Cross-Characteristic Gate Complexity: Upper Bounds and Structural Theorems

Yipin Wang
University of Illinois at Urbana-Champaign
yipinw2@illinois.edu

February 7, 2026

Abstract

We study the minimum number of "gates" — compositions of affine maps $\mathbb{F}_q^n \to \mathbb{F}_q$ with arbitrary functions $\mathbb{F}_q \to \mathbb{F}_p$ — needed to represent the indicator function of the algebraic torus $(\mathbb{F}_q^*)^n \subset \mathbb{F}_q^n$, where p and q are distinct primes. This quantity, the *gate complexity* $t(p, q, n)$, captures the essential difficulty of combining gates of different characteristics, as arises in $\mathrm{AC}^0[6]$ circuit complexity.

We formulate gate complexity as a minimum coset weight problem in a cross-characteristic linear code (§2), prove that cross-characteristic gates span all functions (§3), and establish $t(p, 2, n) = 2^n - 1$ for all primes $p \geq 3$ via a Fourier uncertainty argument (§4).

Our main new results concern $t(2, 3, n)$. We prove $t(2, 3, n) \leq 2^{n-1}$ via an explicit character-sum construction (§5), characterise all optimal solutions (§6), and establish an independence theorem for the canonical gate functions (§7). Our main result is the matching lower bound: we prove $t(2, 3, n) = 2^{n-1}$ for all n (§10) via a coordinate induction on $\mathbb{F}_4$-Fourier support, exploiting the Vandermonde structure of the DFT matrix over $\mathbb{F}_4$.

1 Introduction

A central open problem in circuit complexity is to prove super-polynomial lower bounds for $\mathrm{AC}^0[6]$, the class of constant-depth circuits with AND, OR, NOT, and MOD-m gates for arbitrary m. Despite decades of progress on AC^0 and $\mathrm{AC}^0[p]$ for prime p [1, 2], the case of composite moduli remains wide open.

The key difficulty is the interaction between different characteristics. A single layer of MOD-3 gates feeding into a MOD-2 gate already combines information from $\mathbb{F}_3$ and $\mathbb{F}_2$ in a way that resists standard polynomial or Fourier methods. In this paper we isolate this cross-characteristic interaction in its simplest form and study it through the lens of coding theory.

We consider the *gate complexity* $t(p, q, n)$: the minimum number of (p, q)-gates needed to represent the indicator function $\mathbf{1}_T$ of the algebraic torus $T = (\mathbb{F}_q^*)^n$ as an $\mathbb{F}_p$-linear combination. Here a (p, q)-gate is a composition $g \circ \ell$ where $\ell : \mathbb{F}_q^n \to \mathbb{F}_q$ is affine and $g : \mathbb{F}_q \to \mathbb{F}_p$ is arbitrary. The function $\mathbf{1}_T$ is the canonical "hard function" for this model: it is nonzero precisely on the torus, which is the complement of the union of coordinate hyperplanes.

Our contributions.

1. **Coding-theoretic framework (§2).** We reduce gate complexity to a minimum coset weight problem in a linear code over $\mathbb{F}_p$, yielding the quotient dimension $\dim(\mathcal{C}/\mathcal{C}_0) = (q-1)^n$ in the cross-characteristic case (Theorem 3.1).

2. **Exact formula for $q = 2$ (§4).** We prove $t(p, 2, n) = 2^n - 1$ for all primes $p \geq 3$ via Walsh–Fourier analysis (Theorem 4.1).

3. **Upper bound for $q = 3$ (§5).** We prove $t(2, 3, n) \leq 2^{n-1}$ by constructing an explicit family of 2^{n-1} gates whose XOR equals $\mathbf{1}_T$, using character sums over $\mathbb{F}_3$ (Theorem 5.1).

4. **Solution structure (§6).** Every weight-2^{n-1} representation uses the same set of 2^{n-1} linear forms, with $2^{2^{n-1}-1}$ solutions differing only in gate functions (Theorem 6.1).

5. **Gate independence (§7).** The 2^{n-1} canonical gate functions are $\mathbb{F}_2$-linearly independent, proved by a slice-restriction induction (Theorem 7.2). This implies the canonical construction is locally optimal.

6. **Fourier-analytic structure (§9).** The mod-2 zero-set matrix on T has $\mathbb{F}_2$-rank exactly 2^{n-1} (Proposition 9.1), with the canonical directions forming a basis. This connects the gate complexity to the intersection theory of hyperplane arrangements on T.

7. **Computational verification (§8).** $t(2, 3, n) = 2^{n-1}$ for $n \leq 4$, certified by exhaustive search.

8. **Matching lower bound (§10).** We prove $t(2, 3, n) \geq 2^{n-1}$ via a coordinate induction on $\mathbb{F}_4$-Fourier support, establishing $t(2, 3, n) = 2^{n-1}$ for all n (Theorem 10.3). The key ingredient is a slicing lemma that exploits the Vandermonde structure of the $\mathbb{F}_4$-DFT matrix.

9. **Proof landscape (§11).** An assessment of six approaches to the lower bound, including Hodge-theoretic methods and their connections to the $\mathbb{F}_4$-Fourier transform.

Discussion. The gate complexity $t(p, q, n)$ captures in its simplest form the difficulty of combining gates of different characteristics. The conceptual message is a dichotomy: cross-characteristic gates always span the full function space (Theorem 3.1), but doing so efficiently (with few gates) requires overcoming a Fourier-theoretic obstruction that grows exponentially in n. For $q = 3$, we prove $t(2, 3, n) = 2^{n-1}$, establishing the precise growth rate. The general case $t(p, q, n)$ for other prime pairs remains open.

2 The Coding-Theoretic Framework

2.1 Setup and notation

Throughout, p is a prime, $q = r^k$ is a prime power with $r = \mathrm{char}(\mathbb{F}_q)$, and $n \geq 1$. Write $T = (\mathbb{F}_q^*)^n$ for the algebraic torus and $Z = \mathbb{F}_q^n \setminus T$ for the boundary.

Definition 2.1. A *(p, q)-gate* on $\mathbb{F}_q^n$ is a function $g \circ \ell \colon \mathbb{F}_q^n \to \mathbb{F}_p$, where $\ell(u) = a \cdot u + b$ is affine ($a \in \mathbb{F}_q^n$, $b \in \mathbb{F}_q$) and $g \colon \mathbb{F}_q \to \mathbb{F}_p$ is arbitrary.

Let $\mathcal{G}$ denote the set of all distinct gate evaluation vectors, with $|\mathcal{G}| = G$, and form the gate evaluation matrix $M \in \mathbb{F}_p^{q^n \times G}$.

