Gate Complexity of the Algebraic Torus

Abstract

We determine the gate complexity $t(p,q,n)$—the minimum number of 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 $(\mathbb{F}_q^*)^n$ as an $\mathbb{F}_p$-linear combination—for all primes p and prime powers q with $\mathrm{char}(\mathbb{F}_q) \neq p$.

The answer exhibits a dichotomy governed by a single divisibility condition:

$$t(p,q,n) = \begin{cases} (q-1)^{n-1} & \text{if } p \mid (q-1), \\ \dfrac{q^n-1}{q-1} = |\mathbb{P}^{n-1}(\mathbb{F}_q)| & \text{if } p \nmid (q-1). \end{cases}$$

When $p \mid (q-1)$, the $\mathbb{F}_{p^k}$-Fourier transform of $\mathbf{1}_T$ is supported on the torus T, and the optimal construction uses $(q-1)^{n-1}$ gates indexed by $(\mathbb{F}_q^*)^{n-1}$. When $p \nmid (q-1)$, the Fourier transform has full support on $\mathbb{F}_q^n \setminus \{0\}$, and the optimal construction requires one gate per point of $\mathbb{P}^{n-1}(\mathbb{F}_q)$.

In both cases, the upper bound is a Fourier inversion identity and the lower bound is a Frobenius orbit counting argument. We give a cohomological interpretation: the gate complexity equals the Frobenius trace on $H_c^*(\mathbb{G}_m^{n-1}, \mathbb{F}_p)$, connecting cross-characteristic circuit complexity to étale cohomology. For the special case $q = 3$, we additionally characterise all optimal solutions and establish an independence theorem for canonical gate functions.

1 Introduction

A central open problem in circuit complexity is to prove super-polynomial lower bounds for $\mathsf{AC}^0[6]$, 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 $\mathsf{AC}^0[p]$ for prime p [Raz87, Smo87], 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.

The model. The gate complexity model is inherently depth-2: a single layer of affine maps $\ell_i : \mathbb{F}_q^n \to \mathbb{F}_q$ composed with arbitrary functions $g_i : \mathbb{F}_q \to \mathbb{F}_p$, followed by an $\mathbb{F}_p$-linear combination. This corresponds to a depth-2 circuit with one layer of MOD-q gates feeding into a single MOD-p output gate.

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, the complement of the union of coordinate hyperplanes.

Scope and limitations. Our exponential lower bound applies to this restricted depth-2 setting. A full $\mathsf{AC}^0[6]$ circuit has arbitrary constant depth, and the central open problem is precisely to understand how cross-characteristic interactions compose across multiple layers. We do not address depth ≥ 3; rather, we determine the exact cost of a single cross-characteristic layer, which we view as a necessary first step toward understanding the multi-layer case.

1.1 Main Results

Our main result determines the gate complexity for all primes p and prime powers q with $\mathrm{char}(\mathbb{F}_q) \neq p$.

Theorem 1.1 (Main Theorem)**.** *Let p be a prime and q a prime power with $\mathrm{char}(\mathbb{F}_q) \neq p$. Then*

$$t(p,q,n) = \begin{cases} (q-1)^{n-1} & \text{if } p \mid (q-1), \\ \dfrac{q^n-1}{q-1} = |\mathbb{P}^{n-1}(\mathbb{F}_q)| & \text{if } p \nmid (q-1). \end{cases}$$

The dichotomy is governed by a single divisibility condition. Note that for $p = 2$, the condition $2 \mid (q-1)$ holds for all odd q, so the formula simplifies to $t(2,q,n) = (q-1)^{n-1}$. For $q = 2$, we have $q - 1 = 1$, so $p \nmid 1$ for all primes $p \geq 3$, giving $t(p,2,n) = 2^n - 1 = |\mathbb{P}^{n-1}(\mathbb{F}_2)|$.

Additional results.

(1) **Coding-theoretic framework (Section 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.

(2) **Gate span completeness (Theorem 3.1).** Cross-characteristic gates span all functions $\mathbb{F}_q^n \to \mathbb{F}_p$. This fails in same characteristic, explaining the algebraic core of the $\mathsf{AC}^0[6]$ difficulty.

(3) **Fourier support dichotomy (Theorem 4.2).** Over $\mathbb{F}_{p^k}$, the Fourier transform $\widehat{\mathbf{1}_T}$ is supported on T when $p \mid (q-1)$ and on $\mathbb{F}_q^n \setminus \{0\}$ when $p \nmid (q-1)$.

(4) **Cohomological interpretation (Theorem 9.1).** Gate complexity equals the Frobenius trace on étale cohomology: $t(p,q,n) = \mathrm{Tr}(\mathrm{Frob}_q \mid H_c^*(\mathbb{G}_m^{n-1}, \mathbb{F}_p))$. The code quotient C/C_0 is isomorphic to the space of $\mathbb{F}_q^*$-orbit functions on T.

(5) **Solution structure for $q = 3$ (Section 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.

(6) **Gate independence for $q = 3$ (Theorem 7.3).** The canonical gate functions are $\mathbb{F}_2$-linearly independent, proved by a slice-restriction induction.

(7) **Alternative lower bound via Vandermonde induction (Section 8).** For $q = 3$, an $\mathbb{F}_4$-Fourier support theorem gives a second proof. This approach provably fails for $q \geq 5$.

