Gate Complexity of the Algebraic Torus

Anonymous

Abstract

A (p, q)*-gate* is a function $\mathbb{F}_q^n \to \mathbb{F}_p$ of the form $g \circ \ell$, 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; equivalently, it is a depth-2 subcircuit consisting of a single MOD-q gate followed by a MOD-p gate. We determine the *gate complexity* $t(p, q, n)$—the minimum number of (p, q)-gates whose $\mathbb{F}_p$-linear combination equals the indicator function of the algebraic torus $(\mathbb{F}_q^*)^n$—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 compactly supported étale cohomology $H^*_{c,\text{ét}}(\mathbb{G}_m^{n-1}, \mathbb{F}_p)$.

We also show that depth-3 circuits escape the exponential barrier: for $n < p$, the torus indicator can be computed with $O(n)$ gates. For $n = 2$, the gate complexity model specializes to a random walk whose *Steinberg polynomial* $n_p(q) = \det(I - P|_{\mathrm{St}_p})$ admits a twisted circulant reduction with a spectral gap controlled by the Weil bound for Gauss sums.

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-6 gates. The Razborov–Smolensky method [3, 4] gives exponential lower bounds for $\mathsf{AC}^0[p]$ when p is prime, but breaks down for composite moduli like $6 = 2 \times 3$.

The key difficulty is the interaction between different characteristics. MOD-6 gates can simulate both MOD-2 and MOD-3, combining information from $\mathbb{F}_2$ and $\mathbb{F}_3$ in a way that resists standard polynomial methods. In this paper we isolate this cross-characteristic interaction in its simplest form and study it through the lens of algebraic 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.

Example 1.1. *For $p = 2$, $q = 3$, $n = 2$, a typical $(2,3)$-gate on $\mathbb{F}_3^2$ is*

$$g(x_1 + 2x_2), \quad \textit{where } g\colon \mathbb{F}_3 \to \mathbb{F}_2 \textit{ is defined by } g(0) = 1,\ g(1) = 0,\ g(2) = 0.$$

This gate outputs 1 if and only if $x_1 + 2x_2 \equiv 0 \pmod 3$. The affine map $\ell(x_1, x_2) = x_1 + 2x_2$ computes a MOD-3 linear form, and g applies an arbitrary Boolean post-processing. The gate complexity $t(2,3,n)$ asks: how many such gates must be summed over $\mathbb{F}_2$ to produce the indicator of $(\mathbb{F}_3^*)^n$? Our main theorem gives $t(2,3,n) = 2^{n-1}$.

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 show in Section 10 that depth-3 already escapes the exponential barrier, reducing the gate count from exponential to linear.

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 1.2 (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 compactly supported étale cohomology: $t(p,q,n) = \mathrm{Tr}(\mathrm{Frob}_q \mid H^*_{c,\text{ét}}(\mathbb{G}_m^{n-1}, \mathbb{F}_p))$.

(5) **Depth-3 escape (Section 10).** For $n < p$, the torus indicator can be computed with $n+1$ gates at depth-3—an exponential improvement over depth-2.

(6) **Steinberg polynomial (Section 11).** For $n = 2$, the gate complexity model specializes to a random walk on $\mathbb{P}^1(\mathbb{F}_p)$ whose Steinberg polynomial admits a twisted circulant reduction with a spectral gap controlled by the Weil bound for Gauss sums [9, 10].

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 [3] and Smolensky [4] gives exponential lower bounds for $\mathsf{AC}^0[p]$ for prime p, but fails for composite moduli. Barrington, Straubing, and Thérien [1] studied the algebraic structure of ACC^0 and showed connections to group theory. Viola [6] surveyed the state of small-depth computation and highlighted the $\mathsf{AC}^0[6]$ problem as a central challenge. Williams [7] proved nonuniform ACC^0 lower bounds via a different route (satisfiability algorithms), but the uniform case remains open.

The connection between gate complexity and coding theory parallels work on toric codes [2, 5], where code parameters are controlled by lattice geometry.

The $n = 2$ specialization of the gate complexity model produces a Steinberg polynomial with rich arithmetic structure, developed in companion work [9, 10]. The connection to matrix rigidity (§12.2) relates to Valiant's program for proving circuit lower bounds via rigid matrices [8].

