v}} \mathbf{v}^{\mathbf{k}} u_{s,\mathbf{v}} \equiv 0 \pmod{q}$.*

Proof. The expression is linear in u and vanishes mod q on the $P\mathbb{Z}$ -part (since $q \mid P$). On a generator $\text{Enc}(c|_{\Pi})$ it equals $\sum_{s \in \Pi} p(s) \prod_j c_j(s)^{k_j}$, a full-plane sum of a bivariate polynomial of degree $\leq 2q - 3$. For a monomial $y^a z^b$ we have $\sum_{(y,z) \in \mathbb{F}_q^2} y^a z^b = (\sum_y y^a)(\sum_z z^b)$, and $\sum_y y^a$ vanishes unless a is a positive multiple of $q - 1$ (for $a = 0$ the sum is $q \equiv 0$). A nonzero contribution therefore needs $a, b \geq q - 1$, i.e. total degree $\geq 2q - 2$. $\square$

Proposition 5.2 (Delsarte–Goethals–MacWilliams duality; quoted). *For $0 \leq \rho \leq 2(q - 1) - 1$ one has $\text{GRM}_q(\rho, 2)^{\perp} = \text{GRM}_q(2q - 3 - \rho, 2)$, where $\text{GRM}_q(\rho, 2) \subseteq \mathbb{F}_q^{\mathbb{F}_q^2}$ is the evaluation code of bivariate polynomials of degree $\leq \rho$.*

Lemma 5.3 (Lines to global). *Let $f : \mathbb{F}_q^{m_0} \rightarrow \mathbb{F}_q$ and let e satisfy $2e \leq q - 1$. If the restriction of f to every affine line agrees with a univariate polynomial of degree $\leq e$, then f agrees with a polynomial of total degree $\leq e$.*

Proof. Induction on m_0 ; the case $m_0 = 1$ is trivial. Fix distinct $u_0, \dots, u_e \in \mathbb{F}_q$. Each slice $f|_{x_{m_0}=u_j}$ satisfies the hypothesis on $\mathbb{F}_q^{m_0-1}$, hence by induction lies in $\text{RM}(m_0 - 1, e)$. For each x' , the axis-line restriction $u \mapsto f(x', u)$ is a polynomial of degree $\leq e$, so $f(x', u) = \sum_{i \leq e} c_i(x') u^i$ where each c_i is a fixed linear combination of the slices at $u_0, \dots, u_e$; hence $c_i \in \text{RM}(m_0 - 1, e)$ (reduced representatives, degree $\leq e$). Suppose $M := \max_{i: c_i \neq 0} (\deg c_i + i) > e$; note $M \leq 2e \leq q - 1$. For any ξ', b' , restricting to the line $u \mapsto (\xi' + ub', u)$ gives the polynomial $\sum_i c_i(\xi' + ub') u^i$ of degree $\leq M \leq q - 1$; by hypothesis it agrees on all q points with a polynomial of degree $\leq e < M$, and two polynomials of degree $\leq q - 1$ agreeing on $\mathbb{F}_q$ are identical; hence its u^M -coefficient vanishes. That coefficient equals $\sum_{i: \deg c_i + i = M} (c_i)_{\deg c_i}(b')$, where $(c_i)_D$ denotes the degree- D homogeneous part (terms with $\deg c_i + i < M$ contribute nothing at u^M , and the top coefficient of $c_i(\xi' + ub')$ in u is $(c_i)_{\deg c_i}(b')$, independently of ξ'). So a sum of nonzero homogeneous polynomials of *distinct* degrees $\leq e \leq q - 1$, with individual degrees $\leq q - 1$, vanishes identically on $\mathbb{F}_q^{m_0-1}$; by Lemma 1.2(ii) it is the zero polynomial, so each part is zero, contradicting $c_i \neq 0$. Hence $M \leq e$. $\square$

Proposition 5.4 (Global moment polynomials). *Let F be a layer as above and let $\mathbf{k}$ satisfy $2|\mathbf{k}|\bar{d} \leq q - 1$. Then there is a unique polynomial $P_{\mathbf{k}}$ of total degree $\leq |\mathbf{k}|\bar{d}$ with $P_{\mathbf{k}}(x) = \mu_{\mathbf{k}}(x)$ for all $x \in \mathbb{F}_q^{m_0}$. Moreover $P_0 = 1$.*

Proof. Fix a plane Π ; by Lemma 2.2, $F|_{\Pi}$ is $C|_{\Pi}$ -structured; by Lemma 5.1, $\mu_{\mathbf{k}}|_{\Pi}$ is orthogonal to $\text{GRM}_q(2q - 3 - |\mathbf{k}|\bar{d}, 2)$, hence by Proposition 5.2 lies in $\text{GRM}_q(|\mathbf{k}|\bar{d}, 2)$: every plane restriction of $\mu_{\mathbf{k}}$ is a bivariate polynomial of degree $\leq |\mathbf{k}|\bar{d}$. Every line lies in a plane ($m_0 \geq 2$), so every line restriction has degree $\leq e := |\mathbf{k}|\bar{d}$, and $2e \leq q - 1$; Lemma 5.3 produces the polynomial, and uniqueness follows from Lemma 1.2(ii). Finally $P_0 = 1$ by the augmentation $\text{aug } F \equiv 1$. $\square$

6 Algebraic toolkit

Lemma 6.1 (Hankel–valuation power-sum lemma). *Let $\mathbb{K}$ be a field with a valuation $v : \mathbb{K}^\times \rightarrow \mathbb{Z}$ (i.e. $v(ab) = v(a) + v(b)$ and $v(a + b) \geq \min(v(a), v(b))$). Let $\gamma_1, \dots, \gamma_\nu \in \mathbb{K}^\times$ be distinct with $v(\gamma_j) \leq -1$ and $v(\gamma_i - \gamma_j) \leq 2H$ ($i \neq j$, $H \geq 0$), and let $b_1, \dots, b_\nu \in \mathbb{K}$ with $v(b_j) = 0$. Let $\beta \geq 0$ and $p_l := \sum_j b_j \gamma_j^l$. Then there is l with $1 \leq l \leq \beta + 2H\nu + 2\nu - 1$ and $v(p_l) < -\beta$.*

Proof. Suppose $v(p_l) \geq -\beta$ for all $l \in \{\Lambda, \dots, \Lambda + 2\nu - 2\}$, where $\Lambda := \beta + 2H\nu + 1$. Over any commutative ring,

$$\det (p_{\Lambda+i+j})_{0 \leq i, j < \nu} = \left(\prod_j b_j \gamma_j^\Lambda \right) \prod_{i < j} (\gamma_i - \gamma_j)^2, \quad (6.1)$$

since the matrix equals $V^\top \text{diag}(b_j \gamma_j^\Lambda) V$ with $V_{kj} = \gamma_j^k$ the square Vandermonde matrix, and $\det V = \prod_{i < j} (\gamma_j - \gamma_i)$. The left-hand side, being a sum of ν -fold products of entries, has $v \geq -\nu\beta$. The right-hand side is nonzero and has

$$v(\text{RHS}) \leq \Lambda \sum_j v(\gamma_j) + 2 \sum_{i < j} v(\gamma_i - \gamma_j) \leq -\Lambda\nu + 2H\nu(\nu - 1) \leq -\Lambda\nu + 2H\nu^2 = -\nu\beta - \nu < -\nu\beta,$$

a contradiction. $\square$

Lemma 6.2 (Multivariate separation, SEP). *Let $\mathbb{K}$ be a field and let $\mathbf{p}_1, \dots, \mathbf{p}_M \in \mathbb{K}^J$ be distinct. Then there exist polynomials $\delta_1, \dots, \delta_M \in \text{span}_{\mathbb{K}}\{\mathbf{X}^{\mathbf{t}} : \mathbf{t} \in \{0, \dots, M-1\}^J\}$ with $\delta_u(\mathbf{p}_{u'}) = \delta_{uu'}$. Consequently: (i) the evaluation matrix $(\mathbf{p}_u^{\mathbf{t}})_{u, \mathbf{t} \in \{0..M-1\}^J}$ has full row rank M ; (ii) if $\sum_u w_u \mathbf{p}_u^{\mathbf{t}} = 0$ for all $\mathbf{t} \in \{0..M-1\}^J$ then all $w_u = 0$.*