1.2 Techniques

Upper bound. The construction is a Fourier inversion identity decomposed over projective lines. For each projective point $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$, we define a gate $g_{[a]} \circ \ell_a$ where $\ell_a(x) = a \cdot x$ and $g_{[a]}(v) = c_{[a]} \cdot \mathbf{1}_{v=0}$ with explicit coefficients $c_{[a]}$. The key observation is that the coefficients $c_{[a]}$ vanish in $\mathbb{F}_p$ precisely when $p \mid (q-1)$ and $a \notin T$, reducing the gate count from $|\mathbb{P}^{n-1}(\mathbb{F}_q)|$ to $(q-1)^{n-1}$ in this case.

Lower bound. The lower bound proceeds by a Frobenius orbit counting argument. The $\mathbb{F}_{p^k}$-Fourier transform (where $k = \mathrm{ord}_r(p)$ and $r = \mathrm{char}(\mathbb{F}_q)$) has the property that Fourier support is closed under the Frobenius action $\alpha \mapsto p\alpha$. We show:

- Each gate's Fourier support lies on a single $\mathbb{F}_q$-line through the origin.
- Each such line contains at most $(q-1)/k$ Frobenius orbits in its torus part.
- The Fourier support of $\mathbf{1}_T$ consists of all torus orbits (when $p \mid (q-1)$) or all nonzero orbits (when $p \nmid (q-1)$).
- Covering all required orbits forces $w \geq (q-1)^{n-1}$ or $w \geq (q^n-1)/(q-1)$ gates.

The factors of k cancel perfectly, so the final answer depends only on p, q, and n—not on the multiplicative order of p in $\mathbb{F}_r^*$.

Discussion. The conceptual message is a dichotomy: cross-characteristic gates always span the full function space, but doing so efficiently requires overcoming a Fourier-theoretic obstruction that grows exponentially in n. The formula reveals that the growth rate is controlled by either the torus dimension $|(\mathbb{F}_q^*)|^{n-1} = (q-1)^{n-1}$ or the projective space dimension $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = (q^n-1)/(q-1)$, with the divisibility $p \mid (q-1)$ determining which regime applies.

1.3 Related Work

The polynomial method of Razborov [Raz87] and Smolensky [Smo87] gives exponential lower bounds for $\mathsf{AC}^0[p]$ for prime p, but fails for composite moduli. Barrington, Straubing, and Thérien [BST90] studied the algebraic structure of ACC^0 and showed connections to group theory. Viola [Vio09] surveyed the state of small-depth computation and highlighted the $\mathsf{AC}^0[6]$ problem as a central challenge. Williams [Wil14] proved nonuniform ACC^0 lower bounds via a different route (satisfiability algorithms), but the uniform case remains open.

Recent work by Chattopadhyay and Liao [CL25] studies separations in randomized communication complexity, which involves similar cross-characteristic phenomena. The connection between gate complexity and coding theory parallels work on toric codes [Han02, SS09], where code parameters are controlled by lattice geometry.

The Hodge-theoretic perspective on combinatorics, developed by Huh–Katz [HK12] and Adiprasito–Huh–Katz [AHK18], suggests potential geometric approaches to lower bounds. Greene [Gre76] connected weight enumeration to algebraic geometry, providing another angle on the coding-theoretic structure.

1.4 Organization

Section 2 establishes the coding-theoretic framework. Section 3 proves gate span completeness. Section 4 develops the $\mathbb{F}_{p^k}$-Fourier transform and proves the support dichotomy. Section 5 proves the lower bound via orbit counting. Section 6 proves the upper bound via Fourier inversion. Section 7 analyzes the special case $q = 3$ in detail. Section 8 gives the alternative Vandermonde induction proof for $q = 3$ and shows why it fails for $q \geq 5$. Section 9 gives the cohomological interpretation connecting gate complexity to étale cohomology. Section 10 discusses connections to $\mathsf{AC}^0[6]$ and future directions.

2 The Coding-Theoretic Framework

2.1 Setup and Notation

Throughout, p is a prime, q is a prime power with $\mathrm{char}(\mathbb{F}_q) = r \neq p$, 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 $g \circ \ell : \mathbb{F}_q^n \to \mathbb{F}_p$, where $\ell(u) = a \cdot u + b$ is affine ($a \in \mathbb{F}_q^n$, $b \in \mathbb{F}_q$) and $g : \mathbb{F}_q \to \mathbb{F}_p$ 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 $\mathbb{F}_p$:

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

The quotient C/C_0 maps isomorphically onto $\mathbb{F}_p^T$: every function $T \to \mathbb{F}_p$ is realizable. 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 $\lambda : \mathbb{F}_q^n \to \mathbb{F}_p$ 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 fiber 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 $\psi : (\mathbb{F}_q, +) \to \mathbb{F}_p[\zeta]^*$. Multiplying fiber sums by $\psi(v)$ and summing gives $\widehat{\lambda}(\psi_a) = 0$ 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 $\mathsf{AC}^0[6]$.

4 The $\mathbb{F}_{p^k}$-Fourier Transform

4.1 Setup

Let $r = \mathrm{char}(\mathbb{F}_q)$ and $k = \mathrm{ord}_r(p)$, the multiplicative order of p in $\mathbb{F}_r^*$. Since $r \mid p^k - 1$, the field $\mathbb{F}_{p^k}$ contains a primitive rth root of unity ζ.

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

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

Since $\mathbb{F}_p \subset \mathbb{F}_{p^k}$, any function $f : \mathbb{F}_q^n \to \mathbb{F}_p$ has a well-defined $\mathbb{F}_{p^k}$-Fourier transform.

