Cross-Characteristic Gate Complexity of the Algebraic Torus

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

February 2026

Abstract

We determine 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 is a prime and q is a prime power with $\mathrm{char}(\mathbb{F}_q) \neq p$. This quantity, the gate complexity $t(p, q, n)$, captures the essential cross-characteristic difficulty arising 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 Walsh–Fourier analysis (§4).

Our main result determines $t(2, q, n)$ for all odd prime powers q:

$$t(2, q, n) = (q-1)^{n-1} \quad \text{for all odd prime powers } q \text{ and all } n \geq 1.$$

The upper bound (§5) is an explicit character-sum construction of $(q-1)^{n-1}$ gates whose $\mathbb{F}_2$-sum equals $\mathbf{1}_T$. The matching lower bound (§6) proceeds by a Frobenius orbit counting argument over $\mathbb{F}_{2^k}$ (where k is the order of 2 in $\mathbb{F}_q^*$): the self-duality $\widehat{\mathbf{1}_T} = \mathbf{1}_T$ forces every Frobenius orbit in T to be covered by some gate, and each gate covers at most $(q-1)/k$ of the $(q-1)^n/k$ orbits. The factors of k cancel, yielding the clean bound $w \geq (q-1)^{n-1}$.

For the special case $q = 3$, we additionally characterise all optimal solutions (§7), establish an independence theorem for canonical gate functions (§8), and give an alternative lower bound proof via coordinate induction on $\mathbb{F}_4$-Fourier support (§10). We show that this Fourier support approach, while successful for $q = 3$, provably fails for $q \geq 5$.

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 $\ell\colon \mathbb{F}_q^n \to \mathbb{F}_q$ is affine and $g\colon \mathbb{F}_q \to \mathbb{F}_p$ is arbitrary. The function $\mathbf{1}_T$ is the canonical "hard function" for this model: it is nonzero precisely on the torus, the complement of the union of coordinate hyperplanes.

Main results

1. **Coding-theoretic framework (§2).** We reduce gate complexity to a minimum coset weight problem in a linear code over $\mathbb{F}_p$, with quotient dimension $\dim(C/C_0) = (q-1)^n$ in the cross-characteristic case (Theorem 3.1).
2. **Exact formula for $q = 2$ (§4).** $t(p, 2, n) = 2^n - 1$ for all primes $p \geq 3$ (Theorem 4.1).
3. **Upper bound for general q (§5).** $t(2, q, n) \leq (q-1)^{n-1}$ for all odd prime powers q, via an explicit character-sum construction (Theorem 5.1).
4. **Matching lower bound (§6).** $t(2, q, n) \geq (q-1)^{n-1}$ for all odd prime powers q, via a Frobenius orbit counting argument that uses the self-duality of $\mathbf{1}_T$ under the $\mathbb{F}_{2^k}$-Fourier transform (Theorem 6.5).
5. **Solution structure for $q = 3$ (§7).** Every optimal gate combination uses the same set of 2^{n-1} linear forms, with $2^{2^{n-1}-1}$ solutions differing only in gate functions (Theorem 7.1).
6. **Gate independence for $q = 3$ (§8).** The canonical gate functions are $\mathbb{F}_2$-linearly independent, proved by a slice-restriction induction (Theorem 8.2).
7. **Alternative lower bound via Vandermonde induction (§10).** For $q = 3$, we give a second proof of the lower bound using an $\mathbb{F}_4$-Fourier support theorem proved by coordinate slicing. We show this approach provably fails for $q \geq 5$ (Remark 10.4).
8. **Computational verification (§11).** $t(2, q, n) = (q-1)^{n-1}$ is verified by exhaustive search for $q \in \{3, 5\}$ and small n, and the upper bound, self-duality, and orbit structure are verified for the prime power $q = 9$ $(= \mathbb{F}_{3^2})$.

Discussion

The conceptual message is a dichotomy: cross-characteristic gates always span the full function space (Theorem 3.1), but doing so efficiently requires overcoming a Fourier-theoretic obstruction that grows exponentially in n. The formula $t(2, q, n) = (q-1)^{n-1}$ reveals that the growth rate is controlled by the torus dimension $|(\mathbb{F}_q^*)|^{n-1} = (q-1)^{n-1}$, with the order k of 2 in $\mathbb{F}_q^*$ playing no role in the final answer despite determining the intermediate structure.