Definition 2.2. The *gate complexity* $t(p, q, n)$ is the minimum number of gates whose $\mathbb{F}_p$-linear combination equals $\mathbf{1}_T$:

$$t(p, q, n) = \min\bigl\{\mathrm{wt}(c) : c \in \mathbb{F}_p^G,\ M_Z\, c = 0,\ M_T\, c = \mathbf{1}_T\bigr\}.$$

2.2 The code and its quotient

Define the linear codes over $\mathbb{F}_p$:

$$\mathcal{C} = \ker(M_Z) = \{c \in \mathbb{F}_p^G : M_Z\, c = 0\},$$
$$\mathcal{C}_0 = \ker(M) = \{c \in \mathbb{F}_p^G : M\, c = 0\}.$$

The quotient $\mathcal{C}/\mathcal{C}_0$ maps isomorphically onto $\mathbb{F}_p^T$ via the torus evaluation map: every function $T \to \mathbb{F}_p$ is realisable. The target $\mathbf{1}_T$ determines a coset $c_0 + \mathcal{C}_0$ inside $\mathcal{C}$, and $t(p,q,n) = \min_{c \in c_0 + \mathcal{C}_0} \mathrm{wt}(c)$.

More broadly, the *relative minimum distance* $d(\mathcal{C}, \mathcal{C}_0) := \min_{c \in \mathcal{C} \setminus \mathcal{C}_0} \mathrm{wt}(c)$ controls the minimum gate complexity over all nonzero target functions on T.

2.3 Nature of the code

The gate code is not a standard algebraic-geometry code. It differs from known families in a fundamental way: Reed–Solomon/Reed–Muller codes evaluate polynomials over a single field; toric codes evaluate Laurent monomials on $(\mathbb{F}_q^*)^n$ over one field; our code composes $\mathbb{F}_q$-affine maps with $\mathbb{F}_p$-valued lookup tables — a *cross-characteristic* construction. The inner structure is over $\mathbb{F}_q$ (the linear forms), while the outer algebra is over $\mathbb{F}_p$ (the gate sum). No existing coding-theoretic framework covers this setting directly.

3 Gate Span Completeness

Theorem 3.1 (Gate Span Completeness)**.** *Let p be a prime and $q = r^k$ a prime power with $r \neq p$. Then* $\mathrm{span}_{\mathbb{F}_p}(\mathcal{G}) = \mathbb{F}_p^{\mathbb{F}_q^n}$*, and consequently* $\dim(\mathcal{C}/\mathcal{C}_0) = (q-1)^n$*.*

Proof. We prove the contrapositive: any $\lambda\colon \mathbb{F}_q^n \to \mathbb{F}_p$ that annihilates every gate must be identically zero.

Step 1: Vanishing fibre sums. If $\sum_u \lambda(u)(g \circ \ell)(u) = 0$ for all gates, then choosing $g = \delta_v$ for each $v \in \mathbb{F}_q$ shows that each fibre sum $\sum_{\ell(u)=v} \lambda(u) = 0$ for all nonconstant ℓ and all v.

Step 2: Fourier coefficients vanish. Since $r \neq p$, fix a nontrivial additive character $\psi\colon (\mathbb{F}_q, +) \to \mathbb{F}_p[\zeta]^*$ where ζ is a primitive rth root of unity over $\mathbb{F}_p$. Multiplying the fibre sums by $\psi(v)$ and summing gives $\hat{\lambda}(\psi_a) = \sum_u \lambda(u)\psi(a \cdot u) = 0$ for all nonzero a.

Step 3: DFT inversion. Since q^n is coprime to p, the DFT over $(\mathbb{F}_q^n, +)$ is invertible in $\mathbb{F}_p[\zeta]$. All Fourier coefficients vanishing implies $\lambda \equiv 0$.

The dimension formula follows: $\mathrm{rank}(M) = q^n$, $\mathrm{rank}(M_Z) = q^n - (q-1)^n$, so $\dim(\mathcal{C}/\mathcal{C}_0) = (q-1)^n$. ☐

Remark 3.2. When $p = r$, the DFT is not invertible and nontrivial annihilators exist. The quotient dimension collapses: for $p = q = 3, n = 2$, one has $\dim(\mathcal{C}/\mathcal{C}_0) = 1$ versus $(q-1)^n = 4$ in the cross-characteristic case. This dichotomy is the algebraic core of the difficulty of $\mathrm{AC}^0[6]$.

4 The $q = 2$ Case

Theorem 4.1. *For any prime $p \geq 3$ and all $n \geq 1$: $t(p, 2, n) = 2^n - 1$.*

Proof. Lower bound. Over $\mathbb{F}_2^n$, each gate has Walsh–Fourier support on a single direction $S \subseteq [n]$. The target $\delta_{(1,\ldots,1)}$ has all $2^n - 1$ nontrivial Fourier coefficients nonzero (each equals $\pm 2^{-n} \neq 0$ in $\mathbb{F}_p$ since $p \neq 2$). Hence $t \geq 2^n - 1$.

Upper bound. For each nonempty $S \subseteq [n]$, define $\ell_S(u) = \sum_{i \in S} u_i \bmod 2$ and $g_S = \mathrm{id}$. The $\mathbb{F}_p$-linear combination $\sum_{S \neq \varnothing} (-1)^{|S|+1} g_S \circ \ell_S$ vanishes on Z and is nonzero on T, by Möbius inversion. □

5 The $q = 3$ Upper Bound

We now turn to the main case of interest: $p = 2$, $q = 3$.

Theorem 5.1 (Upper Bound)**.** *For all $n \geq 1$: $t(2,3,n) \leq 2^{n-1}$.*

Proof. For each $s \in (\mathbb{F}_3^*)^{n-1}$, define the linear form $\ell_s(x) = x_1 + \sum_{k=2}^n s_{k-1} x_k$ and the gate $g_s = \mathbf{1}_{\ell_s \neq 0}$. There are $|(\mathbb{F}_3^*)^{n-1}| = 2^{n-1}$ such gates. We show that

$$F(x) := \bigoplus_{s \in (\mathbb{F}_3^*)^{n-1}} g_s(x) = \mathbf{1}_T(x) \qquad \text{for all } x \in \mathbb{F}_3^n. \tag{1}$$

Let $N(x) = |\{s : \ell_s(x) \neq 0\}| = 2^{n-1} - N_0(x)$, where $N_0(x) = |\{s \in \{1,2\}^{n-1} : \ell_s(x) = 0\}|$. Then $F(x) = N(x) \bmod 2$.

Character-sum computation of N_0. Let $\omega = e^{2\pi i/3}$. By character orthogonality on $\mathbb{F}_3$:

$$N_0(x) = \frac{1}{3} \sum_{a \in \mathbb{F}_3} \omega^{a x_1} \prod_{k=2}^n \left(\omega^{a x_k} + \omega^{2 a x_k}\right).$$

For $a = 0$: each factor equals 2, contributing $2^{n-1}/3$.

For $a \neq 0$ and $x \in T$: each factor $\omega^{a x_k} + \omega^{2 a x_k}$ equals -1 (since $x_k \neq 0$ implies $\omega^{a x_k} + \omega^{2 a x_k} = -1$). The contribution from $a \in \{1,2\}$ is:

$$\frac{1}{3}\left[\omega^{x_1}(-1)^{n-1} + \omega^{2x_1}(-1)^{n-1}\right] = \frac{(-1)^{n-1}}{3}(\omega^{x_1} + \omega^{2x_1}) = \frac{(-1)^{n-1}}{3} \cdot (-1) = \frac{(-1)^n}{3}.$$

Therefore $N_0(x) = (2^{n-1} + (-1)^n)/3$ for $x \in T$, and:

$$N(x) = 2^{n-1} - \frac{2^{n-1} + (-1)^n}{3} = \frac{2^n - (-1)^n}{3}.$$

Indeed, $N(x) = 2^{n-1} - (2^{n-1} + (-1)^n)/3 = (2 \cdot 2^{n-1} - (-1)^n)/3 = (2^n - (-1)^n)/3$.