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

$$\widehat{f}(p\alpha) = \widehat{f}(\alpha)^p, \tag{1}$$

so the Fourier support is a union of Frobenius orbits.

4.2 Fourier Support Dichotomy

Proposition 4.1. *Over $\mathbb{F}_{p^k}$, the Fourier transform of $\mathbf{1}_T$ is:*

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

The per-coordinate factor satisfies:

$$S(a) = \begin{cases} q-1 & \text{if } a = 0, \\ -1 & \text{if } a \neq 0. \end{cases}$$

Proof. The torus indicator factorizes as $\mathbf{1}_T(x) = \prod_j \mathbf{1}_{x_j \neq 0}$, so the Fourier transform factorizes. For the sum $S(a) = \sum_{c \in \mathbb{F}_q^*} \chi(-ac)$: if $a = 0$, every term is 1 and $S(0) = q - 1$. If $a \neq 0$, the map $c \mapsto -ac$ is a bijection on $\mathbb{F}_q^*$, so $S(a) = \sum_{t \in \mathbb{F}_q^*} \chi(t) = \sum_{t \in \mathbb{F}_q} \chi(t) - 1 = 0 - 1 = -1$. □

Theorem 4.2 (Fourier Support Dichotomy)**.** *Let $m(\alpha) = |\{j : \alpha_j = 0\}|$ for $\alpha \in \mathbb{F}_q^n$. Then in $\mathbb{F}_{p^k}$:*

$$\widehat{\mathbf{1}_T}(\alpha) = (-1)^{n-m(\alpha)}(q-1)^{m(\alpha)}.$$

Consequently:

(i) If $p \mid (q-1)$: $\widehat{\mathbf{1}_T}(\alpha) \neq 0 \iff \alpha \in T$. In particular, $\widehat{\mathbf{1}_T}(\alpha) = (-1)^n = \mathbf{1}_T(\alpha)$ for $p = 2$, recovering self-duality.

(ii) If $p \nmid (q-1)$: $\widehat{\mathbf{1}_T}(\alpha) \neq 0 \iff \alpha \neq 0$. The Fourier transform has full support on $\mathbb{F}_q^n \setminus \{0\}$.

Proof. By Proposition 4.1, $\widehat{\mathbf{1}_T}(\alpha) = \prod_j S(\alpha_j) = (-1)^{n-m(\alpha)}(q-1)^{m(\alpha)}$. This vanishes in $\mathbb{F}_{p^k}$ if and only if $m(\alpha) \geq 1$ and $q - 1 \equiv 0 \pmod{p}$. □

5 Lower Bound

Lemma 5.1 (Gate Fourier support)**.** *If $g \circ \ell$ is a gate with $\ell(x) = a \cdot x + b$, then* $\operatorname{supp}(\widehat{g \circ \ell}) \subseteq \mathbb{F}_q \cdot a$.

Proof. The Fourier transform of $g \circ \ell$ at α involves a sum over the affine hyperplane $\{x : a \cdot x + b = v\}$. This sum vanishes unless $\alpha \in (\ker a)^\perp = \mathbb{F}_q \cdot a$. □

Lemma 5.2 (Frobenius orbits)**.** *Let $k = \operatorname{ord}_r(p)$. The Frobenius $\alpha \mapsto p\alpha$ acts on $\mathbb{F}_q^n \setminus \{0\}$ with orbits of size dividing k. Each line $\mathbb{F}_q \cdot a$ through a nonzero a contains:*

(a) $(q-1)/k$ Frobenius orbits lying in $\mathbb{F}_q^* \cdot a$ (the torus part of the line), and

(b) one additional orbit $\{0\}$ (which has size 1).

For $a \in T$, the line $\mathbb{F}_q \cdot a$ meets T in exactly $(q-1)/k$ Frobenius orbits.

Proof. The orbits of $\mathbb{F}_q^*$ under multiplication by p have size $k = \operatorname{ord}_r(p)$, giving $(q-1)/k$ orbits. The line $\mathbb{F}_q \cdot a$ intersected with $\mathbb{F}_q^n \setminus \{0\}$ is $\mathbb{F}_q^* \cdot a$, which inherits the orbit decomposition. □

Theorem 5.3 (Lower bound)**.** *For all primes p and prime powers q with $\operatorname{char}(\mathbb{F}_q) \neq p$:*

$$t(p, q, n) \geq \begin{cases} (q-1)^{n-1} & \text{if } p \mid (q-1), \\ \dfrac{q^n - 1}{q-1} & \text{if } p \nmid (q-1). \end{cases}$$

Proof. Suppose $\mathbf{1}_T = \sum_{i=1}^{w} c_i (g_i \circ \ell_i)$ with $c_i \in \mathbb{F}_p^*$. Taking $\mathbb{F}_{p^k}$-Fourier transforms:

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

For any α with $\widehat{\mathbf{1}_T}(\alpha) \neq 0$, at least one gate must satisfy $\widehat{g_i \circ \ell_i}(\alpha) \neq 0$, placing α on the line $\mathbb{F}_q \cdot a_i$ by Lemma 5.1. Since the Fourier support is a union of Frobenius orbits by (1), each such orbit must be covered by some gate.