For $q = 3$, the original proof used a Vandermonde induction establishing an $\mathbb{F}_4$-Fourier support theorem: every nonzero $f\colon \mathbb{F}_3^n \to \mathbb{F}_2$ supported on T satisfies $|\operatorname{supp}(\hat{f})| \geq 2^n$. Attempting to generalise this to $q = 5$ led to a surprising discovery: the analogous $\mathbb{F}_{16}$-Fourier support theorem *fails* for $q = 5$. Functions supported on $T \subset \mathbb{F}_5^2$ can have Fourier support as small as $8 < 16 = 4^2$. This obstruction motivated the orbit counting argument, which is both simpler and fully general.

2 The Coding-Theoretic Framework

2.1 Setup and notation

Throughout, p is a prime, q is a prime power with $\operatorname{char}(\mathbb{F}_q) \neq p$, 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 G denote the set of all distinct gate evaluation vectors, with $|G| = G$, and form the gate evaluation matrix $M \in \mathbb{F}_p^{q^n \times G}$.

Definition 2.2. The gate complexity is

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

2.2 The code and its quotient

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

$$C = \ker(M_Z) = \{c \in \mathbb{F}_p^G : M_Z c = 0\}, \qquad C_0 = \ker(M) = \{c \in \mathbb{F}_p^G : Mc = 0\}.$$

The quotient C/C_0 maps isomorphically onto $\mathbb{F}_p^T$: every function $T \to \mathbb{F}_p$ is realisable. The target $\mathbf{1}_T$ determines a coset $c_0 + C_0$ inside C, and $t(p,q,n) = \min_{c \in c_0 + C_0} \mathrm{wt}(c)$.

3 Gate Span Completeness

Theorem 3.1. *Let p be a prime and q a prime power with $\mathrm{char}(\mathbb{F}_q) \neq p$. Then $\mathrm{span}_{\mathbb{F}_p}(G) = \mathbb{F}_p^{\mathbb{F}_q^n}$, and consequently $\dim(C/C_0) = (q-1)^n$.*

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

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

Step 2. Since $\mathrm{char}(\mathbb{F}_q) \neq p$, fix a nontrivial additive character $\psi\colon (\mathbb{F}_q, +) \to \mathbb{F}_p[\zeta]^*$. Multiplying fibre sums by $\psi(v)$ and summing gives $\hat{\lambda}(\psi_a) = 0$ for all nonzero a.

Step 3. Since q^n is coprime to p, the DFT 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 $\dim(C/C_0) = (q-1)^n$. □

Remark 3.2. When $p = \mathrm{char}(\mathbb{F}_q)$, the DFT is not invertible and nontrivial annihilators exist. The quotient dimension collapses: for $p = q = 3$, $n = 2$, one has $\dim(C/C_0) = 1$ 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 $\delta_{(1,\dots,1)}$ 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 $\sum_{S \neq \emptyset} (-1)^{|S|+1} g_S \circ \ell_S$ vanishes on Z and is nonzero on T, by Möbius inversion. □

5 The General Upper Bound

Theorem 5.1. *For all odd prime powers q and all $n \geq 1$: $t(2, q, n) \leq (q-1)^{n-1}$.*

Proof. For each $s = (s_1, \ldots, s_{n-1}) \in (\mathbb{F}_q^*)^{n-1}$, define

$$\ell_s(x) = x_1 + \sum_{j=2}^{n} s_{j-1} x_j, \qquad g_s = \mathbf{1}_{\ell_s \neq 0},$$

where the arithmetic is in $\mathbb{F}_q$. We show $F(x) := \bigoplus_{s \in (\mathbb{F}_q^*)^{n-1}} g_s(x) = \mathbf{1}_T(x)$ for all $x \in \mathbb{F}_q^n$.

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

Character-sum computation of N_0. Fix a nontrivial additive character $\chi\colon (\mathbb{F}_q, +) \to \mathbb{C}^*$. (For q prime, $\chi(x) = e^{2\pi i x/q}$; for $q = r^e$, $\chi(x) = e^{2\pi i \mathrm{Tr}(x)/r}$ where $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_r$ is the field trace.) Character orthogonality gives $\sum_{a \in \mathbb{F}_q} \chi(av) = q\, \delta_{v=0}$ for $v \in \mathbb{F}_q$, so

$$N_0(x) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi(ax_1) \prod_{k=2}^{n} \Big(\sum_{s_k \in \mathbb{F}_q^*} \chi(a s_k x_k) \Big).$$

We evaluate each inner sum $\Sigma_k(a) := \sum_{s \in \mathbb{F}_q^*} \chi(a s x_k)$ by cases:

- If $a = 0$ or $x_k = 0$: $\Sigma_k(a) = q - 1$.
- If $a \neq 0$ and $x_k \neq 0$: the map $s \mapsto a s x_k$ is a bijection on $\mathbb{F}_q^*$ (since $\mathbb{F}_q$ is a field), so $\Sigma_k(a) = \sum_{t \in \mathbb{F}_q^*} \chi(t) = -1$.