Proof. Induction on J . For $J = 1$ this is Lagrange interpolation. For $J > 1$, group the points by their last coordinate, with values $z_1, \dots, z_p$ ($p \leq M$). Points within a group have distinct truncations in $\mathbb{K}^{J-1}$; take their inductive indicators (individual degrees $\leq M-1$) and multiply by $\prod_{u' \neq u} \frac{X_J - z_{u'}}{z_u - z_{u'}}$ (degree $\leq p-1 \leq M-1$), which vanishes on the other groups. Claims (i) and (ii) follow by applying the functional $\sum_u w_u(\cdot)(\mathbf{p}_u)$ to δ_{u_0} . $\square$

Lemma 6.3 (Class separation, CS). *Let $\mathbb{K}$ be a field and let $\{(u_s, P_s)\}_{s \leq S_1}$, $\{(v_r, Q_r)\}_{r \leq S_2}$ be finite weighted lists with the P_s pairwise distinct and the Q_r pairwise distinct elements of $\mathbb{K}$, and weights in $\mathbb{K}$. Let S be the number of distinct elements of $\{P_s\} \cup \{Q_r\}$. If $\sum_s u_s P_s^l = \sum_r v_r Q_r^l$ for $0 \leq l \leq S-1$, then the lists are equal as finitely supported measures: for every $R \in \mathbb{K}$, $\sum_{s: P_s=R} u_s = \sum_{r: Q_r=R} v_r$.*

Proof. Merge the lists into one list on the distinct elements $R_1, \dots, R_S$ with coefficients $c_i = (P\text{-net}) - (Q\text{-net})$; then $\sum_i c_i R_i^l = 0$ for $0 \leq l \leq S-1$, and the $S \times S$ Vandermonde matrix at distinct nodes is invertible. $\square$

7 The Scalar Decoding Lemma

Theorem 7.1 (Scalar decoding). *Let $2 \leq m_0 \leq 28$ and let $F : \mathbb{F}_q^{m_0} \rightarrow \mathbb{Z}[\mathbb{F}_q]$ satisfy:*

(i) *F is C -structured for a code C of coordinate degree $\leq \bar{d} \leq q^{0.04}$ (with $J = 1$);*

(ii) *$\text{aug } F(x) = 1$ for all x ;*

(iii) there is E_0 with $|E_0| \leq q^{m_0 - c_3}$ and $\sum_{x \notin E_0} \|F(x)\|_2^2 \leq \hat{g}^2 q^{m_0}$, where $16 \leq \hat{g}^2 \leq q^{0.02}$.

Then, with $\hat{t} := \lceil \hat{g}^2 q^{c_3} \rceil$ ($\leq 2q^{0.03}$), there exist $1 \leq r \leq \min(\hat{t}, 2\hat{g}^2)$ distinct polynomials $g_1, \dots, g_r$ of total degree $\leq \bar{d}$, nonzero integers $a_1, \dots, a_r$ with $\sum_j a_j = 1$ and $\sum_j a_j^2 \leq 2\hat{g}^2$, and a set $\mathcal{X} \supseteq E_0$ with $|\mathcal{X}| \leq 3q^{m_0 - c_3}$, such that

$$F(x) = \sum_j a_j e_{g_j(x)} \quad \text{for all } x \notin \mathcal{X},$$

and moreover $\sum_j \bar{a}_j g_j^l = P_l$ in $\mathbb{F}_q[\mathbf{x}]$ for all $0 \leq l \leq L_1 = \lceil q^{0.15} \rceil$, where P_l is the global moment polynomial of Proposition 5.4.

Proof. Write $t_x := |\text{supp } \bar{F}(x)|$ (≥ 1 by (ii), and $\leq \|F(x)\|_2^2$). All moment polynomials used below are within the range of Proposition 5.4 (indeed $2l\bar{d} \leq 2L_1\bar{d} \leq 2q^{0.19} \leq q - 1$).

Step 1 (rank collapse). Put $E_1 := E_0 \cup \{x : t_x > \hat{t}\}$; since $\hat{t} + 1 > \hat{g}^2 q^{c_3}$, Markov's inequality gives $|E_1| \leq 2q^{m_0 - c_3}$. Let $T := \hat{t}$ and $H_T := (P_{i+j})_{0 \leq i, j \leq T}$ over $\mathbb{F}_q[\mathbf{x}]$. For $x \notin E_1$ we have $H_T(x) = V^\top D V$ with $V \in \mathbb{F}_q^{t_x \times (T+1)}$ the Vandermonde matrix of $\text{supp } \bar{F}(x)$ and D the invertible diagonal matrix of weights; as $t_x \leq T + 1$, V has full row rank, so $\text{rank } H_T(x) = t_x$. Let r be the rank of H_T over $\mathbb{F}_q(\mathbf{x})$. Any nonzero $\rho \times \rho$ minor is a polynomial of degree $\leq 2\hat{t}(\hat{t} + 1)\bar{d} \leq 12q^{0.1} < q(1 - 2q^{-c_3})$, hence (Lemma 1.2(i)) is nonzero at some $x \notin E_1$, giving $\rho \leq t_x \leq \hat{t}$; so $r \leq \hat{t}$, and the pointwise rank bound $\leq r$ gives $t_x \leq r$ for $x \notin E_1$. All r -minors cannot vanish off E_1 (same degree bound), so some $x^* \notin E_1$ has $t_{x^*} = r$; there the leading principal minor $\Delta_r := \det(P_{i+j})_{i, j < r}$ is nonzero (square $V^\top D V$), so $\Delta_r \neq 0$ and $\deg \Delta_r \leq 2r^2\bar{d} \leq 8q^{0.1}$. Define the *good set* $\mathcal{G} := \{x \notin E_1 : \Delta_r(x) \neq 0\}$; for $x \in \mathcal{G}$ we get $r \leq \text{rank } H_T(x) = t_x \leq r$, so $t_x = r$. Also $|\mathcal{G}^c| \leq 2q^{m_0 - c_3} + 8q^{m_0 - 0.9}$, and $r \geq 1$ since $P_0 = 1$.

Step 2 (splitting). Let $\Psi(\mathbf{x}, X) := \det M$, where M is the $(r+1) \times (r+1)$ matrix with rows $(P_i, \dots, P_{i+r})$ for $i = 0, \dots, r - 1$ and last row $(1, X, \dots, X^r)$. Expansion along the last row gives $\text{lc}_X \Psi = \Delta_r$, $\deg_X \Psi = r$, $\deg_{\mathbf{x}} \Psi \leq r(2r - 1)\bar{d} \leq 8q^{0.1}$, and total degree $\delta_\Psi \leq D_0 := 9q^{0.1}$. For $x \in \mathcal{G}$ with support $\{v_1, \dots, v_r\}$, the coefficient vector $\mathbf{c}$ of $\chi_x(X) := \prod_i (X - v_i)$ satisfies $M(x, v_{i'})\mathbf{c} = 0$ (the moment rows because $\sum_i \bar{F}(x) v_i^l \chi_x(v_i) = 0$; the last row because $\chi_x(v_{i'}) = 0$), so $\Psi(x, v_{i'}) = 0$ for each i' ; since $\deg_X \Psi(x, \cdot) = r$ with nonzero leading coefficient, $\Psi(x, X) = \Delta_r(x) \chi_x(X)$: at good x , $\Psi(x, \cdot)$ has exactly r distinct roots, namely the support.