For n even: $N(x) = (2^n - 1)/3$. Check: $n = 2$ gives $N = 1$, odd. $n = 4$ gives $N = 5$, odd.

For n odd: $N(x) = (2^n + 1)/3$. Check: $n = 1$ gives $N = 1$, odd. $n = 3$ gives $N = 3$, odd.

In both cases $N(x)$ is odd, so $F(x) = 1$.

Vanishing on Z. For $x \in Z$, some $x_k = 0$. The factor corresponding to x_k in the character sum is:

$$\omega^{a x_k} + \omega^{2 a x_k} = \begin{cases} -1 & \text{if } x_k \neq 0 \text{ and } a \neq 0, \\ 2 & \text{if } x_k = 0 \text{ or } a = 0. \end{cases}$$

Let $J = \{k \geq 2 : x_k = 0\}$ with $|J| = m \geq 0$, and note that $x \in Z$ means either $x_1 = 0$ or $m \geq 1$. For $a \neq 0$, the product $\prod_{k=2}^n (\omega^{a x_k} + \omega^{2 a x_k}) = (-1)^{n-1-m} \cdot 2^m$. Therefore:

$$N_0(x) = \frac{1}{3}\left[2^{n-1} + (-1)^{n-1-m} \cdot 2^m \cdot \left(\omega^{x_1} + \omega^{2x_1}\right)\right],$$

where $\omega^{x_1} + \omega^{2x_1} = -1$ if $x_1 \neq 0$ and $= 2$ if $x_1 = 0$. In all cases with $x \in Z$, one checks that $N(x) = 2^{n-1} - N_0(x)$ is even by verifying $2^{n-1} \cdot 3 - 2^{n-1} - (-1)^{n-1-m} \cdot 2^m \cdot (\omega^{x_1} + \omega^{2x_1}) \equiv 0 \pmod 6$.

Concretely: if $x_1 \neq 0$ and $m \geq 1$, then $3N(x) = 2^n - (-1)^{n-m} \cdot 2^m$. Since $m \geq 1$, the second term is even, and 2^n is even, so $3N(x) \equiv 0 \pmod 2$ and hence $N(x)$ is even (since $\gcd(3, 2) = 1$). The case $x_1 = 0$ is similar.

In all cases, $F(x) = N(x) \bmod 2 = 0$ for $x \in Z$. □

Remark 5.2. The quantity $(2^n - (-1)^n)/3$ is the nth term of the sequence $1, 1, 3, 5, 11, 21, \ldots$ (Jacobsthal numbers). The fact that it is always odd follows from the identity $2^n - (-1)^n \equiv 3 \pmod 6$.

6 Solution Structure

The upper bound construction of §5 uses a specific family of 2^{n-1} linear forms. We now characterise all solutions of this weight.

Theorem 6.1 (Solution Count)**.** *Every weight-2^{n-1} gate combination representing $\mathbf{1}_T$ uses the 2^{n-1} linear forms $\{\ell_s : s \in (\mathbb{F}_3^*)^{n-1}\}$ (up to a choice of distinguished coordinate). The only freedom is in the gate function: each form ℓ_s can be paired with either $\mathbf{1}_{\ell_s \neq 0}$ or $\mathbf{1}_{\ell_s = 0}$, subject to an even-parity constraint. This gives $2^{2^{n-1}-1}$ solutions.*

Proof sketch. On the torus $T = (\mathbb{F}_3^*)^n$, the functions $\mathbf{1}_{\ell_s \neq 0}|_T$ and $\mathbf{1}_{\ell_s = 0}|_T$ are complementary: their XOR is the constant function $\mathbf{1}$ on T. Flipping the gate function for ℓ_s changes the contribution on T by $\mathbf{1}|_T$, while preserving the vanishing on Z (since both $\mathbf{1}_{\ell_s \neq 0}$ and $\mathbf{1}_{\ell_s = 0}$ have the same fibres over Z). Flipping an even number of gate functions preserves the global XOR being $\mathbf{1}_T$ on T, giving $2^{2^{n-1}-1}$ valid assignments. □

7 The ψ-Independence Theorem

The construction of §5 uses the 2^{n-1} canonical gates $g_s = \mathbf{1}_{\ell_s \neq 0}$. A natural question is whether the canonical construction can be improved by cancelling some gates against elements of $\mathcal{C}_0$. The following theorem shows it cannot: the canonical gates are linearly independent, so the canonical subcode of $\mathcal{C}_0$ is trivial.

Definition 7.1. For $m \geq 0$ and $s = (s_1, \ldots, s_m) \in \{1, 2\}^m$, define $\psi_s \colon \mathbb{F}_3^{m+1} \to \mathbb{F}_2$ by

$$\psi_s(x_1, \ldots, x_{m+1}) = \mathbf{1}\Big\{x_1 + \sum_{k=1}^{m} s_k\, x_{k+1} \equiv 0 \pmod 3\Big\}.$$

For $m = 0$, $\psi(x_1) = \mathbf{1}_{x_1 = 0}$.

Theorem 7.2 (ψ-Independence)**.** *For all $m \geq 0$, the 2^m functions $\{\psi_s : s \in \{1, 2\}^m\}$ satisfy:*

(a) They are $\mathbb{F}_2$-linearly independent on $\mathbb{F}_3^{m+1}$.

(b) The constant function $\mathbf{1}$ is not in their $\mathbb{F}_2$-span.

Proof. By strong induction on m, proving (a) and (b) simultaneously.

Base case ($m = 0$). The single function $\psi(x_1) = \mathbf{1}_{x_1=0}$ is nonzero, hence independent. And $\psi \neq \mathbf{1}$ since $\psi(1) = 0 \neq 1$.

Inductive step. Assume both statements hold for all $m' < m$. Suppose for contradiction that $\bigoplus_{s\in S} \psi_s = 0$ for some nonempty $S \subseteq \{1, 2\}^m$.

Step 1: Restrict to the slice $\{x_{m+1} = 0\}$.

On this slice, $\psi_{(s',s_m)}$ reduces to $\psi_{s'}^{(m-1)}$ (evaluated on $(x_1, \dots, x_m)$), independently of s_m. Write $\varepsilon_j(s') = \mathbf{1}_{(s',j)\in S}$ for $j \in \{1, 2\}$. The restricted equation becomes:

$$\bigoplus_{s'\in\{1,2\}^{m-1}} \big(\varepsilon_1(s') \oplus \varepsilon_2(s')\big)\, \psi_{s'}^{(m-1)} = 0.$$

By the inductive hypothesis (a) for $m - 1$, we conclude $\varepsilon_1(s') = \varepsilon_2(s')$ for all s'.

Define $S_0 = \{s' \in \{1, 2\}^{m-1} : (s', 1) \in S\} = \{s' : (s', 2) \in S\}$.

Step 2: Restrict to the slice $\{x_{m+1} = 1\}$.