Torus case ($x \in T$). All $x_k \neq 0$, so for $a \neq 0$: $\Sigma_k(a) = -1$ for every k, and $\chi(ax_1)$ sums over $a \neq 0$ as $\sum_{a \neq 0} \chi(ax_1) = -1$ (since $x_1 \neq 0$). Therefore:

$$N_0(x) = \frac{1}{q}\Big[(q-1)^{n-1} + (-1)^{n-1} \sum_{a \neq 0} \chi(ax_1)\Big] = \frac{(q-1)^{n-1} + (-1)^n}{q},$$

and $N(x) = \big((q-1)^n - (-1)^n\big)/q$.

Parity on T: Since q is odd, $q-1$ is even, so $(q-1)^n$ is even. Also $(-1)^n$ is odd, so $(q-1)^n - (-1)^n$ is odd. Since $\gcd(q, 2) = 1$, the quotient $N(x) = \big((q-1)^n - (-1)^n\big)/q$ is odd. Hence $F(x) = 1$ for $x \in T$.

Vanishing on Z. Let $x \in Z$. Define $J = \{k \in \{2, \ldots, n\} : x_k = 0\}$ with $|J| = m$, and set $\epsilon = \mathbf{1}_{x_1 \neq 0}$.

For $a = 0$: contribution is $(q-1)^{n-1}/q$.

For $a \neq 0$: the factor from coordinate k is $\Sigma_k(a) = q - 1$ if $k \in J$, and $\Sigma_k(a) = -1$ if $k \notin J$. The factor from coordinate 1 is $\chi(ax_1)$. So the $a \neq 0$ contribution is:

$$\frac{1}{q}(q-1)^m \cdot (-1)^{n-1-m} \cdot \sum_{a \neq 0} \chi(ax_1).$$

Now $\sum_{a \neq 0} \chi(ax_1) = -1$ if $x_1 \neq 0$ and $= q - 1$ if $x_1 = 0$. Since $q \cdot N(x) = q(q-1)^{n-1} - q \cdot N_0(x)$:

$$q \cdot N(x) = (q-1)^n - (-1)^{n-1-m}(q-1)^m \cdot \begin{cases} -1 & \text{if } x_1 \neq 0, \\ (q-1) & \text{if } x_1 = 0. \end{cases}$$

We verify $q \cdot N(x)$ is even in all boundary cases. Since $x \in Z$, either $x_1 = 0$ or $m \geq 1$.

Case 1: $x_1 \neq 0$, $m \geq 1$. Then $q \cdot N(x) = (q-1)^n + (-1)^{n-1-m}(q-1)^m$. Both terms contain the factor $(q-1)$ raised to a power ≥ 1. Since $q-1$ is even, both terms are even, hence $q \cdot N(x)$ is even.

Case 2: $x_1 = 0$. Then $q \cdot N(x) = (q-1)^n - (-1)^{n-1-m}(q-1)^{m+1}$. The first term has factor $(q-1)^n$ with $n \geq 1$; the second has $(q-1)^{m+1}$ with $m+1 \geq 1$. Both are even.

In both cases $q \cdot N(x)$ is even. Since q is odd, $N(x)$ is even, giving $F(x) = 0$. □

Remark 5.2. For $q = 3$, the quantity $(2^n - (-1)^n)/3$ is the nth Jacobsthal number. The general formula $((q-1)^n - (-1)^n)/q$ is its base-$(q-1)$ analogue. The proof uses only that $\mathbb{F}_q$ is a finite field of odd order — in particular, it applies equally to prime powers $q = r^e$.

6 The Orbit Counting Lower Bound

This section contains the main result. The proof is clean, uniform in q, and avoids any Vandermonde or coordinate-slicing analysis.

6.1 The $\mathbb{F}_{2^k}$-Fourier transform

Let q be an odd prime power with $\mathrm{char}(\mathbb{F}_q) = r$, and let k be the multiplicative order of the element $2 \in \mathbb{F}_q^*$. Since 2 lies in the prime subfield $\mathbb{F}_r \subset \mathbb{F}_q$, we have $k = \mathrm{ord}_r(2)$; in particular, k depends only on the characteristic r, not on q itself. Since $r \mid 2^k - 1$, $\mathbb{F}_{2^k}$ contains a primitive rth root of unity ζ.