Claim: every irreducible factor of Ψ in $\mathbb{F}_q[\mathbf{x}, X]$ involving X has $\deg_X = 1$. Let $G \mid \Psi$ be irreducible with $n := \deg_X G \geq 1$ and $\delta := \deg G \leq D_0$. Specializing a factorization, for $x \in \mathcal{G}$ we have $\text{lc}_X(G)(x) \neq 0$ (the X -leading coefficients of the factors multiply to $\Delta_r(x) \neq 0$), and $G(x, \cdot)$ divides the squarefree, totally split $\Psi(x, \cdot)$, hence has exactly n distinct roots in $\mathbb{F}_q$. So the hypersurface $V(G) \subset \mathbb{A}^{m_0+1}$ satisfies $\#V(\mathbb{F}_q) \geq n|\mathcal{G}| \geq nq^{m_0}(1 - 3q^{-c_3})$.

- If G is absolutely irreducible, Cafure–Matera's explicit estimate (applicable since $q > 2\delta^4$: indeed $2(9q^{0.1})^4 \leq q^{0.42} < q$) gives

$$\#V(\mathbb{F}_q) \leq q^{m_0} + (\delta - 1)(\delta - 2)q^{m_0 - \frac{1}{2}} + 5\delta^{13/3}q^{m_0 - 1} \leq q^{m_0}(1 + q^{-0.29} + q^{-0.55}).$$

Hence $n \leq \frac{1+2q^{-0.29}}{1-3q^{-0.01}} < 2$, so $n = 1$.

- If G is irreducible but not absolutely irreducible, then over $\bar{\mathbb{F}}_q$ we have $G = c \prod_{i=1}^e G_i$ with $e \geq 2$ and Frobenius permuting the G_i transitively (otherwise an orbit product would be a proper rational factor). Any $\mathbb{F}_q$ -point p with $G_i(p) = 0$ also satisfies $G_{i'}(p) = 0$

0 for some $i' \neq i$ (apply σ with $G_i^\sigma \sim G_{i'}$; σ fixes p). So all rational points lie on $\bigcup_{i < i'} V(G_i) \cap V(G_{i'})$, a variety of dimension $\leq m_0 - 1$ and degree $\leq \delta^2$ (Bézout), whence $\#V(\mathbb{F}_q) \leq \delta^2 q^{m_0-1} \leq q^{m_0-0.79}$ (using the standard bound $\#W(\mathbb{F}_q) \leq \deg W \cdot q^{\dim W}$) — contradicting $\#V(\mathbb{F}_q) \geq \frac{1}{2}q^{m_0}$.

So $\Psi = c(\mathbf{x}) \prod_{j=1}^r (A_j X - B_j)$ with each factor irreducible ($A_j \neq 0$, $\gcd(A_j, B_j) = 1$); degrees of factors add, so $\deg A_j, \deg B_j \leq D_0 =: H_0$. Put $\gamma_j := B_j/A_j \in \mathbb{F}_q(\mathbf{x})$. If $\gamma_i = \gamma_j$ for some $i \neq j$, then the factors are proportional ($B_i A_j = B_j A_i$ together with coprimality), making $\Psi(x, \cdot)$ non-squarefree at good points with $A_i(x) \neq 0$ — which exist, since $c \prod_j A_j = \Delta_r$ is nonzero on $\mathcal{G}$; so the γ_j are pairwise *distinct*. Define the *very good set* $\mathcal{VG} := \{x \in \mathcal{G} : (B_i A_j - B_j A_i)(x) \neq 0 \ \forall i < j\}$; note that $\Delta_r(x) \neq 0$ already forces $c(x) \neq 0$ and all $A_j(x) \neq 0$. Then $|\mathcal{G} \setminus \mathcal{VG}| \leq \binom{r}{2} 2H_0 q^{m_0-1} \leq q^{m_0-0.83}$, and at $x \in \mathcal{VG}$ we have $\text{supp } \bar{F}(x) = \{\gamma_1(x), \dots, \gamma_r(x)\}$, r distinct values.

Step 3 (weights are constants). Solve the Vandermonde system $\sum_j \gamma_j^k W_j = P_k$ ($0 \leq k \leq r-1$) by Cramer's rule over $\mathbb{F}_q(\mathbf{x})$: after clearing denominators (columnwise, $\gamma_j^k = B_j^k A_j^{r-1-k}/A_j^{r-1}$), $W_j = U_j/V_0$ with $\deg U_j, \deg V_0 \leq D_A := r^2 H_0 + r\bar{d} \leq q^{0.17}$ and $V_0 \neq 0$ on $\mathcal{VG}$; uniqueness of the solution gives $W_j(x) = \bar{F}(x)_{\gamma_j(x)} \neq 0$ at every $x \in \mathcal{VG}$. Suppose some W_j is nonconstant. Let $M_1 := \lfloor q^{0.05} \rfloor$ and $R_{\text{sm}} := \{\rho \bmod q : \rho \in \mathbb{Z}, |\rho| \leq M_1\}$. The set of x where W_j is defined and takes a value in R_{sm} has size $\leq (2M_1 + 1)D_A q^{m_0-1} \leq q^{m_0-0.77}$ (each level set is contained in the zero set of $U_j - \lambda V_0 \not\equiv 0$), and V_0 vanishes at $\leq D_A q^{m_0-1}$ points. At every other $x \in \mathcal{VG}$, the integer $F(x)_{\gamma_j(x)} \equiv W_j(x) \notin R_{\text{sm}}$, so $|F(x)_{\gamma_j(x)}| > M_1$ and $\|F(x)\|^2 > M_1^2 \geq \frac{1}{4}q^{0.1}$. There are $\geq |\mathcal{VG}| - 2q^{m_0-0.77} \geq \frac{1}{2}q^{m_0}$ such points, all outside E_0 , giving mass $> \frac{1}{8}q^{m_0+0.1} > \hat{g}^2 q^{m_0}$ — contradicting (iii). So each W_j is a constant $\bar{a}_j \in \mathbb{F}_q^\times$.

Step 4 (polynomiality and degree). For $0 \leq l \leq L_1$, the rational function $\sum_j \bar{a}_j \gamma_j^l - P_l$ vanishes on $\mathcal{VG}$; its numerator over $\prod_j A_j^l$ has degree $\leq l(\bar{d} + rH_0) \leq L_1(\bar{d} + rH_0) \leq 19q^{0.28} < q(1 - 3q^{-c_3})$, so by Lemma 1.2,

$$\sum_j \bar{a}_j \gamma_j^l = P_l \quad \text{in } \mathbb{F}_q(\mathbf{x}), \quad 0 \leq l \leq L_1. \quad (7.1)$$

No finite poles. Fix an irreducible π and the π -adic valuation v_π ; let $S := \{j : v_\pi(\gamma_j) \leq -1\}$ and suppose $S \neq \emptyset$. For $i \neq j$, $v_\pi(\gamma_i - \gamma_j) \leq v_\pi(B_i A_j - B_j A_i) \leq \deg(B_i A_j - B_j A_i) \leq 2H_0$. Apply Lemma 6.1 ($\beta = 0$, $H = H_0$, weights $\bar{a}_j$): some $l \leq 2H_0|S| + 2|S| - 1 \leq 40q^{0.13} \leq L_1$ has $v_\pi(\sum_{j \in S} \bar{a}_j \gamma_j^l) < 0$. But by (7.1), $\sum_{j \in S} \bar{a}_j \gamma_j^l = P_l - \sum_{j \notin S} \bar{a}_j \gamma_j^l$ has $v_\pi \geq 0$: a contradiction. So every γ_j is a polynomial (a priori of degree $\leq H_0$).