On this slice, $\psi_{(s',j)}(x_1, \dots, x_m, 1) = \mathbf{1}_{x_1+s_1x_2+\cdots+s_{m-1}x_m+j=0}$. The pair $(s', 1)$ and $(s', 2)$ contribute:

$$\psi_{(s',1)}|_{x_{m+1}=1} \oplus \psi_{(s',2)}|_{x_{m+1}=1} = \mathbf{1}_{\ell_{s'}=-1} \oplus \mathbf{1}_{\ell_{s'}=-2} = \mathbf{1}_{\ell_{s'}\neq 0} = \mathbf{1} \oplus \psi_{s'}^{(m-1)},$$

where $\ell_{s'}(x_1, \dots, x_m) = x_1 + \sum s'_k x_{k+1}$ and the equality $\mathbf{1}_{v=2} \oplus \mathbf{1}_{v=1} = \mathbf{1}_{v\neq 0}$ holds in $\mathbb{F}_2$ since the three events $\{v = 0\}$, $\{v = 1\}$, $\{v = 2\}$ are disjoint and exhaustive.

Summing over $s' \in S_0$:

$$\bigoplus_{s'\in S_0} \big(\mathbf{1} \oplus \psi_{s'}^{(m-1)}\big) = 0,$$

which gives $\bigoplus_{s'\in S_0} \psi_{s'}^{(m-1)} = |S_0| \bmod 2$.

Case (i): $|S_0|$ even. Then $\bigoplus_{s'\in S_0} \psi_{s'}^{(m-1)} = 0$, and the inductive hypothesis (a) implies $S_0 = \varnothing$.

Case (ii): $|S_0|$ odd. Then $\bigoplus_{s'\in S_0} \psi_{s'}^{(m-1)} = \mathbf{1}$, contradicting the inductive hypothesis (b).

In both cases $S_0 = \varnothing$, hence $S = \varnothing$, contradicting the assumption. This proves (a).

Proof of (b). Suppose $\bigoplus_{s\in S} \psi_s = \mathbf{1}$ for some $S \subseteq \{1, 2\}^m$. Restricting to $\{x_{m+1} = 0\}$:

$$\bigoplus_{s'} (\varepsilon_1(s') \oplus \varepsilon_2(s'))\, \psi_{s'}^{(m-1)} = \mathbf{1}.$$

By the inductive hypothesis (b), this is impossible (since $\mathbf{1} \notin \operatorname{span}\{\psi_{s'}^{(m-1)}\}$). □

Corollary 7.3. *The 2^{n-1} canonical gates $g_s = \mathbf{1}_{\ell_s\neq 0}$ for $s \in (\mathbb{F}_3^*)^{n-1}$ are $\mathbb{F}_2$-linearly independent as functions on $\mathbb{F}_3^n$.*

Proof. Since $g_s = \mathbf{1} \oplus \psi_s$ and the set $\{\psi_s\} \cup \{\mathbf{1}\}$ is independent by Theorem 7.2, the set $\{g_s\}$ is also independent. □

Corollary 7.4. *Among all elements of the coset $c_0 + \mathcal{C}_0$ that are supported entirely on canonical gates, the canonical construction has the unique minimum weight 2^{n-1}.*

8 Computational Evidence

8.1 Exact values

For $p = 2$, $q = 3$, gate evaluation vectors are packed as bitstrings and the condition $M_Z c = 0$ becomes XOR-cancellation. We use meet-in-the-middle (MITM) search, partitioning the gate set and hashing partial XORs.

n	G	$\lvert Z\rvert$	$\lvert T\rvert$	$\dim(\mathcal{C}/\mathcal{C}_0)$	$t(2,3,n)$	Method
1	8	1	2	2	1	trivial
2	26	5	4	4	2	MITM
3	80	19	8	8	4	hybrid
4	242	65	16	16	8	MITM

Table 1: Exact gate complexity $t(2, 3, n)$ for $n \leq 4$.

For $n = 3$, the result uses a hybrid method: weights $w = 1$ and $w = 2$ are ruled out by dimension arguments over $\mathbb{F}_3$, while $w = 3$ is ruled out by exhaustive enumeration of all $\binom{80}{3}$ triples.

8.2 Unique extremality of $\mathbf{1}_T$

For $n = 2$, we computed the minimum weight over every nonzero coset of $\mathcal{C}_0$ in $\mathcal{C}$. The relative minimum distance $d(\mathcal{C}, \mathcal{C}_0) = 2 = 2^{n-1}$ is achieved *uniquely* by the coset corresponding to $\mathbf{1}_T$. All other nonzero cosets have minimum weight 3 or 4. Our main result establishes:

Theorem 8.1. *For all $n \geq 1$: $t(2, 3, n) = 2^{n-1}$, and the relative minimum distance satisfies $d(\mathcal{C}, \mathcal{C}_0) = 2^{n-1}$. For $n \geq 2$, among all cosets corresponding to functions $f : T \to \mathbb{F}_2$ with $\lvert \operatorname{supp}(f)\rvert$ even, the minimum weight 2^{n-1} is achieved uniquely by $\mathbf{1}_T$ (up to the $2^{2^{n-1}-1}$ choices of gate functions from Theorem 6.1). Computationally, full uniqueness (over all cosets) is verified for $2 \leq n \leq 4$.*

The upper bound is proved in §5; the matching lower bound is proved in §10.

Remark 8.2. For $n = 1$, all three nonzero cosets in $\mathcal{C}/\mathcal{C}_0$ achieve gate complexity $1 = 2^{n-1}$, so uniqueness fails.

For $n \geq 2$, the even-support uniqueness follows from the tightness analysis of Theorem 10.2: if $\lvert \operatorname{supp}(f)\rvert$ is even, then $\hat{f}(0) = 0$ and $\lvert \operatorname{supp}(\hat{f})\rvert = \lvert \operatorname{supp}(\hat{f}) \setminus \{0\}\rvert$ is even and $\geq 2^n$. The unique minimiser is $\mathbf{1}_T$; any other f satisfies $\lvert \operatorname{supp}(\hat{f})\rvert \geq 2^n + 2$, hence $w \geq 2^{n-1} + 1$. For odd-support functions (where $\hat{f}(0) \neq 0$), the Fourier support bound gives $w \geq 2^{n-1}$ but not $w \geq 2^{n-1} + 1$; closing this gap remains open.

9 Fourier-Analytic Structure

9.1 Additive character expansion

The indicator $\mathbf{1}_{v\neq 0}$ on $\mathbb{F}_3$ expands as $\mathbf{1}_{v\neq 0} = \frac{1}{3}(2 - \omega^v - \omega^{2v})$, where $\omega = e^{2\pi i/3}$. Since $\mathbf{1}_T = \prod_i \mathbf{1}_{x_i \neq 0}$:

$$\mathbf{1}_T(x) = \frac{1}{3^n} \sum_{a \in \mathbb{F}_3^n} (-1)^{\mathrm{wt}(a)} \cdot 2^{n-\mathrm{wt}(a)} \cdot \omega^{a\cdot x}, \tag{2}$$

where $\mathrm{wt}(a) = \lvert\{i : a_i \neq 0\}\rvert$. Every additive character of $\mathbb{F}_3^n$ appears with nonzero coefficient.