Case $p \mid (q-1)$**:** By Theorem 4.2(i), the Fourier support is T. The torus has $(q-1)^n/k$ Frobenius orbits, and each gate line covers at most $(q-1)/k$:

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

Case $p \nmid (q-1)$**:** By Theorem 4.2(ii), the Fourier support is $\mathbb{F}_q^n \setminus \{0\}$, which has $(q^n - 1)/k$ Frobenius orbits. Each gate line covers at most $(q-1)/k$ orbits in $\mathbb{F}_q^n \setminus \{0\}$ (namely the orbits in $\mathbb{F}_q^* \cdot a_i$):

$$w \cdot \frac{q-1}{k} \geq \frac{q^n - 1}{k} \implies w \geq \frac{q^n - 1}{q-1} = |\mathbb{P}^{n-1}(\mathbb{F}_q)|.$$ □

Remark 5.4. The factors of k cancel perfectly in the lower bound. This means the gate complexity depends only on q and n, not on the multiplicative order of p. The extension field $\mathbb{F}_{p^k}$ serves as an auxiliary tool but leaves no trace in the final answer.

6 Upper Bound

Theorem 6.1 (Upper bound)**.** *For all primes p and prime powers q with* $\mathrm{char}(\mathbb{F}_q) \neq p$ *and* $n \geq 1$*:*

$$t(p, q, n) \leq \begin{cases} (q-1)^{n-1} & \text{if } p \mid (q-1), \\ \dfrac{q^n - 1}{q-1} & \text{if } p \nmid (q-1). \end{cases}$$

Proof. For each nonzero direction $a \in \mathbb{F}_q^n \setminus \{0\}$, define the homogeneous linear form $\ell_a(x) = a \cdot x$ and the gate function $g_a : \mathbb{F}_q \to \mathbb{F}_p$ by

$$g_a(v) = c_{[a]} \cdot \mathbf{1}_{v=0},$$

where $[a]$ denotes the projective class of a and

$$c_{[a]} = \frac{(-1)^{n-m(a)} \cdot (q-1)^{m(a)}}{q^{n-1}} \in \mathbb{F}_p, \tag{2}$$

with $m(a) = |\{j : a_j = 0\}|$ as before, and q^{n-1} is inverted in $\mathbb{F}_p$ (possible since $\mathrm{char}(\mathbb{F}_q) \neq p$). The coefficient $c_{[a]}$ depends only on the projective class $[a]$ since $m(ta) = m(a)$ for $t \in \mathbb{F}_q^*$.

Claim: The function

$$F(x) = \sum_{[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)} c_{[a]} \cdot \mathbf{1}_{a \cdot x = 0}$$

satisfies $F(x) = \mathbf{1}_T(x) + C$ for a constant $C \in \mathbb{F}_p$.

Proof of claim. Expand each indicator using the additive characters of $\mathbb{F}_q$:

$$\mathbf{1}_{a \cdot x = 0} = \frac{1}{q} \sum_{s \in \mathbb{F}_q} \chi(s \cdot a \cdot x) = \frac{1}{q} + \frac{1}{q} \sum_{s \in \mathbb{F}_q^*} \chi(s \cdot a \cdot x).$$

Substituting into F and using $\alpha = sa$ to parametrize $\mathbb{F}_q^n \setminus \{0\}$:

$$F(x) = C_0 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^n \setminus \{0\}} \frac{c_{[\alpha]}}{q-1} \chi(\alpha \cdot x),$$

where we used the fact that each $\alpha \neq 0$ is counted once for each $s \in \mathbb{F}_q^*$ in its projective class, and the factor $1/(q-1)$ compensates.

By Fourier inversion, $\mathbf{1}_T(x) = q^{-n} \sum_\alpha \widehat{\mathbf{1}_T}(\alpha) \chi(\alpha \cdot x)$. Matching coefficients shows $F(x) = \mathbf{1}_T(x) + C$ for some constant C.

Since a constant function can be absorbed into any single gate (by adjusting $g_a(v)$ for one gate), the number of gates equals the number of projective classes $[a]$ for which $c_{[a]} \neq 0$ in $\mathbb{F}_p$.

Counting nonzero gates. The coefficient $c_{[a]} = (-1)^{n-m(a)}(q-1)^{m(a)}/q^{n-1}$ vanishes in $\mathbb{F}_p$ if and only if $p \mid (q-1)$ and $m(a) \geq 1$ (since q^{n-1} is invertible and $(-1)^{n-m(a)}$ is a unit).

- If $p \mid (q-1)$: $c_{[a]} \neq 0$ only when $m(a) = 0$, i.e., $a \in T$. The number of such projective classes is $|T|/(q-1) = (q-1)^{n-1}$.
- If $p \nmid (q-1)$: $c_{[a]} \neq 0$ for all $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$, giving $(q^n - 1)/(q-1)$ gates. □

Proof of Theorem 1.1. Combine Theorem 5.3 and Theorem 6.1. □

7 The Special Case $q = 3$

For $q = 3$ and $p = 2$, the formula gives $t(2, 3, n) = 2^{n-1}$. This case admits a more detailed analysis.

7.1 Explicit Construction

The gates are indexed by $s \in (\mathbb{F}_3^*)^{n-1} = \{1, 2\}^{n-1}$. For each $s = (s_1, \ldots, s_{n-1})$, define

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

Then $\bigoplus_{s \in \{1,2\}^{n-1}} g_s(\ell_s(x)) = \mathbf{1}_T(x)$ in $\mathbb{F}_2$.