Degree $\leq \bar{d}$. Let $S := \{j : \deg \gamma_j \geq \bar{d} + 1\}$, $\nu := |S|$, and suppose $\nu \geq 1$. Set $p_l^S := \sum_{j \in S} \bar{a}_j \gamma_j^l = P_l - \sum_{j \notin S} \bar{a}_j \gamma_j^l$, of degree $\leq l\bar{d}$ for $0 \leq l \leq L_1$. Take $\Lambda := 2\nu\bar{d} + 1$; the window satisfies $\Lambda + 2\nu - 2 \leq 2r\bar{d} + 2r \leq 10q^{0.07} \leq L_1$. Identity (6.1) for the S -family with offset Λ : the left-hand side has degree $\leq \nu(\Lambda + 2\nu - 2)\bar{d}$, while the right-hand side is nonzero of degree $\geq \Lambda \sum_{j \in S} \deg \gamma_j \geq \Lambda\nu(\bar{d} + 1)$. Hence $\Lambda(\bar{d} + 1) \leq (\Lambda + 2\nu - 2)\bar{d}$, i.e. $\Lambda \leq (2\nu - 2)\bar{d} < \Lambda$, a contradiction. So all $\deg \gamma_j \leq \bar{d}$; set $g_j := \gamma_j$.

Step 5 (lift and junk). Let $a_j \in (-q/2, q/2]$ lift $\bar{a}_j$ (so $a_j \neq 0$). Call $x \in \mathcal{VG}$ *clean* if $F(x) = \sum_j a_j e_{g_j(x)}$ as integer measures. At $x \in \mathcal{VG}$ we have $\bar{F}(x) = \sum_j \bar{a}_j e_{g_j(x)}$ with distinct atoms; if x is not clean, some entry of $F(x)$ differs from its canonical lift by a nonzero multiple of q , so $\|F(x)\|^2 \geq q^2/4$; hence at most $4\hat{g}^2 q^{m_0-2}$ points of $\mathcal{VG}$ are unclean. At clean x : $\sum_j a_j = \text{aug } F(x) = 1$ (exactly, over $\mathbb{Z}$) and $\|F(x)\|^2 = \sum_j a_j^2$; averaging the mass bound over

the clean points ($\geq q^{m_0}(1 - 3q^{-c_3}) \geq \frac{1}{2}q^{m_0}$ of them, all outside E_0) gives $\sum_j a_j^2 \leq 2\hat{g}^2$, and in particular $r \leq 2\hat{g}^2$. Let $\mathcal{X}$ be the complement of the clean set; collecting the estimates, $|\mathcal{X}| \leq 2q^{m_0-c_3} + 8q^{m_0-0.9} + q^{m_0-0.83} + 4q^{m_0-1.98} \leq 3q^{m_0-c_3}$. Finally, (7.1) with $\gamma_j = g_j$ is the stated polynomial identity. $\square$

8 The Tuple Decoding Lemma

The naive route — decode each slot marginal and place the support in the product grid — is *unsound*: marginals of signed measures can cancel. For instance, $e_{(0,0)} + e_{(1,1)} - e_{(0,1)} - e_{(1,0)} + e_{(2,2)}$ has both slot marginals equal to e_2 , hiding the values 0, 1. We repair this by a *formal mixing coordinate*: one extra domain variable θ , with the mix $\ell_\theta(\mathbf{v}) := v_1 + \theta v_2 + \dots + \theta^{J-1} v_J$, turns the tuple problem into a scalar problem one dimension up, with no loss of information.

Theorem 8.1 (Tuple decoding). *Let $2 \leq m_0 \leq 27$, $1 \leq J \leq 27$, and let $F : \mathbb{F}_q^{m_0} \rightarrow \mathbb{Z}[\mathbb{F}_q^J]$ satisfy: (i) F is C -structured with C of coordinate degree $\leq \bar{d} \leq q^{0.035}$; (ii) $\text{aug } F \equiv 1$; (iii) $\sum_x \|F(x)\|_2^2 \leq \hat{g}^2 q^{m_0}$ with $16 \leq \hat{g}^2 \leq q^{0.003}$. Then there exist $1 \leq r \leq 2\hat{g}^2$ distinct tuples $\gamma_j = (\gamma_j^1, \dots, \gamma_j^J)$ of polynomials of total degree $\leq \bar{d} + J - 1$, nonzero integers b_j with $\sum_j b_j = 1$ and $\sum_j b_j^2 \leq 2\hat{g}^2$, and a set $\mathcal{X}$ with $|\mathcal{X}| \leq 4q^{m_0-c_3/2}$, such that*

$$F(x) = \sum_j b_j e_{\gamma_j(x)} \quad (x \notin \mathcal{X}), \quad \text{and} \quad \sum_j \bar{b}_j \gamma_j^{\mathbf{k}} = P_{\mathbf{k}} \quad \text{in } \mathbb{F}_q[\mathbf{x}] \quad \text{for all } |\mathbf{k}| \leq L_2, \quad (8.1)$$

where $P_{\mathbf{k}}$ are the global moment polynomials of Proposition 5.4 and $\gamma^{\mathbf{k}} := \prod_j (\gamma_j^j)^{k_j}$.

Proof. Let $\hat{t} := \lceil \hat{g}^2 q^{c_3} \rceil$ and let $t_x := |\text{supp } F(x)|$ be the integer support size (this is the right count both for the ℓ_1 - ℓ_2 comparison and for the atom bookkeeping below; it dominates the mod- q support size). Each nonzero integer entry contributes ≥ 1 to $\|F(x)\|_2^2$, so $t_x \leq \|F(x)\|_2^2$ and Markov's inequality gives $|\{x : t_x > \hat{t}\}| \leq q^{m_0-c_3}$.

The θ -extension. Define $\tilde{F} : \mathbb{F}_q^{m_0+1} \rightarrow \mathbb{Z}[\mathbb{F}_q]$ by $\tilde{F}(x, \theta_0) := (\ell_{\theta_0})_* F(x)$. By Lemma 2.2 (pointwise pushforward along the point-dependent map ℓ_{θ_0}), $\tilde{F}$ is $\tilde{C}$ -structured, where $\tilde{C} := \{\tilde{c}(x, \theta_0) = \sum_j \theta_0^{j-1} c_j(x) : \mathbf{c} \in C\}$ is a linear code on $\mathbb{F}_q^{m_0+1}$ of coordinate degree $\leq \tilde{d} := \bar{d} + J - 1 \leq q^{0.04}$. Augmentation is preserved. As for mass, $\|\tilde{F}(x, \theta_0)\|_2^2 \leq \|F(x)\|_1^2 \leq t_x \|F(x)\|_2^2$, so with $E'_0 := \{x : t_x > \hat{t}\} \times \mathbb{F}_q$ (of size $\leq q^{(m_0+1)-c_3}$) we get $\sum_{(x, \theta_0) \notin E'_0} \|\tilde{F}\|^2 \leq \hat{t} \hat{g}^2 q^{m_0+1}$, and $16 \leq \hat{t} \hat{g}^2 \leq 2q^{0.016} \leq q^{0.02}$. Apply Theorem 7.1 to $\tilde{F}$ (domain dimension $m_0 + 1 \leq 28$): we obtain $\tilde{r} \leq \hat{t}' := \lceil \hat{t} \hat{g}^2 q^{c_3} \rceil \leq 2q^{0.03}$ distinct polynomials $\tilde{g}_j(\mathbf{x}, \theta)$ of degree $\leq \tilde{d}$, nonzero integers $\tilde{a}_j$, and $\tilde{\mathcal{X}}$ with $|\tilde{\mathcal{X}}| \leq 3q^{(m_0+1)-c_3}$, such that $\tilde{F} = \sum_j \tilde{a}_j e_{\tilde{g}_j}$ off $\tilde{\mathcal{X}}$.

Reconstruction. Call x *good* if: (a) $t_x \leq \hat{t}$; (b) $|\{\theta_0 : (x, \theta_0) \in \tilde{\mathcal{X}}\}| \leq q^{1-c_3/2}$; (c) for all $j \neq j'$, $\tilde{g}_j(x, \cdot) \neq \tilde{g}_{j'}(x, \cdot)$ as polynomials in θ . The failure sets have sizes: (a) $\leq q^{m_0-c_3}$; (b) $\leq 3q^{(m_0+1)-c_3}/q^{1-c_3/2} = 3q^{m_0-c_3/2}$ (Markov); (c) for each pair, some θ -coefficient of $\tilde{g}_j - \tilde{g}_{j'}$ is a nonzero polynomial in $\mathbf{x}$ of degree $\leq \tilde{d}$, giving $\leq \tilde{r}^2 \tilde{d} q^{m_0-1} \leq q^{m_0-0.9}$.