Fix the nontrivial additive character $\chi \colon \mathbb{F}_q \to \mathbb{F}_{2^k}^*$ defined by $\chi(x) = \zeta^{\mathrm{Tr}(x)}$, where $\mathrm{Tr} \colon \mathbb{F}_q \to \mathbb{F}_r$ is the field trace. (For q prime, this reduces to $\chi(x) = \zeta^x$.) The $\mathbb{F}_{2^k}$-Fourier transform of $f \colon \mathbb{F}_q^n \to \mathbb{F}_{2^k}$ is

$$\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_q^n} f(x)\, \chi(-\alpha \cdot x), \qquad \alpha \in \mathbb{F}_q^n,$$

where $\alpha \cdot x = \sum_i \alpha_i x_i \in \mathbb{F}_q$. Since $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$, any function $f \colon \mathbb{F}_q^n \to \mathbb{F}_2$ has a well-defined $\mathbb{F}_{2^k}$-Fourier transform.

The *Frobenius* $\sigma \colon x \mapsto x^2$ acts on $\mathbb{F}_{2^k}$ with order k. Since Tr is $\mathbb{F}_r$-linear and $2 \in \mathbb{F}_r$, we have $\sigma(\chi(v)) = \chi(v)^2 = \zeta^{2\,\mathrm{Tr}(v)} = \zeta^{\mathrm{Tr}(2v)} = \chi(2v)$, so σ acts on $\mathbb{F}_q^n$ as $\alpha \mapsto 2\alpha$ (scalar multiplication by $2 \in \mathbb{F}_q$). For f taking values in $\mathbb{F}_2 = \mathbb{F}_{2^k}^{\sigma}$:

$$\hat{f}(2\alpha) = \hat{f}(\alpha)^2, \tag{1}$$

so the Fourier support is a union of Frobenius orbits.

6.2 Self-duality of $\mathbf{1}_T$

Proposition 6.1. *Over* $\mathbb{F}_{2^k}$*:* $\widehat{\mathbf{1}_T} = \mathbf{1}_T$*. That is,* $\widehat{\mathbf{1}_T}(\alpha) = 1$ *if* $\alpha \in T$ *and* $\widehat{\mathbf{1}_T}(\alpha) = 0$ *if* $\alpha \notin T$*.*

Proof. The torus indicator factorises: $\mathbf{1}_T(x) = \prod_{j=1}^n \mathbf{1}_{x_j \neq 0}$. The Fourier transform factorises accordingly:

$$\widehat{\mathbf{1}_T}(\alpha) = \prod_{j=1}^{n} \Big(\sum_{c \in \mathbb{F}_q^*} \chi(-\alpha_j c) \Big).$$

For each factor:

- If $\alpha_j \neq 0$: $\sum_{c\in\mathbb{F}_q^*} \chi(-\alpha_j c) = \sum_{c\in\mathbb{F}_q} \chi(-\alpha_j c) - 1 = 0 - 1 = -1 = 1$ in $\mathbb{F}_{2^k}$ (since char = 2). Here the full character sum vanishes because $c \mapsto -\alpha_j c$ is a bijection and χ is nontrivial.
- If $\alpha_j = 0$: $\sum_{c\in\mathbb{F}_q^*} \chi(0) = q - 1 \equiv 0$ in $\mathbb{F}_{2^k}$ (since q is odd, $q-1$ is even).

Therefore $\widehat{\mathbf{1}_T}(\alpha) = \prod_j [\alpha_j \neq 0] = \mathbf{1}_T(\alpha)$. □

Corollary 6.2. $\mathrm{supp}(\widehat{\mathbf{1}_T}) = T$, *with* $|\mathrm{supp}(\widehat{\mathbf{1}_T})| = (q-1)^n$.

6.3 Gate Fourier support

Lemma 6.3. *Let $g \circ \ell$ be a gate with $\ell(x) = a \cdot x + b$. Then $\mathrm{supp}(\widehat{g \circ \ell}) \subseteq \mathbb{F}_q \cdot a$.*

Proof. We have $\widehat{g \circ \ell}(\alpha) = \sum_{v\in\mathbb{F}_q} g(v) \sum_{\{x: a\cdot x + b = v\}} \omega^{-\alpha\cdot x}$. The inner sum over the affine hyperplane $\{x : a \cdot x = v - b\}$ vanishes unless $\alpha \in (\ker a)^\perp = \mathbb{F}_q \cdot a$. □

6.4 Frobenius orbits

The Frobenius $\alpha \mapsto 2\alpha$ acts on $T = (\mathbb{F}_q^*)^n$ with orbits of size exactly k (the order of 2 in $\mathbb{F}_q^*$).