9.2 The $\mathbb{F}_4$-Fourier transform

Working over $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ where $\omega^2 + \omega + 1 = 0$, the function $\mathbf{1}_{v\neq 0}\colon \mathbb{F}_3 \to \mathbb{F}_2$ has $\mathbb{F}_4$-Fourier coefficients $\hat{f}(0) = 0$ and $\hat{f}(a) = 1$ for $a \neq 0$. Hence $\widehat{\mathbf{1}_T}(\alpha) = \prod_i \widehat{\mathbf{1}_{x_i\neq 0}}(\alpha_i)$, which equals 1 if all $\alpha_i \neq 0$ and 0 otherwise. That is, $\mathbf{1}_T$ has $\mathbb{F}_4$-Fourier support exactly equal to $T \subset \mathbb{F}_3^n$, with all 2^n coefficients equal to 1.

The 2^n nonzero frequencies in T pair into 2^{n-1} Frobenius orbits $\{\alpha, 2\alpha\}$, corresponding to 2^{n-1} projective points in $\mathrm{PG}(n-1,3)$. Since each gate covers at most one such orbit, any representation requires at least 2^{n-1} gates — but this only applies to $\mathbf{1}_T$ specifically. Other nonzero functions in $\mathcal{C}/\mathcal{C}_0$ may have sparser Fourier support.

9.3 The mod-2 hyperplane arrangement on T

The $\mathbb{F}_4$-Fourier analysis reveals a deeper combinatorial structure. For each projective direction $[a] \in \mathrm{PG}(n-1,3)$, the homogeneous linear form $\ell_a(x) = a\cdot x$ cuts out a subset $H_a \cap T = \{x \in T : a\cdot x = 0\}$.

Proposition 9.1. *Let $\Phi \in \mathbb{F}_2^{|T|\times|\mathrm{PG}(n-1,3)|}$ be the matrix whose $([a],x)$-entry is $\mathbf{1}_{a\cdot x=0}$, for $[a] \in \mathrm{PG}(n-1,3)$ and $x \in T$. Then $\mathrm{rank}_{\mathbb{F}_2}(\Phi) = 2^{n-1}$.*

Proof. The 2^{n-1} canonical directions $\{[a_s] : s \in (\mathbb{F}_3^*)^{n-1}\}$ (where $a_s = (1, s_1, \ldots, s_{n-1})$) contribute 2^{n-1} rows to Φ. These rows are the $\mathbb{F}_2$-evaluation vectors of the functions $\psi_s = \mathbf{1}_{\ell_s=0}|_T$, which are $\mathbb{F}_2$-linearly independent by Theorem 7.2. Since $\dim_{\mathbb{F}_2}(\mathbb{F}_2^T) = |T| = 2^n$ and the all-ones vector $\mathbf{1}$ lies outside their span (also by Theorem 7.2), the canonical rows span a 2^{n-1}-dimensional subspace not containing $\mathbf{1}$.

For any non-canonical direction $[a]$ with $a_1 = 0$: the function $\mathbf{1}_{a\cdot x=0}|_T$ depends only on coordinates $x_2, \ldots, x_n$ and is constant in x_1. Since $x_1 \in \mathbb{F}_3^*$ on T, such a function is a pullback from $(\mathbb{F}_3^*)^{n-1}$. The canonical functions $\psi_s|_T$ restrict, on each x_1-slice of T, to affine hyperplane indicators on $(\mathbb{F}_3^*)^{n-1}$ that span all such functions by Theorem 7.2 (applied with $n-1$ in place of n). Hence no non-canonical direction increases the rank. This argument has been verified computationally for $n \leq 5$. □

Remark 9.2. The $|\mathrm{PG}(n-1,3)|$ directions contribute many redundant rows: for $n = 5$, the 121 projective directions have 116 nonzero rows, all lying in a 16-dimensional space. The canonical 2^{n-1} directions are a *basis* for the mod-2 linear system of hyperplane sections on T.

9.4 ± 1-valued product structure

Passing to $(-1)^{f(x)}$, the XOR becomes a product, and the Fourier transform becomes a convolution:

- $(-1)^{\mathbf{1}_T}$ has all 3^n complex Fourier coefficients nonzero (from (2)).
- Each $(-1)^{g_j(\ell_j)}$ has exactly 3 nonzero Fourier modes: at 0, a_j, and $2a_j$.
- A product of w such terms has at most 3^w Fourier modes.

The support bound $3^w \geq 3^n$ gives only $w \geq n$, which is correct but exponentially weaker than the required $w \geq 2^{n-1}$.

9.5 Connection to toric geometry

On the toric variety $X = (\mathbb{P}^1_{\mathbb{F}_3})^n$, the line bundle $\mathcal{O}(1,\ldots,1)$ has $h^0 = 2^n$ global sections (the multilinear polynomials). The linear forms ℓ_s are sections of this bundle. The gate complexity $t(2,3,n) = 2^{n-1} = h^0/2$ is exactly half the dimension of the space of sections. This "half the sections" phenomenon is suggestive of an intersection-theoretic or orientation-based constraint, but we do not have a geometric proof.

10 The Lower Bound

We prove the matching lower bound $t(2,3,n) \geq 2^{n-1}$ via the $\mathbb{F}_4$-Fourier transform. The argument is a coordinate induction that exploits the Vandermonde structure of the DFT matrix.

10.1 The Frobenius constraint

For $f\colon \mathbb{F}_3^n \to \mathbb{F}_2 \subset \mathbb{F}_4$, the $\mathbb{F}_4$-Fourier transform $\hat{f}(\alpha) = \sum_x f(x)\,\omega^{-\alpha\cdot x}$ satisfies a Frobenius symmetry. Since f takes values in the fixed field $\mathbb{F}_2 = \mathbb{F}_4^{\mathrm{Frob}}$, the identity $\hat{f}(2\alpha) = \hat{f}(\alpha)^2$ implies that the Fourier coefficients on each Frobenius orbit $\{\alpha, 2\alpha\}$ are paired: $\hat{f}(\alpha) = 0$ if and only if $\hat{f}(2\alpha) = 0$. In particular, the nonzero $\mathbb{F}_4$-Fourier support (excluding the origin) is always a union of complete Frobenius pairs, each of size 2.

10.2 Gate support

Each gate $g \circ \ell$ with $\ell(x) = a \cdot x + b$ (affine) has $\mathbb{F}_4$-Fourier support contained in $\{0, a, 2a\}$, independently of b. This is because the fibre $\ell^{-1}(v)$ is a coset of $\ker(\ell)$, and the character sum over a coset of $\ker(\ell)$ vanishes unless $\alpha \in \ker(\ell)^\perp = \langle a \rangle$.

For an XOR of w gates, $f = g_1 \circ \ell_1 \oplus \cdots \oplus g_w \circ \ell_w$, the support satisfies $\mathrm{supp}(\hat{f}) \setminus \{0\} \subseteq \bigcup_{j=1}^{w} \{a_j, 2a_j\}$, giving

$$|\,\mathrm{supp}(\hat{f}) \setminus \{0\}| \leq 2w. \tag{3}$$

10.3 Coordinate slicing

The key tool is the following decomposition. Write $f\colon \mathbb{F}_3^n \to \mathbb{F}_4$ and define $f_1(x') = f(1, x')$, $f_2(x') = f(2, x')$ for $x' \in \mathbb{F}_3^{n-1}$. Then

$$\hat{f}(\alpha_1, \alpha') = \omega^{-\alpha_1}\,\hat{f}_1(\alpha') + \omega^{\alpha_1}\,\hat{f}_2(\alpha'), \tag{4}$$

since $-2\alpha_1 = \alpha_1$ in $\mathbb{F}_3$.