Fix a good x and let $S_x := \text{supp } F(x)$ (so $|S_x| = t_x$, with integer weights $w_{\mathbf{v}} := F(x)_{\mathbf{v}} \neq 0$). Call θ_0 *valid* if: $(x, \theta_0) \notin \tilde{\mathcal{X}}$; ℓ_{θ_0} is injective on S_x (this excludes the roots of at most $\binom{\hat{t}}{2}$ nonzero polynomials $\langle (1, \theta, \dots, \theta^{J-1}), \mathbf{v} - \mathbf{v}' \rangle$ of degree $\leq J - 1$, i.e. $\leq \hat{t}^2 J$ values); and the values $\tilde{g}_j(x, \theta_0)$ are pairwise distinct (excluding $\leq \tilde{r}^2 \tilde{d}$ values). At least $q - q^{1-c_3/2} - \hat{t}^2 J - \tilde{r}^2 \tilde{d} \geq q/2$ valid θ_0 exist. For valid θ_0 the two integer measures

$$\sum_{\mathbf{v} \in S_x} w_{\mathbf{v}} e_{\ell_{\theta_0}(\mathbf{v})} = \tilde{F}(x, \theta_0) = \sum_j \tilde{a}_j e_{\tilde{g}_j(x, \theta_0)}$$

have distinct atoms on each side, so the atom sets coincide with matching weights; in particular $t_x = \tilde{r}$, and there is a bijection $\sigma_{\theta_0} : S_x \rightarrow [\tilde{r}]$ with $\tilde{g}_{\sigma_{\theta_0}(\mathbf{v})}(x, \theta_0) = \ell_{\theta_0}(\mathbf{v})$ and $\tilde{a}_{\sigma_{\theta_0}(\mathbf{v})} = w_{\mathbf{v}}$. Fix $\mathbf{v} \in S_x$: by pigeonhole some j has $\sigma_{\theta_0}(\mathbf{v}) = j$ for at least $(q/2)/\tilde{r} \geq \frac{1}{4}q^{0.97} > \tilde{d}$ valid θ_0 , whence the polynomial identity in θ :

$$\tilde{g}_j(x, \theta) = \sum_{j=1}^J v_j \theta^{j-1}. \quad (8.2)$$

Distinct $\mathbf{v}$ yield distinct right-hand sides, hence distinct j (by (c)); since $|S_x| = t_x = \tilde{r}$, the assignment $\mathbf{v} \mapsto j(\mathbf{v})$ is a bijection, every $\tilde{g}_j(x, \cdot)$ has the form (8.2), and $w_{\mathbf{v}} = \tilde{a}_{j(\mathbf{v})}$.

Globalization. Write $\tilde{g}_j(\mathbf{x}, \theta) = \sum_{i \geq 0} \gamma_{j,i+1}(\mathbf{x}) \theta^i$ with $\gamma_{j,i} \in \mathbb{F}_q[\mathbf{x}]$ of degree $\leq \tilde{d}$. By (8.2), for every good x the coefficients with $i \geq J$ vanish; since the good set has $\geq q^{m_0}(1 - 5q^{-c_3/2})$ points and $\tilde{d} < q/2$, these coefficients vanish identically. Set $\gamma_j := (\gamma_{j,1}, \dots, \gamma_{j,J})$ (distinct tuples, degrees $\leq \tilde{d}$), $b_j := \tilde{a}_j$ and $r := \tilde{r}$. For every good x , $F(x) = \sum_j b_j e_{\gamma_j(x)}$ with the tuples $\gamma_j(x)$ pairwise distinct (by (c) and (8.2)). Hence at good x the augmentation gives $\sum_j b_j = 1$ over $\mathbb{Z}$, and $\|F(x)\|^2 = \sum_j b_j^2$; averaging the mass bound over good points gives $\sum_j b_j^2 \leq 2\hat{g}^2$ and $r \leq 2\hat{g}^2$. Let $\mathcal{X}$ be the non-good set: $|\mathcal{X}| \leq q^{m_0-c_3} + 3q^{m_0-c_3/2} + q^{m_0-0.9} \leq 4q^{m_0-c_3/2}$.

Moment identities. For $|\mathbf{k}| \leq L_2$ we have $2|\mathbf{k}|\tilde{d} \leq 2q^{0.335} \leq q - 1$, so $P_{\mathbf{k}}$ exists (of degree $\leq |\mathbf{k}|\tilde{d}$) and equals $\mu_{\mathbf{k}}$ everywhere; at good x , $\mu_{\mathbf{k}}(x) = \sum_j \bar{b}_j \gamma_j(x)^{\mathbf{k}}$; the difference of the two polynomials has degree $\leq |\mathbf{k}|\tilde{d} \leq q^{0.34} < q(1 - 4q^{-c_3/2})$ and vanishes off $\mathcal{X}$, hence is zero (Lemma 1.2). $\square$

9 Decoding the layers; converting penalties into class identities

Let (F_1, F_2, F_3, F_6) be a coherent integer proof (Definition 4.1). Apply Theorem 7.1 to F_1 (budget g^2 , $E_0 = \emptyset$) and Theorem 8.1 to F_2, F_3, F_6 (budget $g^2 \leq q^{0.003}$; coordinate degrees $d, d_3, d_6 \leq q^{0.031} \leq q^{0.035}$). This yields:

- F_1 : a list $\{(a_i, A_i)\}_{i \leq r_1}$ with A_i distinct, $\deg A_i \leq d$, $a_i \in \mathbb{Z} \setminus \{0\}$, $\sum_i a_i = 1$, $\sum_i a_i^2 \leq 2g^2$; $|\mathcal{X}_1| \leq 3q^{m-c_3}$.
- F_2 : $\{(b_j, \gamma_j)\}_{j \leq r_2}$, distinct triples, $\deg \gamma_j' \leq d_+ := d + 2$; $|\mathcal{X}_2| \leq 4q^{m'-c_3/2}$; identities (8.1) up to L_2 .
- F_3 : $\{(c_k, \mathbf{B}_k)\}_{k \leq r_3}$, $\deg B_{k\kappa} \leq d_3 + 26$; $|\mathcal{X}_3| \leq 4q^{m'-c_3/2}$.
- F_6 : $\{(f_k, \mathbf{D}_k)\}_{k \leq r_6}$, $\deg D_{k\kappa} \leq d_6 + 7$; $|\mathcal{X}_6| \leq 4q^{m-c_3/2}$.

All list sizes are $\leq 2g^2$, all weights are nonzero integers of absolute value $\leq \sqrt{2}g < q/2$ (hence nonzero mod q), and every *net* (sum of weights over a sublist) has absolute value $\leq 2g^2 < q/2$; hence **mod- q equalities of nets upgrade to $\mathbb{Z}$ -equalities**. *Class measures*: for a weighted list of polynomials, $\sum_j n_j [P_j]$ denotes the induced finitely supported $\mathbb{Z}$ - (or $\mathbb{F}_q$ -) valued measure on the polynomial ring.