Lemma 6.4. *(a) T has $(q-1)^n/k$ Frobenius orbits.*

(b) Each $\mathbb{F}_q$-line $\mathbb{F}_q \cdot a$ (for $a \in T$) meets T in $\{ta : t \in \mathbb{F}_q^*\}$, which consists of $(q-1)/k$ Frobenius orbits.

Proof. For (a): every Frobenius orbit in T has size exactly k since the order of 2 in $\mathbb{F}_q^*$ is k and the action is free on T. For (b): $\mathbb{F}_q^*$ decomposes into $(q-1)/k$ orbits under scalar multiplication by $2 \in \mathbb{F}_q^*$, and $\{ta : t \in \mathbb{F}_q^*\}$ inherits this decomposition. (That $k \mid q-1$ follows from Lagrange's theorem applied to $\mathbb{F}_q^*$.) □

6.5 The main theorem

Theorem 6.5. *For all odd prime powers q and all $n \geq 1$: $t(2, q, n) \geq (q-1)^{n-1}$.*

Proof. Suppose $\mathbf{1}_T = g_1 \circ \ell_1 \oplus \cdots \oplus g_w \circ \ell_w$. By linearity of the $\mathbb{F}_{2^k}$-Fourier transform:

$$\widehat{\mathbf{1}_T} = \sum_{i=1}^{w} \widehat{g_i \circ \ell_i}. \tag{2}$$

By Corollary 6.2, $\widehat{\mathbf{1}_T}(\alpha) \neq 0$ for every $\alpha \in T$. For any Frobenius orbit $O \subset T$, fix $\alpha \in O$; then $\widehat{\mathbf{1}_T}(\alpha) = 1 \neq 0$, so at least one summand $\widehat{g_i \circ \ell_i}(\alpha)$ is nonzero. By Lemma 6.3, $\alpha \in \mathbb{F}_q \cdot a_i$, meaning O is one of the Frobenius orbits lying on the line $\mathbb{F}_q \cdot a_i$.

Each gate's line $\mathbb{F}_q \cdot a_i$ covers at most $(q-1)/k$ Frobenius orbits in T (Lemma 6.4(b)). The w gates together cover at most $w \cdot (q-1)/k$ orbits. Since all $(q-1)^n/k$ orbits must be covered:

$$w \cdot \frac{q-1}{k} \geq \frac{(q-1)^n}{k},$$

giving $w \geq (q-1)^{n-1}$. □

Theorem 6.6. *For all odd prime powers q and all $n \geq 1$: $t(2, q, n) = (q-1)^{n-1}$.*

Proof. Combine Theorem 5.1 (upper bound) and Theorem 6.5 (lower bound). □

Remark 6.7. The factors of k (the order of 2 in $\mathbb{F}_q^*$) cancel perfectly in the lower bound. This means the gate complexity depends only on q and n, not on the multiplicative order of 2. The extension field $\mathbb{F}_{2^k}$ serves as an auxiliary tool but leaves no trace in the final answer. For prime powers $q = r^e$, $k = \mathrm{ord}_r(2)$ depends only on the characteristic r.

Remark 6.8. The orbit counting argument succeeds because it asks only whether $\widehat{\mathbf{1}_T}(\alpha) \neq 0$ (which is guaranteed by self-duality) rather than bounding the Fourier support of arbitrary functions. This sidesteps the failure of the $\mathbb{F}_{2^k}$-Fourier support theorem for $q \geq 5$ (see §10).

7 Solution Structure for $q = 3$

Theorem 7.1. *For $q = 3$: 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. 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 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. Flipping an even number of gate functions preserves the global XOR being $\mathbf{1}_T$, giving $2^{2^{n-1}-1}$ valid assignments. □

8 The ψ-Independence Theorem

The construction of §5 (specialised to $q = 3$) uses 2^{n-1} canonical gates $g_s = \mathbf{1}_{\ell_s \neq 0}$. The following theorem shows these are linearly independent, so the canonical construction is locally optimal.