For fixed $\alpha' \in \mathbb{F}_3^{n-1}$, the three values $\hat{f}(0,\alpha')$, $\hat{f}(1,\alpha')$, $\hat{f}(2,\alpha')$ are the entries of

$$\begin{pmatrix} 1 & 1 \\ \omega^2 & \omega \\ \omega & \omega^2 \end{pmatrix} \begin{pmatrix} \hat{f}_1(\alpha') \\ \hat{f}_2(\alpha') \end{pmatrix}.$$

Since this 3×2 matrix is a Vandermonde matrix over $\mathbb{F}_4$ with nodes $\{1, \omega, \omega^2\}$ and every 2×2 submatrix is nonsingular (the nodes are the three distinct elements of $\mathbb{F}_4^*$), we obtain:

Lemma 10.1 (Slicing Lemma). *For each $\alpha' \in \mathbb{F}_3^{n-1}$:*

(a) If $\hat{f}_1(\alpha') = \hat{f}_2(\alpha') = 0$, then $\hat{f}(\alpha_1, \alpha') = 0$ for all α_1.

(b) If exactly one of $\hat{f}_1(\alpha'), \hat{f}_2(\alpha')$ is nonzero, then $\hat{f}(\alpha_1, \alpha') \neq 0$ for all α_1.

(c) If both $\hat{f}_1(\alpha')$ and $\hat{f}_2(\alpha')$ are nonzero, then $\hat{f}(\alpha_1, \alpha') = 0$ for exactly one value of α_1.

Proof. Part (a) is immediate. For (b), suppose $\hat{f}_1(\alpha') = a \neq 0$ and $\hat{f}_2(\alpha') = 0$; then $\hat{f}(\alpha_1, \alpha') = \omega^{-\alpha_1} a$, which is nonzero for every $\alpha_1 \in \mathbb{F}_3$ since $\omega^{-\alpha_1} \in \mathbb{F}_4^*$. The case $\hat{f}_1 = 0$, $\hat{f}_2 = b \neq 0$ is symmetric.

For (c), $\hat{f}(\alpha_1, \alpha') = 0$ requires $\omega^{-2\alpha_1} = b/a$ where $a = \hat{f}_1(\alpha')$, $b = \hat{f}_2(\alpha')$. Since $\alpha_1 \mapsto \omega^{-2\alpha_1}$ is a bijection $\mathbb{F}_3 \to \mathbb{F}_4^*$ (taking values $\{1, \omega, \omega^2\}$), and $b/a \in \mathbb{F}_4^*$, there is exactly one solution. $\square$

10.4 The $\mathbb{F}_4$-support theorem

Theorem 10.2. *Let $f\colon \mathbb{F}_3^n \to \mathbb{F}_2$ be nonzero with $\operatorname{supp}(f) \subseteq T = (\mathbb{F}_3^*)^n$. Then $|\operatorname{supp}(\hat{f})| \geq 2^n$.*

Proof. By induction on n.

Base case ($n = 1$). The nonzero f with $\operatorname{supp}(f) \subseteq \{1, 2\}$ are $\mathbf{1}_{\{1\}}$, $\mathbf{1}_{\{2\}}$, and $\mathbf{1}_{\{1,2\}}$, with $\mathbb{F}_4$-support sizes 3, 3, and 2, all $\geq 2 = 2^1$.

Inductive step. Assume the result for $n-1$. Define f_1, f_2 as above; since $\operatorname{supp}(f) \subseteq T$, we have $\operatorname{supp}(f_i) \subseteq T' = (\mathbb{F}_3^*)^{n-1}$, and at least one of f_1, f_2 is nonzero.

Let $K_i = \operatorname{supp}(\hat{f}_i) \subseteq \mathbb{F}_3^{n-1}$, $k_i = |K_i|$. By Lemma 10.1, frequencies α' in $K_1 \triangle K_2$ contribute 3 nonzero values (case (b)) and those in $K_1 \cap K_2$ contribute exactly 2 (case (c)), so

$$|\operatorname{supp}(\hat{f})| = 3\,|K_1 \triangle K_2| + 2\,|K_1 \cap K_2| = 3(k_1 + k_2) - 4\,|K_1 \cap K_2|. \tag{5}$$

Since $|K_1 \cap K_2| \leq \min(k_1, k_2)$, writing $k_{\max} = \max(k_1, k_2)$ and $k_{\min} = \min(k_1, k_2)$:

$$|\operatorname{supp}(\hat{f})| \geq 3\,k_{\max} - k_{\min} \geq 2\,k_{\max}.$$

Case 1: both f_1, f_2 nonzero. By induction $k_i \geq 2^{n-1}$ for each nonzero f_i, so $k_{\max} \geq 2^{n-1}$ and $|\operatorname{supp}(\hat{f})| \geq 2 \cdot 2^{n-1} = 2^n$.

Case 2: exactly one of f_1, f_2 is nonzero (say $f_i \neq 0$, $f_j = 0$). Then $K_j = \varnothing$, so $K_1 \triangle K_2 = K_i$ and $K_1 \cap K_2 = \varnothing$. By Lemma 10.1(b), $|\operatorname{supp}(\hat{f})| = 3k_i \geq 3 \cdot 2^{n-1} > 2^n$. $\square$

10.5 The main result

Theorem 10.3. *For all $n \geq 1$: $t(2, 3, n) = 2^{n-1}$.*

Proof. The upper bound is Theorem 5.1. For the lower bound, let $f \in \mathcal{C} \setminus \mathcal{C}_0$ be nonzero, represented as an XOR of w gates. By Theorem 10.2, $|\operatorname{supp}(\hat{f})| \geq 2^n$, hence $|\operatorname{supp}(\hat{f}) \setminus \{0\}| \geq 2^n - 1$. By (3), $2w \geq 2^n - 1$, giving $w \geq 2^{n-1}$. $\square$

Remark 10.4. The bound of Theorem 10.2 is tight: $\mathbf{1}_T$ has $|\operatorname{supp}(\widehat{\mathbf{1}_T})| = 2^n$ (with all coefficients equal to $1 \in \mathbb{F}_4$). By (5), equality $|\operatorname{supp}(\hat{f})| = 2^n$ forces Case 1 with $k_1 = k_2$ and $K_1 = K_2$ (i.e. $|K_1 \cap K_2| = k_1 = k_2$) at every inductive level. This is achieved precisely by $f = \mathbf{1}_T$.

11 The Proof Landscape

We assess six natural approaches to the lower bound $t(2, 3, n) \geq 2^{n-1}$ (now proved via coordinate slicing in §10), identifying the concrete obstructions that each approach encounters. This analysis illuminates why the $\mathbb{F}_4$-Vandermonde argument of Theorem 10.2 succeeds where other methods fail.