Lemma 9.1 (Slot pinning). *For each ι : $\sum_j b_j [\gamma_j'] = \sum_i a_i [A_i \circ \pi_\iota]$ as $\mathbb{Z}$ -valued class measures on $\mathbb{F}_q[w]$.*

Proof. By (P1), $\text{marg}_l F_2(w) = F_1(\pi_l w)$ for all w . For $w \notin \mathcal{X}_2 \cup \pi_l^{-1}(\mathcal{X}_1)$ (a set of size $\leq 4q^{m'-c_3/2} + 3q^{m'-c_3} \leq 5q^{m'-c_3/2}$), taking l -th moments of both sides gives, mod q , $\sum_j \bar{b}_j \gamma_j^l(w)^l = \sum_i \bar{a}_i A_i(\pi_l w)^l$. For $0 \leq l \leq \lceil q^{0.004} \rceil$, both sides are polynomials of degree $\leq l d_+ \leq q^{0.035} < q(1 - 5q^{-c_3/2})$, so by Lemma 1.2 they are equal as polynomials. Since $\lceil q^{0.004} \rceil \geq r_1 + r_2$, Lemma 6.3 (over $\mathbb{K} = \mathbb{F}_q(w)$) gives equality of the $\mathbb{F}_q$ -class measures; nets upgrade to $\mathbb{Z}$. $\square$

Lemma 9.2 (P4 matching: clause composites). *Define $\text{Comp}_j := \hat{\Phi} \cdot \prod_l (\gamma_j^l - s_l) \in \mathbb{F}_q[w]$ and $G_k := \sum_{\kappa} Z_{\kappa} B_{k\kappa}$. Then $\sum_j \bar{b}_j [\text{Comp}_j] = \sum_k \bar{c}_k [G_k]$ as $\mathbb{F}_q$ -class measures. Consequently, **every class of the composite list whose net is nonzero mod q equals some G_k and hence vanishes identically on $H^{m'}$ (each Z_{κ} vanishes on $H^{m'}$).***

Proof. By (P4), $(\Theta_w)_* F_2(w) = (\Xi_w)_* F_3(w)$ for all w . For $w \notin \mathcal{X}_2 \cup \mathcal{X}_3$, the l -th moments give, mod q , $\sum_j \bar{b}_j \text{Comp}_j(w)^l = \sum_k \bar{c}_k G_k(w)^l$. Degrees: $\deg \text{Comp}_j \leq m'(h-1) + 3d_+ \leq 210h$ and $\deg G_k \leq h + d_3 + 26 \leq 270h$; for $0 \leq l \leq \lceil q^{0.004} \rceil (\geq r_2 + r_3)$ we have $l \cdot 270h \leq q^{0.036} < q(1 - 8q^{-c_3/2})$, so Lemma 1.2 upgrades these to polynomial identities, and Lemma 6.3 concludes. $\square$

Lemma 9.3 (P6 matching: a Boolean class exists). *There is $i^* \leq r_1$ with $a_{i^*} \neq 0$ and $A_{i^*}(x) \in \{0, 1\}$ for every $x \in H^m$.*

Proof. By (P6) and the same derivation (exceptional set $\mathcal{X}_1 \cup \mathcal{X}_6$, degrees $\leq \max(2d, h + d_6 + 7) \leq 130h$, window $\lceil q^{0.004} \rceil \geq r_1 + r_6$),

$$\sum_i \bar{a}_i [A_i^2 - A_i] = \sum_k \bar{f}_k [G_k^{(6)}], \quad G_k^{(6)} := \sum_{\kappa \leq m} Z_{\kappa} D_{k\kappa},$$

as $\mathbb{F}_q$ -class measures on $\mathbb{F}_q[x_1, \dots, x_m]$. Partition $\{1, \dots, r_1\}$ according to the polynomial $A_i^2 - A_i$; the part nets sum to $\sum_i \bar{a}_i = \bar{1} \neq 0$, so some part $\mathcal{P}$ has net $\neq 0 \pmod{q}$. By the measure equality, its polynomial equals some $G_k^{(6)}$, and every $G_k^{(6)}$ vanishes identically on H^m (each Z_{κ} does; the zero polynomial also qualifies). Pick any $i^* \in \mathcal{P}$: then $(A_{i^*}^2 - A_{i^*})|_{H^m} = 0$, i.e. A_{i^*} is Boolean on H^m , and $a_{i^*} \neq 0$. (The pairing $A \leftrightarrow 1 - A$ merging into one part is harmless: any member serves.) $\square$

Remark. Lemma 9.3 deliberately uses *only polynomial-identity class facts evaluated on H^m* , never table values at points of H^m : the subcube H^m (of size $h^m \leq q^{m/40}$) is far smaller than any exceptional set, so pointwise facts there would be worthless.

10 Moment membership, the extended window, and triple rigidity

Lemma 10.1 (Moment membership, MM). *Write $F_2 = \sum_{i \in I} c_i \text{Enc}(A'_i \pi) + P\mu$ with $c_i \in \mathbb{Z}$ and $A'_i \in \text{RM}(m, d)$ distinct (possible since F_2 is C_2 -structured; I may be astronomically large). Then for every $\mathbf{k}$ and every w ,*

$$\mu_{\mathbf{k}}(F_2)(w) \equiv \sum_i \bar{c}_i A'_i(y_1)^{k_1} A'_i(y_2)^{k_2} A'_i(y_3)^{k_3} \pmod{q}.$$

Moreover, if $2|\mathbf{k}|d \leq q - 1$, then as polynomials

$$P_{\mathbf{k}} = \sum_i \bar{c}_i \prod_{\iota} A'_i(y_{\iota})^{k_{\iota}}; \quad (10.1)$$

in particular $P_{\mathbf{k}}$ does not involve the s -variables, it involves the block y_{ι} only if $k_{\iota} > 0$, and $\deg_{y_{\iota}} P_{\mathbf{k}} \leq k_{\iota}d$ — **uniformly in the other components of $\mathbf{k}$** .

Proof. The first display follows from $\text{Enc}(A'\pi)(w) = e_{(A'(y_1), A'(y_2), A'(y_3))}$, the linearity of $\mu_{\mathbf{k}}$, and $q \mid P$. The right-hand side of (10.1) is a polynomial of total degree $\leq |\mathbf{k}|d < q$ computing the same function as $P_{\mathbf{k}}$ (of degree $\leq |\mathbf{k}|d < q$); by Lemma 1.2(ii) they are equal as polynomials, and the structural properties are inherited from each summand. $\square$

Lemma 10.2 (Extended-window identities, R+). *For all $\mathbf{k}$ with $|\mathbf{k}| \leq L_2 = \lfloor q^{0.3} \rfloor$,*

$$\sum_j \bar{b}_j \prod_{\iota} \gamma_j^{\iota}(w)^{k_{\iota}} = \sum_i \bar{c}_i \prod_{\iota} A'_i(y_{\iota})^{k_{\iota}} \quad \text{in } \mathbb{F}_q[w]. \quad (\text{R+})$$

Proof. Concatenate (8.1) for F_2 with (10.1); both are valid for $|\mathbf{k}| \leq L_2$ (indeed $2|\mathbf{k}|d \leq q - 1$ holds). $\square$

Theorem 10.3 (Triple rigidity, R2). $\sum_j b_j[\gamma_j] = \sum_i a_i[(A_i\pi_1, A_i\pi_2, A_i\pi_3)]$ as $\mathbb{Z}$ -valued class measures on tuples; equivalently, $r_2 = r_1$ and, after reindexing, $b_i = a_i$ and $\gamma_i = (A_i\pi_1, A_i\pi_2, A_i\pi_3)$.

Proof. Write $\theta_{\mathbf{k}}$ for the common polynomial in (R+).