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 proves that depth-3 circuits escape the exponential barrier. Section 11 describes the connection to the Steinberg polynomial. Section 12 discusses connections to matrix rigidity, $\mathsf{AC}^0[6]$, 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 $\dim(C/C_0) = (q-1)^n$. $\square$

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 $\alpha \in (\ker a)^{\perp} = \mathbb{F}_q \cdot a$. $\square$

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. $\square$

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

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

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 $\mathbb{F}_q^* \cdot a_i$):

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

$\square$

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* $n \geq 1$*:*

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

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 1.2. 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 $\mathbf{1}|_T$, 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. □

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 compactly supported étale cohomology. This section may be skipped without loss of continuity; the main theorem depends only on Sections 5–6. Throughout this section, $H_c^*(X, \mathbb{F}_p)$ denotes $H^*_{c,\text{ét}}(X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathbb{F}_p)$, the compactly supported étale cohomology of the base change to the algebraic closure.

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 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)**.** *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 $\mathbb{F}_q$ 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 $\mathbb{F}_q$ 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:

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

□

9.3 Geometric Interpretation of the Dichotomy

Remark 9.2 (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.*

10 Depth-3 Circuits: Escaping the Exponential Barrier

The exponential lower bound of Theorem 1.2 applies to depth-2 circuits. A natural question is whether increased depth can circumvent this barrier. We show that depth-3 suffices to reduce the gate complexity from exponential to linear.

10.1 The Depth-3 Construction

Theorem 10.1. *For $n < p$, the torus indicator $\mathbf{1}_T$ can be computed by a depth-3 circuit with $n+1$ gates.*

Proof. We construct a two-layer circuit:

Layer 1 (n gates): For each coordinate $i \in [n]$, define the gate

$$b_i = g_i(\ell_i(x)) \in \mathbb{F}_p$$

where $\ell_i(x) = x_i$ (the i-th coordinate projection) and $g_i : \mathbb{F}_q \to \mathbb{F}_p$ is defined by

$$g_i(v) = \begin{cases} 1 & \text{if } v \neq 0 \\ 0 & \text{if } v = 0 \end{cases}$$

Thus $b_i = \mathbf{1}[x_i \neq 0] \in \{0, 1\} \subset \mathbb{F}_p$.

Layer 2 (1 gate): The intermediate values $(b_1, \ldots, b_n) \in \mathbb{F}_p^n$ are fed into a single gate

$$h\left(\sum_{i=1}^{n} b_i\right)$$

where $h : \mathbb{F}_p \to \mathbb{F}_p$ is defined by

$$h(s) = \begin{cases} 1 & \text{if } s = n \\ 0 & \text{otherwise} \end{cases}$$

Correctness: We have $x \in T$ if and only if all $b_i = 1$, which occurs if and only if $\sum_i b_i = n$. The condition $n < p$ ensures that the sum $\sum_i b_i$ equals the integer n in $\mathbb{F}_p$ (no wraparound), so $h(\sum_i b_i) = 1$ if and only if all coordinates are nonzero.

The total gate count is $n + 1$. □

Remark 10.2. *The constraint $n < p$ is necessary for the construction. When $n \geq p$, the sum $\sum_i b_i$ can equal $n \mod p$ without all $b_i = 1$, breaking correctness.*

10.2 The Depth Gap

Corollary 10.3 (Exponential Depth Gap)**.** *For fixed p and q with $p \mid (q-1)$ and $n < p$:*

$$\frac{t_2(p, q, n)}{t_3(p, q, n)} = \frac{(q-1)^{n-1}}{n+1} = \Omega\left(\frac{(q-1)^{n-1}}{n}\right).$$

The depth-2 complexity is exponential while depth-3 is linear—an exponential separation.

10.3 Why the Fourier Method Fails at Depth 3

The lower bound of Section 5 relied on covering the Fourier support with lines. This argument is inherently depth-2: it exploits the fact that each depth-2 gate has Fourier support on a single line.

At depth 3, intermediate values can be combined nonlinearly before the final output. The Fourier support of a depth-3 circuit is no longer constrained to a union of lines—the intermediate layer "mixes" Fourier modes in a way that defeats the covering argument.