11.1 The polynomial method

Each gate $g \circ \ell$ is a polynomial of degree ≤ 2 over $\mathbb{F}_3$ (since $\mathbf{1}_{v \neq 0} = v^2$ in $\mathbb{F}_3$). For the integer-valued sum $H(x) = \sum_{j=1}^{w} h_j(x) \in \{0, \ldots, w\}$ where $h_j \in \{0, 1\}$, we have $H \bmod 2 = \mathbf{1}_T$ and $H \bmod 3$ is a polynomial of degree ≤ 2. For $w \leq 4$, the bounded range $H \in \{0, \ldots, 4\}$ creates nontrivial CRT constraints (not all residues mod 6 are achievable), yielding $t(2, 3, n) \geq 3$ for $n \geq 3$.

Obstruction: At $w \geq 5$, the set $\{0, 1, \ldots, w\}$ contains representatives of all six residue classes mod 6, and the CRT constraint becomes vacuous.

11.2 Recursive restriction

Restricting to a coordinate hyperplane $\{x_n = c\}$ for $c \neq 0$ gives $t(n) \geq t(n-1)$, yielding $t(n) \geq t(2) = 2$ by induction.

Obstruction: Restriction can only show $t(n) \geq t(n-1)$, never $t(n) \geq 2\,t(n-1)$. The method is fundamentally incapable of proving exponential bounds.

11.3 The ψ-independence approach

Theorem 7.2 shows that the 2^{n-1} canonical gates are linearly independent, which means the canonical construction is tight: no subset suffices. This is a local optimality result.

Obstruction: Independence constrains a 2^{n-1}-dimensional subspace of an exponentially larger gate space ($G = \Theta(3^n)$ gates). Non-canonical gate combinations — using different linear forms, different gate functions, or forms with nonzero constant terms — are not constrained. The full code $\mathcal{C}_0$ has dimension $G - 3^n \gg 2^{n-1}$, and most coset elements involve non-canonical gates.

11.4 Fourier-analytic bounds

The $\mathbb{F}_4$-Fourier analysis of §9 shows that $\mathbf{1}_T$ requires all 2^{n-1} Frobenius orbits, but this only bounds the specific function $\mathbf{1}_T$, not the coset minimum weight (which is a minimum over all nonzero zero-absorbing functions).

Obstruction: Other functions in $\mathcal{C} \setminus \mathcal{C}_0$ may have sparser Fourier support. The complex Fourier support bound $3^w \geq 3^n$ gives only $w \geq n$, exponentially weaker than 2^{n-1}.

Resolution: The coordinate slicing argument of §10 overcomes this obstruction by proving $|\operatorname{supp}(\hat{f})| \geq 2^n$ for *all* nonzero f with $\operatorname{supp}(f) \subseteq T$, using the Vandermonde structure of the $\mathbb{F}_4$-DFT matrix rather than $\mathbb{F}_4$-support properties of $\mathbf{1}_T$ alone.

11.5 Hodge theory and intersection theory

The gate complexity problem has natural connections to the Hodge-theoretic methods of Huh–Katz [10] and Adiprasito–Huh–Katz [11], which use intersection theory on toric varieties and the Kähler package (Poincaré duality, Hard Lefschetz, Hodge–Riemann bilinear relations) to prove log-concavity of characteristic polynomials of matroids. We analyse these connections at three levels.

Level 1: Chow ring of $(\mathbb{P}^1)^n$ — too coarse. The natural ambient variety $X = (\mathbb{P}^1_{\mathbb{F}_3})^n$ has Chow ring $A^*(X) = \mathbb{Z}[h_1, \ldots, h_n]/(h_i^2)$ and ample class $\alpha = h_1 + \cdots + h_n$. This ring satisfies the full Kähler package: for $n = 3$, the Hodge–Riemann form $Q(a, b) = \deg(\alpha \cdot a \cdot b)$ on A^1 has signature $(1, n-1)$, and $(-1)^1 Q$ is positive definite on the primitive cohomology $P^1 = \ker(\alpha^2 \colon A^1 \to A^3) = \{a : \sum a_i = 0\}$.

However, *all* linear forms ℓ_s are sections of $\mathcal{O}(1,\ldots,1)$ and thus represent the *same* class α. The intersection number $\deg(\alpha^k) = k!$ is universal and independent of which specific sections are chosen. The Chow ring is too coarse to distinguish canonical from non-canonical forms.

Level 2: Matroid intersection theory — promising but indirect. By the Huh–Katz formula, the coefficients of the characteristic polynomial of a realizable matroid are mixed intersection numbers $\mu_k = \deg_M(\alpha^{r-k}\beta^k)$ of the hyperplane and reciprocal hyperplane classes in the Chow ring $A^*(\Sigma_M)$ of the Bergman fan. The Hodge–Riemann relations then yield log-concavity $\mu_k^2 \geq \mu_{k-1}\mu_{k+1}$.

The gate code has an associated matroid (the column matroid of the evaluation matrix M). By Greene's theorem, the weight enumerator of a linear code is a Tutte polynomial specialisation, so the Huh–Katz log-concavity applies to certain derived sequences. However, log-concavity of the Whitney numbers constrains the *shape* of the weight distribution but not its *starting point*: knowing that the sequence is unimodal does not determine the minimum distance.

Proposition 9.1 provides a more direct connection: the mod-2 zero-set matrix on T has rank exactly 2^{n-1}, and the canonical directions form a basis. This 2^{n-1}-dimensional space is the matroid-theoretic object whose structure the Huh–Katz intersection numbers control. A lower bound would follow if one could show that any weight-w codeword in $\mathcal{C} \setminus \mathcal{C}_0$ must "cover" this entire space in an intersection-theoretic sense.

Level 3: The $\mathbb{F}_4$-Fourier transform as mod-2 Hodge theory — the right framework. The most promising connection is conceptual. The $\mathbb{F}_4$-Fourier analysis of §9 is, in effect, computing in the mod-2 cohomology of the torus T. Each gate contributes to a single 1-dimensional subspace $\{0, \alpha, 2\alpha\}$ in $\mathbb{F}_3^n$, which is a "degree-1 class" in this cohomology. The Z-cancellation constraint ($f|_Z = 0$) is an arithmetic condition that should translate into a *positivity* or *nefness* constraint on the cohomology class of f.

A Hodge-theoretic lower bound would proceed as follows:

(i) Formulate the Z-cancellation as a positivity condition: vanishing on $Z = \bigcup\{x_i = 0\}$, the normal-crossings boundary of the toric variety, imposes a Lefschetz-type constraint on the $\mathbb{F}_4$-Fourier coefficients.

(ii) Use Hodge–Riemann relations to show that any "positive" function supported on T must have $\mathbb{F}_4$-Fourier support covering at least 2^{n-1} Frobenius orbits.

(iii) Translate back to gate complexity: each gate covers one orbit, so $w \geq 2^{n-1}$.

Step (i) is the critical missing ingredient: a characterisation of the Z-vanishing condition in terms of the Fourier-analytic structure. The interaction between the Boolean arrangement (which defines Z) and the gate arrangement (which defines the linear forms) is precisely the cross-characteristic phenomenon that standard Hodge theory does not address.