Phase I (locality). *Claim:* for each slot ι and each variable ξ outside the block y_{ι} (i.e. in $y_{\iota'}$ with $\iota' \neq \iota$, or in s), $\deg_{\xi} \gamma_j^{\iota} = 0$ for all j . Take $\iota = 1$ (the other cases are symmetric, using the tag pairs (1,3) and (1,2)). Fix a foreign ξ and let $v := -\deg_{\xi}$, a valuation on $\mathbb{F}_q(w)$ with $v \leq 0$ on nonzero polynomials and $v = 0$ exactly on the ξ -free ones. Group the indices j by the pair $(\psi_u, \chi_u) := (\gamma_j^2, \gamma_j^3)$: say $\mathcal{N} \leq r_2$ distinct pairs. Fix a group u_0 . By Lemma 6.2 the evaluation matrix $(\psi_u^{t_2} \chi_u^{t_3})_{u, \mathbf{t} \in \{0, \dots, \mathcal{N}-1\}^2}$ over $\mathbb{F}_q(w)$ has rank $\mathcal{N}$; choose $\mathcal{N}$ independent columns, let $\Delta \neq 0$ be the corresponding minor, and solve by Cramer's rule for $c_{\mathbf{t}} = (\text{cofactor})/\Delta$ with $\sum_{\mathbf{t}} c_{\mathbf{t}} \psi_u^{t_2} \chi_u^{t_3} = \delta_{uu_0}$. Entry ξ -degrees are $\leq 2(\mathcal{N} - 1)d_+$, so $\deg_{\xi} \Delta$ and all cofactor degrees are $\leq 2r_2^2 d_+$. For every k with $k + 2r_2 \leq L_2$, grouping (R+) at $\mathbf{k} = (k, t_2, t_3)$ gives

$$Q_k := \sum_{j \in u_0} \bar{b}_j (\gamma_j^1)^k = \frac{1}{\Delta} \sum_{\mathbf{t}} (\text{cofactor})_{\mathbf{t}} \theta_{(k, t_2, t_3)}.$$

By Lemma 10.1, $\deg_{\xi} \theta_{(k, t_2, t_3)} \leq r_2 d$ (more precisely $\leq t_2 d$ if $\xi \in y_2$, $\leq t_3 d$ if $\xi \in y_3$, and $= 0$ if $\xi \in s$) — **uniformly in k** . Hence $v(Q_k) \geq -\bar{D}$ for all such k , where $\bar{D} := 5r_2^2 d_+ \leq q^{0.04}$. Let $S := \{j \in u_0 : \deg_{\xi} \gamma_j^1 \geq 1\}$ and suppose $S \neq \emptyset$, $\nu := |S|$. Within the group the γ_j^1 are pairwise distinct (the tuples are distinct and the pair is fixed). For $j \notin S$ the terms $\bar{b}_j (\gamma_j^1)^k$ are ξ -free, so $p_k := \sum_{j \in S} \bar{b}_j (\gamma_j^1)^k$ satisfies $v(p_k) \geq -\bar{D}$ for all $k \leq L_2 - 2r_2$. Apply Lemma 6.1 with $H = 0$ (differences are nonzero polynomials, so $v \leq 0$), $\beta = \bar{D}$ and weights $\bar{b}_j \in \mathbb{F}_q^{\times}$: some $l \leq \bar{D} + 2\nu - 1 \leq q^{0.05} \leq L_2 - 2r_2$ has $v(p_l) < -\bar{D}$, a contradiction. So $S = \emptyset$. Applying this to all foreign ξ and all slots: $\gamma_j^{\iota} = G_j^{\iota}(y_{\iota})$ with $G_j^{\iota} \in \mathbb{F}_q[y_{\iota}]$ of degree $\leq d_+$.

Phase II (coupling). Substitute $y_2 := y_1$ into (R+) (a ring homomorphism, so identities are preserved). The right-hand side becomes $\sum_i \bar{c}_i A'_i(y_1)^{k_1+k_2} A'_i(y_3)^{k_3}$, a function of (k_1+k_2, k_3) only. Subtracting the identities for (k_1, k_2, k_3) and (k_1-1, k_2+1, k_3) (with $k_1 \geq 1$),

$$\sum_j \bar{b}_j (G_j^1(y_1) - G_j^2(y_1)) G_j^1(y_1)^{k_1-1} G_j^2(y_1)^{k_2} G_j^3(y_3)^{k_3} = 0.$$

The nodes $\mathbf{n}_j := (G_j^1(y_1), G_j^2(y_1), G_j^3(y_3)) \in \mathbb{F}_q(y_1, y_3)^3$ are pairwise distinct (coordinatewise equality forces equality of the polynomial triples, i.e. $j = j'$). Taking $(k_1 - 1, k_2, k_3) = \mathbf{t} \in \{0, \dots, r_2 - 1\}^3$ (all with $|\mathbf{k}| \leq 3r_2 \leq L_2$), Lemma 6.2(ii) gives $\bar{b}_j(G_j^1 - G_j^2) = 0$ for every j ; since $\bar{b}_j \neq 0$, $G_j^1 = G_j^2$. The substitution $y_3 := y_1$ likewise gives $G_j^1 = G_j^3$. So every tuple is coupled: $\gamma_j = (G_j\pi_1, G_j\pi_2, G_j\pi_3)$ with $G_j := G_j^1$ pairwise distinct.

Phase III (identification). Lemma 9.1 with $\iota = 1$ reads $\sum_j b_j[G_j(y_1)] = \sum_i a_i[A_i(y_1)]$ with all atoms distinct on each side; hence the weighted sets coincide: $\{(b_j, G_j)\} = \{(a_i, A_i)\}$. $\square$

11 Endgame

Lemma 11.1 (Injectivity of composites). *The map $A \mapsto \text{Comp}_A := \hat{\Phi} \cdot \prod_{\iota=1}^3 (A(y_\iota) - s_\iota)$ is injective on $\mathbb{F}_q[x_1, \dots, x_m]$ (for arbitrary degrees), and $\text{Comp}_A \neq 0$.*

Proof. We have $\hat{\Phi} \neq 0$ (as φ has a clause), and each factor $A(y_\iota) - s_\iota$ is a nonzero polynomial, monic of degree 1 in s_ι and hence irreducible in the UFD $\mathbb{F}_q[w]$ (a factorization would have a unit degree-0-in- s_ι factor). If $\text{Comp}_A = \text{Comp}_{A''}$, cancel $\hat{\Phi}$: the irreducible factors of $\prod_\iota (A(y_\iota) - s_\iota)$ match those of $\prod_\iota (A''(y_\iota) - s_\iota)$ up to scalars. Only the ι -th factor on each side involves s_ι (the three variable blocks (y_ι, s_ι) are disjoint), so $A(y_1) - s_1 = c(A''(y_1) - s_1)$ for a scalar c ; comparing s_1 -coefficients gives $c = 1$, hence $A = A''$. $\square$

Theorem 11.2 (Extraction). *If a coherent integer proof exists, then φ is satisfiable.*

Proof. Decode as in §9. By Theorem 10.3, $r_2 = r_1$ and the layer-2 classes are $\{(a_i, (A_i\pi_1, A_i\pi_2, A_i\pi_3))\}_{i \leq r_1}$; thus the composite list of Lemma 9.2 is $\{(a_i, \text{Comp}_{A_i})\}_{i \leq r_1}$.

(a) Every class is clause-good. By Lemma 11.1 the Comp_{A_i} are pairwise distinct, so each class of the composite partition is a singleton $\{i\}$ with net a_i , and $\bar{a}_i \neq 0$ (since $0 < |a_i| < q/2$). By Lemma 9.2, **for every** i the polynomial $\text{Comp}_{A_i} = \hat{\Phi} \prod_\iota (A_i(y_\iota) - s_\iota)$ vanishes identically on $H^{m'}$.

(c') A Boolean class exists. By Lemma 9.3 there is i^* with $a_{i^*} \neq 0$ and A_{i^*} Boolean on H^m .