Definition 8.1. 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

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

Theorem 8.2. *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 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 $\psi \neq 1$ since $\psi(1) = 0$.

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

Step 1: Restrict to $\{x_{m+1} = 0\}$. On this slice, $\psi_{(s', s_m)}$ reduces to $\psi_{s'}^{(m-1)}$, independently of s_m. Write $\varepsilon_j(s') = \mathbf{1}_{(s',j) \in S}$ for $j \in \{1,2\}$. The restricted equation becomes $\bigoplus_{s'} (\varepsilon_1(s') \oplus \varepsilon_2(s')) \psi_{s'}^{(m-1)} = 0$. By induction (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 $\{x_{m+1} = 1\}$. On this slice, $\psi_{(s',1)}|_{x_{m+1}=1} \oplus \psi_{(s',2)}|_{x_{m+1}=1} = \mathbf{1}_{\ell_{s'} \neq 0} = 1 \oplus \psi_{s'}^{(m-1)}$. Summing over $s' \in S_0$: $\bigoplus_{s' \in S_0} (1 \oplus \psi_{s'}^{(m-1)}) = 0$, giving $\bigoplus_{s' \in S_0} \psi_{s'}^{(m-1)} = |S_0| \bmod 2$.

If $|S_0|$ is even, induction (a) gives $S_0 = \emptyset$. If $|S_0|$ is odd, induction (b) is contradicted. Either way $S = \emptyset$, proving (a). Part (b) follows similarly by restricting the equation $\bigoplus_S \psi_s = 1$ to $\{x_{m+1} = 0\}$ and applying induction (b). $\square$

Corollary 8.3. *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 $\mathbb{F}_3^n$.*

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 $\mathbf{1}_T = \prod_i \mathbf{1}_{x_i\neq 0}$:

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

Every additive character of $\mathbb{F}_3^n$ appears with nonzero coefficient.

9.2 The mod-2 hyperplane arrangement on T

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 $\{[a_s] : s \in (\mathbb{F}_3^*)^{n-1}\}$ contribute rows that 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 8.2. Non-canonical directions with $a_1 = 0$ restrict to pullbacks from $(\mathbb{F}_3^*)^{n-1}$, which lie in the span of the canonical rows by induction. Hence no non-canonical direction increases the rank. $\square$

9.3 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.

10 The Vandermonde Induction for $q = 3$

For the special case $q = 3$, we give an alternative lower bound proof that establishes a stronger result: an $\mathbb{F}_4$-Fourier support theorem for all functions supported on T.

10.1 Coordinate slicing

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

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

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

For fixed α', 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 Vandermonde matrix over $\mathbb{F}_4$ has every 2×2 submatrix nonsingular:

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 is nonzero, then $\hat{f}(\alpha_1, \alpha') \neq 0$ for all α_1.
(c) If both are nonzero, then $\hat{f}(\alpha_1, \alpha') = 0$ for exactly one α_1.

Theorem 10.2 ($\mathbb{F}_4$-Support Theorem)**.** *Let $f\colon \mathbb{F}_3^n \to \mathbb{F}_2$ be nonzero with* $\operatorname{supp}(f) \subseteq T$. *Then* $|\operatorname{supp}(\hat{f})| \geq 2^n$.

Proof. By induction on n. The base case $n = 1$ is verified directly. For the inductive step, let $K_i = \operatorname{supp}(\hat{f}_i)$ with $k_i = |K_i|$. By Lemma 10.1:

$$|\operatorname{supp}(\hat{f})| = 3|K_1 \triangle K_2| + 2|K_1 \cap K_2| \geq 2\max(k_1, k_2).$$

Since each nonzero f_i satisfies $\operatorname{supp}(f_i) \subseteq T' = (\mathbb{F}_3^*)^{n-1}$, induction gives $k_i \geq 2^{n-1}$, yielding $|\operatorname{supp}(\hat{f})| \geq 2 \cdot 2^{n-1} = 2^n$. □

Corollary 10.3. $t(2, 3, n) \geq 2^{n-1}$.