7.2 Solution Structure

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 $1|_T$, 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. □

7.3 The ψ-Independence Theorem

The construction 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 7.2. For $m \geq 0$ and $s = (s_1, \ldots, s_m) \in \{1, 2\}^m$, define $\psi_s : \mathbb{F}_3^{m+1} \to \mathbb{F}_2$ by

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

Theorem 7.3 (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 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 $s' \in S_0$:

$$\bigoplus_{s'\in S_0} (1 \oplus \psi_{s'}^{(m-1)}) = 0, \quad \text{giving} \quad \bigoplus_{s'\in S_0} \psi_{s'}^{(m-1)} = |S_0| \mod 2.$$

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). □

Corollary 7.4. *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* $\mathbb{F}_3^n$*.*

8 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.

8.1 Coordinate Slicing

Write $f : \mathbb{F}_3^n \to \mathbb{F}_4$ and define $f_1(x') = f(1, x')$, $f_2(x') = f(2, x')$ for $x' \in \mathbb{F}_3^{n-1}$. Then

$$\widehat{f}(\alpha_1, \alpha') = \omega^{-\alpha_1} \widehat{f_1}(\alpha') + \omega^{\alpha_1} \widehat{f_2}(\alpha'),$$

since $-2\alpha_1 = \alpha_1$ in $\mathbb{F}_3$, where $\omega = e^{2\pi i/3}$.

For fixed α', the three values $\widehat{f}(0, \alpha')$, $\widehat{f}(1, \alpha')$, $\widehat{f}(2, \alpha')$ are the entries of

$$\begin{pmatrix} 1 & 1 \\ \omega^2 & \omega \\ \omega & \omega^2 \end{pmatrix} \begin{pmatrix} \widehat{f_1}(\alpha') \\ \widehat{f_2}(\alpha') \end{pmatrix}.$$

Since this 3×2 Vandermonde matrix over $\mathbb{F}_4$ has every 2×2 submatrix nonsingular:

Lemma 8.1 (Slicing Lemma)**.** *For each* $\alpha' \in \mathbb{F}_3^{n-1}$*:*

(a) If $\widehat{f_1}(\alpha') = \widehat{f_2}(\alpha') = 0$*, then* $\widehat{f}(\alpha_1, \alpha') = 0$ *for all* α_1*.*

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

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

Theorem 8.2 ($\mathbb{F}_4$-Support Theorem)**.** *Let* $f : \mathbb{F}_3^n \to \mathbb{F}_2$ *be nonzero with* $\mathrm{supp}(f) \subseteq T$*. Then* $|\mathrm{supp}(\widehat{f})| \geq 2^n$*.*

Proof. By induction on n. The base case $n = 1$ is verified directly. For the inductive step, let $K_i = \mathrm{supp}(\widehat{f_i})$ with $k_i = |K_i|$. By Lemma 8.1:

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

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

Corollary 8.3. $t(2, 3, n) \geq 2^{n-1}$*.*

Proof. For $f \in C \setminus C_0$, Theorem 8.2 gives $|\mathrm{supp}(\widehat{f})| \geq 2^n$, hence $|\mathrm{supp}(\widehat{f}) \setminus \{0\}| \geq 2^n - 1$. Since each gate covers at most one Frobenius pair, $2w \geq 2^n - 1$, giving $w \geq 2^{n-1}$. □

8.2 Failure for $q \geq 5$

Remark 8.4 (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 $f : \mathbb{F}_5^2 \to \mathbb{F}_2$ with $\mathrm{supp}(f) \subseteq T$ is $|\mathrm{supp}(\widehat{f})| = 8$, 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 $|\mathrm{supp}(\widehat{f})| \geq 2 \cdot 4^{n-1}$, a factor of 2 short of the needed 4^n.

This failure motivated the orbit counting argument of Section 5, which sidesteps the Fourier support theorem entirely.

9 Cohomological Interpretation

The gate complexity admits a striking cohomological interpretation: it equals the Frobenius trace on the étale cohomology of the orbit space of the Fourier support.

9.1 Two Orbit Spaces

The multiplicative group $\mathbb{F}_q^*$ acts diagonally on $\mathbb{F}_q^n \setminus \{0\}$:

$$t \cdot (x_1, \ldots, x_n) = (tx_1, \ldots, tx_n).$$

This action restricts to the torus $T = (\mathbb{F}_q^*)^n$. The two relevant orbit spaces are:

1. **The torus quotient:** $T/\mathbb{F}_q^* \cong (\mathbb{F}_q^*)^{n-1}$ via $(x_1, \ldots, x_n) \mapsto (x_2/x_1, \ldots, x_n/x_1)$.

$$|T(\mathbb{F}_q)/\mathbb{F}_q^*| = \frac{(q-1)^n}{q-1} = (q-1)^{n-1}.$$

2. **Projective space:** $(\mathbb{F}_q^n \setminus \{0\})/\mathbb{F}_q^* = \mathbb{P}^{n-1}(\mathbb{F}_q)$.

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{q^n - 1}{q-1} = 1 + q + q^2 + \cdots + q^{n-1}.$$

The torus quotient embeds in projective space: $(\mathbb{F}_q^*)^{n-1} \cong T/\mathbb{F}_q^* \hookrightarrow \mathbb{P}^{n-1}$. The complement is the coordinate hyperplane arrangement.

9.2 Equivariance of the Fourier Transform

The $\mathbb{F}_{p^k}$-Fourier transform is $\mathbb{F}_q^*$-equivariant:

$$\widehat{f(t \cdot -)}(\alpha) = \widehat{f}(t^{-1}\alpha).$$

Thus the Fourier support $\mathrm{supp}(\widehat{f})$ is $\mathbb{F}_q^*$-invariant, and the orbit space $\mathrm{supp}(\widehat{f})/\mathbb{F}_q^*$ is well-defined.