Combination. Define $\alpha(v) := A_{i^*}(\iota_{\text{var}}(v)) \in \{0, 1\}$ for each variable v of φ . Let $\mathcal{C}$ be any clause and $w := w(\mathcal{C}) \in H^{m'}$. Then $\hat{\Phi}(w) = \hat{\phi}(w) = 1$, so by (a) applied at the point w we get $\prod_\iota (A_{i^*}(y_\iota) - s_\iota) = 0$, i.e. $A_{i^*}(y_\iota) = s_\iota$ for some ι ; since $y_\iota = \iota_{\text{var}}(v_\iota) \in H^m$, this says $\alpha(v_\iota) = s_\iota = 1 - b_\iota$, i.e. the literal ℓ_ι is true under α . So α satisfies every clause. $\square$

Corollary 11.3 (Soundness). *If φ is unsatisfiable, then $\text{dist}_2(t^*, L) > q^c \Delta_\varphi$.*

Proof. Otherwise Proposition 4.2 yields a coherent integer proof, and Theorem 11.2 a satisfying assignment. $\square$

12 Parameter ledger and proof of the main theorem

12.1 Ledger

Throughout, $N \geq N_0 = 2^{2 \cdot 10^4}$, hence $q \geq 2^{10^5}$ and every explicit constant $\leq 2^{100}$ is $\leq q^{0.001}$ (absorption). Base quantities: $h \leq q^{1/40}$; $d = 60h \leq q^{0.026}$; $d_+ = d + 2$; $d_3 = 267h + 3 \leq q^{0.031}$; $d_6 = 128h \leq q^{0.029}$; $\tilde{d} \leq \bar{d} + 26 \leq q^{0.032}$; $g^2 = 16q^{0.002} \leq q^{0.003}$; list sizes $r_\bullet \leq 2g^2 \leq q^{0.0031}$; $\hat{t} \leq 2q^{0.03}$; windows $L_1 = \lceil q^{0.15} \rceil$, $L_2 = \lfloor q^{0.3} \rfloor$.

#	Requirement	Instantiation	Check
1	Bertrand: $d^{40} \leq q < 2d^{40}$	—	✓
2	scalar cap $\bar{d} \leq q^{0.04}$	max: $d_3 + 26 \leq q^{0.032}$	✓
3	scalar budgets $16 \leq \hat{g}^2 \leq q^{0.02}$	direct: g^2 ; θ -calls: $\hat{t}g^2 \leq 2q^{0.016}$	✓
4	Step-1 minor SZ: $2\hat{t}(\hat{t} + 1)\bar{d} < q(1 - 2q^{-c_3})$	$\leq 12q^{0.1}$	✓
5	Prop. 5.4 ranges used: $2l\bar{d} \leq q - 1$ for $l \leq \max(2\hat{t}, L_1)$; $2 \mathbf{k} \bar{d} \leq q - 1$ for $ \mathbf{k} \leq L_2$	$2L_1\bar{d} \leq q^{0.2}$; $2L_2d_3 \leq 2q^{0.335}$	✓
6	CM precondition $q > 2\delta^4$, $\delta \leq D_0 = 9q^{0.1}$	$2\delta^4 \leq q^{0.42}$	✓
7	CM slack: $(\delta-1)(\delta-2)q^{-1/2} + 5\delta^{13/3}q^{-1} \leq 2q^{-0.29}$	—	✓
8	conjugate case: $\delta^2q^{-1} \leq q^{-0.79} \ll 1$	—	✓
9	very-good losses $\leq r^2 2H_0q^{-1} \leq q^{-0.83}$	$H_0 = D_0$	✓
10	Step 3: $D_A = r^2 H_0 + r\bar{d} \leq q^{0.17}$; $(2M_1+2)D_Aq^{-1} \leq q^{-0.77}$; $M_1^2/32 > \hat{g}^2$	$M_1 = \lfloor q^{0.05} \rfloor$; $q^{0.1}/32 > q^{0.02}$	✓
11	no-poles window $2H_0r+2r \leq 40q^{0.13} \leq L_1$	—	✓
12	degree window $2r\bar{d}+2r \leq 10q^{0.07} \leq L_1$	—	✓
13	(7.1)-SZ: $L_1(\bar{d} + rH_0) \leq 19q^{0.28} < q/2$	—	✓
14	lift: $\text{unclean} \leq 4\hat{g}^2q^{m_0-2}$; $\sqrt{2}\hat{g} < q/2$; $ \mathcal{X} \leq 3q^{m_0-c_3}$	—	✓
15	tuple: $ E'_0 \leq q^{(m_0+1)-c_3}$ (scalar E_0 -cap)	—	✓
16	tuple: valid θ_0 count $\geq q - q^{0.995} - \hat{t}^2 J - \tilde{r}^2 \tilde{d} \geq q/2$; pigeonhole $(q/2)/\tilde{r} > \tilde{d}$	$\frac{1}{4}q^{0.97} > q^{0.032}$	✓
17	tuple exceptional $\leq 4q^{m_0-c_3/2}$; downstream SZ uses $1 - 8q^{-c_3/2} > \frac{1}{2}$	—	✓
18	(8.1)/(R+) SZ: $L_2\tilde{d} \leq q^{0.34} < q/2$; MM-form $L_2d < q$	—	✓
19	CS windows: $\lceil q^{0.004} \rceil \geq r_1 + r_2$, $r_2 + r_3$, $r_1 + r_6$ ($\leq 4g^2 \leq q^{0.0032}$); degrees $l \cdot 270h \leq q^{0.036} < q/2$	Lemmas 9.1–9.3	✓
20	Phase I: $\bar{D} = 5r_2^2d_+ \leq q^{0.04}$; window $\bar{D}+2r_2-1+2r_2 \leq q^{0.05} \leq L_2$; $k+2r_2 \leq L_2$	—	✓
21	Phase II window $3r_2 \leq q^{0.004} \leq L_2$	—	✓
22	completeness degrees: $50h \leq d_3$, $15h \leq d_6$, $m(h-1) \leq d$	—	✓
23	soundness radius: $q^c \Delta_\varphi < q^{31}$; $ \ell_\rho(F) \leq 2q^{41}$; $W \cdot 3q^{41} < q^{1043} < P - q^{31}$; $q^{31} < W$	Prop. 4.2	✓
24	nets: $2g^2 < q/2 \pmod{q}$ to $\mathbb{Z}$ upgrades)	$32q^{0.002} < q/2$	✓
25	$n \leq 2q^{54} \leq q^{55}$; $(1 + q^{-10}) \leq q^{10^{-5}}$; $c - 10^{-5} \geq 55c'$	$9.9 \times 10^{-4} = 55 \cdot 1.8 \times 10^{-5}$	✓

12.2 Proof of Theorem 1.1

The reduction of §2 maps a 3CNF formula φ to $(B_0/R, t^*/R)$ in deterministic polynomial time (§2.5), with lattice rank $n \leq q^{55}$ by (2.2). If φ is satisfiable, then $\text{dist}_2(t^*, L) \leq \Delta_\varphi$ (Proposition 3.3), so the output instance has distance $\leq \Delta_\varphi/R \leq 1$: a YES instance. If φ is unsatisfiable, then $\text{dist}_2(t^*, L) > q^c \Delta_\varphi$ (Corollary 11.3), so the output distance exceeds

$$\frac{q^c \Delta_\varphi}{R} \geq \frac{q^c}{1 + q^{-10}} \geq q^{c-10^{-5}} = q^{9.9 \times 10^{-4}} \geq (q^{55})^{1.8 \times 10^{-5}} \geq n^{c'},$$

a NO instance (ledger #25). Degenerate inputs are handled by §2.6 (for $n = 1$ we have $n^{c'} = 1$, and the fixed instances have distances 0 and $3/2$). Composing with the Cook–Levin reduction of any NP language to 3SAT completes the proof, with $c' = 1.8 \times 10^{-5}$. ■

External results used without proof. Cook–Levin; Bertrand’s postulate; polynomial-time Hermite normal form computation with polynomial bit-sizes (Kannan–Bachem); the Delsarte–Goethals–MacWilliams duality $\text{GRM}_q(\rho, 2)^\perp = \text{GRM}_q(2q - 3 - \rho, 2)$ (Proposition 5.2); Cafure–Matera’s explicit estimate $|\#V(\mathbb{F}_q) - q^{\dim V}| \leq (\delta - 1)(\delta - 2)q^{\dim V - 1/2} + 5\delta^{13/3}q^{\dim V - 1}$ for absolutely irreducible affine V of degree δ under $q > 2\delta^4$, and the elementary bound $\#W(\mathbb{F}_q) \leq \deg W \cdot q^{\dim W}$. The use of the Cafure–Matera bound has massive slack: any bound of the shape $q^{m_0} + \delta^{O(1)}q^{m_0 - 1/2}$ valid for $q > \delta^{O(1)}$ suffices, since $\delta \leq 9q^{0.1}$ here.