Proof. For $f \in C \setminus C_0$, Theorem 10.2 gives $|\operatorname{supp}(\hat{f})| \geq 2^n$, hence $|\operatorname{supp}(\hat{f}) \setminus \{0\}| \geq 2^n - 1$. Since each gate covers at most one Frobenius pair, $2w \geq 2^n - 1$, giving $w \geq 2^{n-1}$. □

Remark 10.4. **Failure for $q \geq 5$.** The $\mathbb{F}_{16}$-Fourier support theorem does *not* hold for $q = 5$. Exhaustive computation for $n = 2$ reveals:

- The minimum Fourier support for a nonzero $f\colon \mathbb{F}_5^2 \to \mathbb{F}_2$ with $\operatorname{supp}(f) \subseteq T$ is $|\operatorname{supp}(\hat{f})| = 8$, not $4^2 = 16$.
- The 10 worst-case functions have Hamming weight 8 or 12 and their Fourier support covers exactly 2 of the 4 Frobenius orbits.
- Several of these functions are coset indicators of index-2 subgroups of $(\mathbb{F}_5^*)^2 \cong (\mathbb{Z}/4\mathbb{Z})^2$.

The obstruction is the Vandermonde structure: the 5×4 Vandermonde matrix V over $\mathbb{F}_{16}$ with nodes at the 5th roots of unity has 4×4 submatrices that can be singular (a degree-3 polynomial over $\mathbb{F}_{16}$ can vanish at up to 3 of the 5 nodes). The coordinate slicing induction yields only $|\operatorname{supp}(\hat{f})| \geq 2 \cdot 4^{n-1}$, a factor of 2 short of the needed 4^n.

This failure motivated the orbit counting argument of §6, which sidesteps the Fourier support theorem entirely.

11 Computational Verification

For $q = 3$, the results $t(2, 3, n) = 2^{n-1}$ for $n \leq 4$ are certified by exhaustive or meet-in-the-middle search. For $q = 5$, exact values are computed for $n \leq 2$, with the upper bound construction and orbit counting lower bound verified for $n \leq 4$.

For the prime power $q = 9$ ($= \mathbb{F}_{3^2}$), the upper bound construction, self-duality $\widehat{\mathbf{1}_T} = \mathbf{1}_T$, and orbit structure are verified for $n \leq 3$. Here $k = \operatorname{ord}_3(2) = 2$ (since the element $2 = -1 \in \mathbb{F}_3$ has order 2), so Frobenius orbits in T have size 2 and $\mathbb{F}_9^*$ decomposes into $(q-1)/k = 4$ orbits per line. The orbit counting yields the correct lower bound $(q-1)^{n-1} = 8^{n-1}$.

Additionally, the structural claims are verified computationally:

- $\operatorname{supp}(\widehat{\mathbf{1}_T}) = T$ for $q \in \{3, 5, 7, 11, 13, 9\}$ and $n \leq 3$ (resp. $n \leq 2$ for $q = 9$).
- Gate Fourier support lies on one $\mathbb{F}_q$-line for $q \in \{3, 5\}$ and $n \leq 2$.
- The orbit counting lower bound matches $(q-1)^{n-1}$ for all tested parameters including $q = 9$.
- For $q = 3$: $\operatorname{rank}_{\mathbb{F}_2}(\Phi) = 2^{n-1}$ for $n \leq 5$.

q	k	n	G	$\lvert T\rvert$	$t(2,q,n)$	Method
3	2	1	8	2	1	trivial
3	2	2	26	4	2	MITM
3	2	3	80	8	4	hybrid
3	2	4	242	16	8	MITM
5	4	1	31	4	1	trivial
5	4	2	181	16	4	exhaustive
$9 = 3^2$	2	1	—	8	1	UB+orbits
$9 = 3^2$	2	2	—	64	8	UB+orbits

Table 1: Gate complexity $t(2, q, n)$ for small parameters. In all cases $t(2, q, n) = (q - 1)^{n-1}$. For $q \leq 5$, exact values are certified by exhaustive search. For $q = 9$, the upper bound construction and orbit counting lower bound are verified directly.

12 The Proof Landscape

We assess the approaches to the lower bound, now that it has been proved by orbit counting (§6) and, for $q = 3$, by Vandermonde induction (§10).

12.1 The polynomial method

Each gate $g \circ \ell$ is a polynomial of degree $\leq q - 1$ over $\mathbb{F}_q$. For the integer-valued sum $H(x) = \sum_{j=1}^{w} h_j(x) \in \{0, \dots, w\}$, we have $H \bmod 2 = \mathbf{1}_T$ and $H \bmod q$ is a low-degree polynomial. For small w, the bounded range of H creates CRT constraints, yielding weak bounds.

Obstruction: At $w \geq q + 1$, all residues modulo $2q$ are achievable and the constraint becomes vacuous.

12.2 Recursive restriction

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

Obstruction: Restriction gives $t(n) \geq t(n - 1)$, never $t(n) \geq (q - 1)\, t(n - 1)$.