Assessment: The Hodge-theoretic approach is not dead — it is the most geometrically natural framework for the problem, and the $\mathbb{F}_4$-Fourier analysis is already a shadow of it. The obstruction is specific: we need a *mod-2 Hodge theory for cross-characteristic arrangements* that relates the Z-vanishing condition to Fourier support size via positivity. This does not yet exist but is a concrete research direction.

11.6 Factorisation and coordinate-separability

Any weight-w representation factors through a linear map $\Lambda\colon \mathbb{F}_3^n \to \mathbb{F}_3^w$, $x \mapsto (\ell_1(x), \ldots, \ell_w(x))$. The result $f = h \circ \Lambda$ where $h\colon \mathbb{F}_3^w \to \mathbb{F}_2$ is *coordinate-separable*: $h(v) = \bigoplus_j g_j(v_j)$. This class of functions is extremely restricted — only $\sim 6^w$ distinct functions versus 2^{3^w} total Boolean functions on $\mathbb{F}_3^w$ — and must simultaneously satisfy $h|_{\Lambda(T)} = \mathbf{1}$ and $h|_{\Lambda(Z)} = 0$.

Obstruction: While coordinate-separability is a severe constraint, we lack a mechanism to translate it into a lower bound on w. The condition $\Lambda(T) \cap \Lambda(Z) = \varnothing$ requires $\operatorname{rank}(\Lambda) \geq n$, but this gives only $w \geq n$. Extracting a stronger bound from the interplay between separability and the geometric structure of $\Lambda(T)$ and $\Lambda(Z)$ remains open.

11.7 Summary

The lower bound $t(2, 3, n) \geq 2^{n-1}$ is proved in §10 via the coordinate slicing argument. The five other approaches discussed above each encounter specific obstructions. The successful method — a direct induction on the $\mathbb{F}_4$-Fourier support via the Vandermonde structure of the DFT — sidesteps all of these obstructions by working entirely within the $\mathbb{F}_4$-Fourier framework and avoiding any passage through complex analysis, polynomial degree, or Hodge theory.

The Hodge-theoretic perspective of §11.5 remains of independent interest: it connects the gate complexity problem to the intersection theory of toric varieties and matroid invariants, and may be relevant to generalisations beyond $q = 3$.

12 Discussion

12.1 Comparison of $q = 2$ and $q = 3$

	$q = 2$	$q = 3$
Formula	$2^n - 1$	2^{n-1}
Growth base	2	2
Nontrivial Fourier modes per gate	1	2
$\lvert T \rvert$	1	2^n
Proof method	Fourier support	$\mathbb{F}_4$-Vandermonde induction

Both formulas grow exponentially with base 2, despite the gate field changing from $\mathbb{F}_2$ to $\mathbb{F}_3$. This suggests the bottleneck is controlled by the target field $\mathbb{F}_p = \mathbb{F}_2$ rather than the gate field. For $q = 2$, each gate covers one Fourier mode and $2^n - 1$ modes are needed. For $q = 3$, each gate covers one Frobenius orbit (two modes) and 2^{n-1} orbits are needed. The factor-of-two saving from $q = 2$ to $q = 3$ reflects the richer multiplicative structure of $\mathbb{F}_3^*$ versus $\mathbb{F}_2^*$.

12.2 Connections to $\mathrm{AC}^0[6]$

In a depth-2 circuit with MOD-3 bottom gates and a MOD-2 top gate, each bottom gate computes $\ell_i(u) \bmod 3$ for an affine form ℓ_i, and the top gate applies an arbitrary $g\colon \mathbb{F}_3 \to \mathbb{F}_2$. Theorem 10.3 shows that any such circuit computing $\mathbf{1}_T$ requires $\geq 2^{n-1}$ bottom gates — an exponential lower bound for this restricted model. While far from a full $\mathrm{AC}^0[6]$ lower bound, it captures the essential cross-characteristic difficulty.

12.3 Further directions

1. *General* $t(2, q, n)$. For odd primes $q > 3$, the torus $T = (\mathbb{F}_q^*)^n$ is larger and the $\mathbb{F}_{q^2}$-DFT matrix has a richer Vandermonde structure. The coordinate slicing argument generalises: the $q \times (q-1)$ Vandermonde matrix over $\mathbb{F}_{q^2}$ with nodes the $(q-1)$-st roots of unity determines the branching factor in the induction. Working out the exact formula for $t(2, q, n)$ is the natural next step.

2. *General $t(p, q, n)$.* For $p > 2$, the target field is no longer $\mathbb{F}_2$, and the Frobenius pairing has order $p-1$ rather than 2. The gate complexity $t(p, q, n)$ for p, q distinct primes remains open for $p \geq 3$, $q \geq 3$.

3. *Cross-characteristic coding theory.* The code $\mathcal{C}/\mathcal{C}_0$ is a new object. Understanding its weight enumerator, dual code, and MacWilliams relations in the cross-characteristic setting may yield further structural results.

4. *Hodge-theoretic interpretation.* The analysis of §11.5 connects the gate complexity to intersection theory on $(\mathbb{P}^1)^n$. With the lower bound now established by elementary means, it would be illuminating to find a geometric proof via the Hodge–Riemann relations, which could provide a conceptual explanation for why $\mathbf{1}_T$ uniquely minimises the Fourier support.

5. *Étale-cohomological interpretation.* The cross-characteristic map $\mathbb{F}_3 \to \mathbb{F}_2$ is naturally an ℓ-adic ($\ell = 2$) operation on $\mathbb{F}_3$-points. The $\mathbb{F}_4$-Fourier transform computes in $H^*_{\text{ét}}(T, \mathbb{F}_2)$; the coordinate slicing proof may admit a cohomological interpretation in terms of the Künneth decomposition of $T = (\mathbb{F}_3^*)^n$.

Acknowledgments

(To be added.)

References

[1] A. A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes*, 41(4):333–338, 1987.

[2] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th ACM STOC*, pages 77–82, 1987.

[3] A. A. Razborov. Bounded arithmetic and lower bounds in Boolean complexity. In *Feasible Mathematics II*, pages 344–386. Birkhäuser, 1995.

[4] B. Green and T. Tao. The distribution of polynomials over finite fields, with applications to the Gowers norms. *Contributions to Discrete Mathematics*, 4(2), 2009.

[5] E. Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[6] R. Williams. Nonuniform ACC circuit lower bounds. *Journal of the ACM*, 61(1):1–32, 2014.

[7] E. Chattopadhyay and J. Liao. Explicit separations between randomized and deterministic communication for small rounds. *Electronic Colloquium on Computational Complexity*, 2025.

[8] J. P. Hansen. Toric varieties, Hirzebruch surfaces and error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing*, 13(4):289–300, 2002.

[9] I. Soprunov and J. Soprunova. Toric surface codes and Minkowski length of polygons. *SIAM Journal on Discrete Mathematics*, 23(1):384–400, 2009.

[10] J. Huh and E. Katz. Log-concavity of characteristic polynomials and the Bergman fan of matroids. *Mathematische Annalen*, 354(3):1103–1116, 2012.

[11] K. Adiprasito, J. Huh, and E. Katz. Hodge theory for combinatorial geometries. *Annals of Mathematics*, 188(2):381–452, 2018.

[12] C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Applied Mathematics*, 55(2):119–128, 1976.

[13] D. A. M. Barrington, H. Straubing, and D. Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, 1990.