9.3 The Unified Cohomological Theorem

Let $S = \mathrm{supp}(\widehat{\mathbf{1}_T}) \subseteq \mathbb{F}_q^n$ denote the Fourier support of the torus indicator.

Theorem 9.1 (Gate Complexity as Frobenius Trace—Unified)**.** *For all primes p and prime powers q with $\mathrm{char}(\mathbb{F}_q) \neq p$:*

$$t(p, q, n) = |S/\mathbb{F}_q^*| = \mathrm{Tr}(\mathrm{Frob}_q \mid H^*(S/\mathbb{F}_q^*, \mathbb{F}_p)),$$

where:

Condition	*Support S*	*Orbit space $S/\mathbb{F}_q^*$*	$t(p, q, n)$
$p \mid (q-1)$	T	$\mathbb{G}_m^{n-1}$	$(q-1)^{n-1}$
$p \nmid (q-1)$	$\mathbb{F}_q^n \setminus \{0\}$	$\mathbb{P}^{n-1}$	$(q^n-1)/(q-1)$

Proof. We prove each case separately.

Case 1: $p \mid (q-1)$**.** By Theorem 4.2, $\mathrm{supp}(\widehat{\mathbf{1}_T}) = T$, so $S/\mathbb{F}_q^* = T/\mathbb{F}_q^* \cong \mathbb{G}_m^{n-1}$.

The compactly supported cohomology of $\mathbb{G}_m$ over $\overline{\mathbb{F}_q}$ with $\mathbb{F}_p$-coefficients is:

$$H_c^i(\mathbb{G}_m, \mathbb{F}_p) = \begin{cases} \mathbb{F}_p & i = 1, 2 \\ 0 & \text{otherwise} \end{cases}$$

with Frobenius eigenvalue 1 on H_c^1 and eigenvalue q on H_c^2. The alternating trace is:

$$\mathrm{Tr}(\mathrm{Frob}_q \mid H_c^*(\mathbb{G}_m, \mathbb{F}_p)) = -1 + q = q - 1 = |\mathbb{G}_m(\mathbb{F}_q)|.$$

By Künneth, for $\mathbb{G}_m^{n-1}$:

$$\mathrm{Tr}(\mathrm{Frob}_q \mid H_c^*(\mathbb{G}_m^{n-1}, \mathbb{F}_p)) = (q-1)^{n-1} = t(p, q, n).$$

□

Case 2: $p \nmid (q-1)$**.** By Theorem 4.2, $\mathrm{supp}(\widehat{\mathbf{1}_T}) = \mathbb{F}_q^n \setminus \{0\}$, so $S/\mathbb{F}_q^* = \mathbb{P}^{n-1}$.

The cohomology of projective space over $\overline{\mathbb{F}_q}$ is:

$$H^k(\mathbb{P}^{n-1}, \mathbb{F}_p) = \begin{cases} \mathbb{F}_p & k = 0, 2, 4, \ldots, 2(n-1) \\ 0 & \text{otherwise} \end{cases}$$

with Frobenius eigenvalue $q^{k/2}$ on H^k. The trace is:

$$\mathrm{Tr}(\mathrm{Frob}_q \mid H^*(\mathbb{P}^{n-1}, \mathbb{F}_p)) = \sum_{j=0}^{n-1} q^j = \frac{q^n - 1}{q - 1} = |\mathbb{P}^{n-1}(\mathbb{F}_q)| = t(p, q, n).$$

9.4 The Localization Sequence

The inclusion $\mathbb{G}_m^{n-1} \hookrightarrow \mathbb{P}^{n-1}$ (as the complement of coordinate hyperplanes) gives rise to a localization sequence in cohomology:

$$\cdots \to H_c^k(\mathbb{G}_m^{n-1}, \mathbb{F}_p) \to H^k(\mathbb{P}^{n-1}, \mathbb{F}_p) \to H^k(Z, \mathbb{F}_p) \to \cdots$$

where $Z = \mathbb{P}^{n-1} \setminus \mathbb{G}_m^{n-1}$ is the boundary (coordinate hyperplane arrangement).

The Frobenius traces satisfy:

$$\begin{aligned} \mathrm{Tr}(\mathrm{Frob} \mid H^*(\mathbb{P}^{n-1})) &= \frac{q^n - 1}{q - 1}, \\ \mathrm{Tr}(\mathrm{Frob} \mid H_c^*(\mathbb{G}_m^{n-1})) &= (q-1)^{n-1}, \\ \mathrm{Tr}(\mathrm{Frob} \mid H^*(Z)) &= \frac{q^n - 1}{q - 1} - (q-1)^{n-1} \quad \text{(by additivity).} \end{aligned}$$

Proposition 9.2 (Boundary Vanishing)**.** *When $p \mid (q-1)$:*

$$\mathrm{Tr}(\mathrm{Frob} \mid H^*(Z)) \equiv 0 \pmod{p}.$$

Proof. When $p \mid (q-1)$, we have $q \equiv 1 \pmod{p}$, so:

$$\frac{q^n - 1}{q-1} = 1 + q + \cdots + q^{n-1} \equiv n \pmod{p},$$

and $(q-1)^{n-1} \equiv 0 \pmod{p}$ for $n \geq 2$. Thus the boundary trace is $\equiv n \pmod{p}$.