12.3 The ψ-independence approach

Theorem 8.2 shows the canonical gates are linearly independent, establishing local optimality. But the full code C_0 has dimension $G - q^n \gg (q - 1)^{n-1}$, and most coset elements involve non-canonical gates.

12.4 Fourier support bounds

For $q = 3$, the $\mathbb{F}_4$-support theorem (Theorem 10.2) gives a tight lower bound. For $q \geq 5$, this fails (Remark 10.4). The orbit counting argument works because it asks only about $\mathbf{1}_T$ rather than all torus-supported functions.

12.5 Factorisation and coordinate-separability

Any weight-w representation factors through $\Lambda\colon \mathbb{F}_q^n \to \mathbb{F}_q^w$. The result $f = h \circ \Lambda$ where h is coordinate-separable. While this is a severe constraint, translating it into a bound on w stronger than $w \geq n$ remains open.

13 Discussion

13.1 Comparison across q

	$q=2$	$q=3$	$q=5$	general q
Formula	2^n-1	2^{n-1}	4^{n-1}	$(q-1)^{n-1}$
Growth base	2	2	4	$q-1$
$\mathbb{F}_{2^k}$-Fourier modes per gate	1	2	4	$q-1$
$\lvert T\rvert$	1	2^n	4^n	$(q-1)^n$
Frobenius orbit size	1	2	4	$k=\mathrm{ord}_r(2)$
Proof method	Walsh–Fourier	orbit counting	orbit counting	orbit counting

The growth base $q-1$ reflects the multiplicative group $\mathbb{F}_q^*$. The gate complexity $t(2,q,n) = (q-1)^{n-1}$ is the number of Frobenius orbits in T, divided by the number of orbits per $\mathbb{F}_q$-line, independent of the Frobenius order k.

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

In a depth-2 circuit with MOD-q bottom gates and a MOD-2 top gate, each bottom gate computes $\ell_i(u) \bmod q$ and the top gate applies an arbitrary $g\colon \mathbb{F}_q \to \mathbb{F}_2$. Theorem 6.6 shows that any such circuit computing $\mathbf{1}_T$ requires $\geq (q-1)^{n-1}$ bottom gates — an exponential lower bound for this restricted model.

13.3 Further directions

1. **General $t(p,q,n)$ for $p>2$.** For $p>2$, the target field is no longer $\mathbb{F}_2$, and the Frobenius has order $\mathrm{ord}_r(p)$ rather than $\mathrm{ord}_r(2)$. The self-duality argument partially generalises: over $\mathbb{F}_{p^k}$ with $k=\mathrm{ord}_r(p)$, the per-coordinate factor for $\alpha_j \neq 0$ is $\sum_{c\in\mathbb{F}_q^*} \chi(-\alpha_j c) = -1$, which is nonzero in $\mathbb{F}_{p^k}$ for all p. However, the $\alpha_j = 0$ factor is $q-1$, which vanishes in $\mathbb{F}_{p^k}$ if and only if $p \mid (q-1)$. When $p \mid (q-1)$, self-duality holds and the orbit counting argument gives $t(p,q,n) \geq (q-1)^{n-1}/\,\mathrm{ord}_r(p)$. When $p \nmid (q-1)$, $\widehat{\mathbf{1}_T}$ has full support on $\mathbb{F}_q^n$, which may yield stronger bounds.

2. **Cross-characteristic coding theory.** The code C/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.

3. **Hodge-theoretic interpretation.** The analysis connects the gate complexity to intersection theory on $(\mathbb{P}^1)^n$. A geometric proof of the lower bound via the Hodge–Riemann relations, explaining why $\mathbf{1}_T$ uniquely minimises gate complexity, remains of independent interest.

4. **Étale-cohomological interpretation.** The cross-characteristic map $\mathbb{F}_q \to \mathbb{F}_2$ is naturally an ℓ-adic ($\ell = 2$) operation on $\mathbb{F}_q$-points. The $\mathbb{F}_{2^k}$-Fourier transform computes in $H^*_{\text{ét}}(T, \mathbb{F}_2)$; the self-duality $\widehat{\mathbf{1}_T} = \mathbf{1}_T$ may admit a cohomological interpretation via the Künneth decomposition of $T = (\mathbb{F}_q^*)^n$.

Acknowledgments

I thank Prof. Makrand Sinha for lecturing on the beautiful topic of analysis on Boolean functions, which initiated this line of thought.

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. *ECCC*, 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.