However, the *Fourier-theoretic* vanishing is stronger: the Fourier coefficients $\widehat{\mathbf{1}_T}(\alpha)$ vanish identically for $\alpha \in Z$ (not just mod p), because each such coefficient factors through $\sum_{t \in \mathbb{F}_q^*} \chi(t) = 0$ when one coordinate of α is zero and another is nonzero. □

9.5 The Code Quotient as Orbit Functions

Proposition 9.3. *When $p \mid (q-1)$, the code quotient C/C_0 is isomorphic to the space of $\mathbb{F}_q^*$-orbit functions on T:*

$$C/C_0 \cong \mathbb{F}_p^{T/\mathbb{F}_q^*} \cong \mathbb{F}_p^{(q-1)^{n-1}}.$$

When $p \nmid (q-1)$, the code quotient satisfies:

$$\dim(C/C_0) = |\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{q^n - 1}{q-1}.$$

Proof sketch. In both cases, define $\pi : C \to \mathbb{F}_p^{S/\mathbb{F}_q^*}$ by $\pi(f)([\alpha]) = \sum_{\beta \in [\alpha]} \widehat{f}(\beta)$, summing over the $\mathbb{F}_q^*$-orbit of α in the Fourier support S.

The key observation is that the Fourier support condition defining C (namely $\widehat{f}|_T = 0$ or $\widehat{f}|_{\mathbb{F}_q^n \setminus \{0\}} = 0$ depending on the case) interacts with the orbit structure to give $\ker(\pi|_C) = C_0$. □

9.6 Geometric Interpretation of the Dichotomy

Remark 9.4 (Cohomological Origin of the Dichotomy). The dichotomy $p \mid (q-1)$ vs. $p \nmid (q-1)$ has a clean cohomological explanation:

- The Frobenius eigenvalues on $H^*(\mathbb{P}^{n-1})$ are $1, q, q^2, \ldots, q^{n-1}$.
- When $p \mid (q-1)$: $q \equiv 1 \pmod{p}$, so all eigenvalues collapse to 1 in $\mathbb{F}_p$. The "boundary" cohomology (from $Z = \mathbb{P}^{n-1} \setminus \mathbb{G}_m^{n-1}$) becomes invisible mod p.
- When $p \nmid (q-1)$: the eigenvalues $1, q, q^2, \ldots$ remain distinct in $\mathbb{F}_p$, and the full projective space contributes.

This eigenvalue collapse is analogous to the splitting of Hodge filtrations in p-adic Hodge theory when certain divisibility conditions are met.

9.7 The Depth Filtration

The Fourier support admits a natural stratification by coordinate structure, leading to a filtration of gate complexities.

Definition 9.5 (Depth Filtration)**.** For $0 \leq k \leq n-1$, define:

$$F_k = \{x \in \mathbb{F}_q^n \setminus \{0\} : \text{at most } k \text{ coordinates of } x \text{ are zero}\}.$$

The **depth-k gate complexity** is

$$t_k(p, q, n) = |F_k \cap \operatorname{supp}(\widehat{\mathbf{1}_T})/\mathbb{F}_q^*|.$$

Note that $F_0 = T$ (the torus), and $F_{n-1} = \mathbb{F}_q^n \setminus \{0\}$. The filtration is nested:

$$F_0 \subset F_1 \subset \cdots \subset F_{n-1},$$

inducing $t_0 \leq t_1 \leq \cdots \leq t_{n-1} = t(p, q, n)$.

Proposition 9.6 (Depth Filtration Dichotomy)**.** *1. When $p \mid (q-1)$: $t_k(p, q, n) = (q-1)^{n-1}$ for all k. The filtration collapses.*

2. When $p \nmid (q-1)$: the filtration is strict, with

$$t_k(p, q, n) = \sum_{j=0}^{k} \binom{n}{j} (q-1)^{n-j-1}.$$

Proof. When $p \mid (q-1)$, $\operatorname{supp}(\widehat{\mathbf{1}_T}) = T = F_0$ by Theorem 4.2, so $F_k \cap \operatorname{supp}(\widehat{\mathbf{1}_T}) = T$ for all k.

When $p \nmid (q-1)$, $\operatorname{supp}(\widehat{\mathbf{1}_T}) = \mathbb{F}_q^n \setminus \{0\}$, so $F_k \cap \operatorname{supp}(\widehat{\mathbf{1}_T}) = F_k$. The stratum with exactly j zero coordinates contributes $\binom{n}{j}$ choices for which coordinates vanish, and each such stratum is isomorphic to $(\mathbb{F}_q^*)^{n-j}$, giving $(q-1)^{n-j-1}$ orbits under the diagonal $\mathbb{F}_q^*$-action. ∎

Example 9.7 ($q = 3$, $n = 2$)**.**

- For $p = 2$ ($p \mid 2$): $t_0 = t_1 = 2$.
- For $p = 5$ ($p \nmid 2$): $t_0 = 2$, $t_1 = 2 + 2 \cdot 1 = 4 = |\mathbb{P}^1(\mathbb{F}_3)|$.

Remark 9.8 (Cohomological Interpretation of Depth). The depth filtration corresponds to the stratification of $\mathbb{P}^{n-1}$ by coordinate hyperplanes. The cohomology of each stratum Σ_j (points with exactly j zero homogeneous coordinates) contributes to the graded piece:

$$\operatorname{gr}_j(t) = t_j - t_{j-1} = \binom{n}{j} (q-1)^{n-j-1} \quad (\text{when } p \nmid (q-1)).$$

This matches the Frobenius trace on $H_c^*(\Sigma_j/\mathbb{F}_q^*, \mathbb{F}_p)$.

10 Discussion

10.1 Comparison Across q

	$q = 2$	$q = 3$	$q = 5$	general q
Formula (when $p \mid (q-1)$)	—	2^{n-1}	4^{n-1}	$(q-1)^{n-1}$
Formula (when $p \nmid (q-1)$)	$2^n - 1$	$(3^n - 1)/2$	$(5^n - 1)/4$	$(q^n - 1)/(q-1)$
Growth base	2	2 or 3/2	4 or 5/4	$q-1$ or q
$\|T\|$	1	2^n	4^n	$(q-1)^n$

The growth base $q-1$ (when $p \mid (q-1)$) reflects the multiplicative group $\mathbb{F}_q^*$. The gate complexity $t(p, q, n)$ equals the number of Frobenius orbits that must be covered, divided by the number of orbits per $\mathbb{F}_q$-line.

10.2 Phase Transition at $p \mid (q-1)$

The ratio of the two formulas is

$$\frac{(q^n-1)/(q-1)}{(q-1)^{n-1}} = \frac{1+q+\cdots+q^{n-1}}{(q-1)^{n-1}} \sim \frac{q^{n-1}}{(q-1)^{n-1}} \to \left(\frac{q}{q-1}\right)^{n-1}$$

as $n \to \infty$. For small q, this ratio is significant: for $q = 3$, the jump from $p = 2$ (giving 2^{n-1}) to $p = 5$ (giving $(3^n - 1)/2$) is a factor of roughly $(3/2)^{n-1}$.

10.3 Connections to $\mathsf{AC}^0[6]$

In a depth-2 circuit with $\mathsf{MOD}\text{-}q$ bottom gates and a $\mathsf{MOD}\text{-}p$ top gate, each bottom gate computes $\ell_i(u) \mod q$ and the top gate applies an arbitrary $g : \mathbb{F}_q \to \mathbb{F}_p$. Theorem 1.1 shows that any such circuit computing $\mathbf{1}_T$ requires $\geq (q-1)^{n-1}$ or $\geq (q^n - 1)/(q-1)$ bottom gates—an exponential lower bound for this restricted model.

10.4 Projective-Geometric Interpretation

The dichotomy has a clean projective interpretation. A gate with linear part $\ell_a(x) = a \cdot x$ probes the hyperplane $H_a = \{x : a \cdot x = 0\}$ in $\mathbb{F}_q^n$. The torus T avoids all coordinate hyperplanes, so detecting T requires distinguishing it from Z.

When $p \mid (q-1)$, the Fourier analysis over $\mathbb{F}_{p^k}$ sees only T: the boundary Fourier coefficients vanish. The gate complexity equals $(q-1)^{n-1}$, the number of $\mathbb{F}_q^*$-orbits in T modulo scaling.

When $p \nmid (q-1)$, the Fourier analysis sees all of $\mathbb{F}_q^n \setminus \{0\}$: boundary directions carry nonzero Fourier mass. The gate complexity jumps to $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^{n-1}$, the total number of hyperplane directions.

10.5 Further Directions

1. **Higher depth.** Our model is depth-2. Can the cross-characteristic framework extend to depth-3 and beyond? This is the real $\mathsf{AC}^0[6]$ question. The cohomological interpretation (Section 9) suggests that higher-depth circuits may correspond to derived functors or higher filtration levels.

2. **Cross-characteristic coding theory.** The code C/C_0 is a new object, now identified with the space of orbit functions (Proposition 9.3). Understanding its weight enumerator, dual code, and MacWilliams relations in the cross-characteristic setting may yield further structural results.

3. **Non-abelian generalizations.** The torus $T = \mathbb{G}_m^n$ is abelian. Extending the framework to non-abelian algebraic groups (e.g., SL_2, GL_n) could yield new complexity-theoretic invariants via the geometric Langlands correspondence.

4. **Quantum codes.** The orbit space $T/\mathbb{F}_q^* \cong \mathbb{G}_m^{n-1}$ suggests connections to quantum error correction. The gate code C/C_0 may admit a CSS-type quantum lift, with the self-duality $\widehat{\mathbf{1}_T} = \mathbf{1}_T$ ensuring transversal logical operations.

References

[AHK18] K. Adiprasito, J. Huh, and E. Katz. Hodge theory for combinatorial geometries. *Annals of Mathematics*, 188(2):381–452, 2018.

[BST90] D. A. M. Barrington, H. Straubing, and D. Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, 1990.

[CL25] E. Chattopadhyay and J. Liao. Explicit separations between randomized and deterministic communication for small rounds. ECCC, 2025.

[Gre76] C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Applied Mathematics*, 55(2):119–128, 1976.

[Han02] J. P. Hansen. Toric varieties, Hirzebruch surfaces and error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing*, 13(4):289–300, 2002.

[HK12] J. Huh and E. Katz. Log-concavity of characteristic polynomials and the Bergman fan of matroids. *Mathematische Annalen*, 354(3):1103–1116, 2012.

[Mil80] J. S. Milne. *Étale Cohomology.* Princeton Mathematical Series, 33. Princeton University Press, 1980.

[Raz87] 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.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th ACM STOC*, pages 77–82, 1987.

[SS09] I. Soprunov and J. Soprunova. Toric surface codes and Minkowski length of polygons. *SIAM Journal on Discrete Mathematics*, 23(1):384–400, 2009.

[Vio09] E. Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[Wil14] R. Williams. Nonuniform ACC circuit lower bounds. *Journal of the ACM*, 61(1):1–32, 2014.