Open Problem 10.4. *Determine the depth-3 gate complexity $t_3(p, q, n)$ for $n \geq p$. Our construction requires $n < p$; when $n \geq p$, is $t_3(p, q, n)$ still $O(n)$, or does it grow faster?*

11 Connection to the Steinberg Polynomial

The gate complexity model specializes, at $n = 2$, to a weighted random walk on the projective line $\mathbb{P}^1(\mathbb{F}_p)$ whose spectral theory reveals deep structure in the cross-characteristic interaction. The Steinberg polynomial $n_p(q)$ and its arithmetic properties are developed in [9]; the twisted circulant reduction and spectral gap are established in [10].

11.1 The $n = 2$ Specialization

When $n = 2$, the gate complexity setup reduces to a single linear form $\ell(x_1, x_2) = x_1 + sx_2$ for $s \in \mathbb{F}_p^*$. The states $[1 : s]$ for $s \in \mathbb{F}_p$ together with $[0 : 1] = \infty$ form the projective line $\mathbb{P}^1(\mathbb{F}_p)$, and the weights

$$w_r = \frac{q^{p-r}}{q^p - 1}$$

define a $(p + 1) \times (p + 1)$ transition matrix P on $\mathbb{P}^1(\mathbb{F}_p)$. The **Steinberg representation** $\mathrm{St}_p = \{f : \mathbb{P}^1(\mathbb{F}_p) \to \mathbb{C} : \sum_x f(x) = 0\}$ is the p-dimensional irreducible summand of the permutation representation, and P preserves the decomposition $V = \mathbf{1} \oplus \mathrm{St}_p$.

The transition matrix factors as $P = L_w \cdot \pi(w_0)$, where $w_0 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is the coordinate-swap permutation and $L_w = \sum_{r=0}^{p-1} w_r\, \pi(U(r))$ is a weighted average over the upper-triangular translations $U(r) = \left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$. The weights $w_r = q^{p-r}/(q^p - 1)$ form a Gibbs (geometric) distribution on $\mathbb{F}_p$, which degenerates to the uniform distribution $w_r = 1/p$ in the limit $q \to 1$ [10].

11.2 The Steinberg Polynomial

Define the **Steinberg polynomial** $n_p(q) = (q^p - 1) \det(I - P|_{\mathrm{St}_p}) \in \mathbb{Z}[q]$. In [9], it is shown that $n_p(q)$ has remarkable arithmetic structure: it admits a palindromic/anti-palindromic decomposition governed by the Legendre symbol $\left(\frac{-2}{p}\right)$, its roots have absolute value either 1 or $1/\sqrt{2}$ (the latter matching Frobenius eigenvalues of abelian varieties over $\mathbb{F}_2$), and its factorization pattern is controlled by the cousin prime structure of consecutive primes. These properties are verified for all 24 primes $p \leq 97$; we refer to [9] for the full development.

11.3 The Twisted Circulant Reduction

The main structural result of [10] is a *twisted circulant reduction*: the $(p+1)$-dimensional computation of $\det(I - P|_{\mathrm{St}_p})$ reduces exactly to a $(p - 1)$-dimensional determinant

$$n_p(q) = -(q - 1)(q^p - 1) \det(I - C),$$

where C is the $(p-1) \times (p-1)$ matrix on $\mathbb{F}_p^*$ defined by $C[j, j'] = w_{j'-j^{-1} \bmod p}$. The entries of C mix the additive structure of the Gibbs weights with the multiplicative structure of inversion in $\mathbb{F}_p^*$: explicitly, $C = Q \cdot W$ where Q is the inversion permutation $j \mapsto j^{-1}$ and W is the additive convolution by the Gibbs weights restricted to $\mathbb{F}_p^*$.

The reduction proceeds in two steps. First, a *boundary decoupling* identity shows that the boundary state $0 \in \mathbb{P}^1(\mathbb{F}_p)$ contributes nothing to the Steinberg determinant (the Schur complement equals 1 exactly). Second, a *rank-one correction* via the matrix determinant lemma extracts the factor $(1-q)$, which explains the divisibility $(q-1) \mid n_p(q)$ observed in [9]. Both steps rest on a single identity: $\mathbf{w}^T(I-C)^{-1}\mathbf{1} = -q$, proved by a telescoping argument that identifies the transpose resolvent $(I - W^T)^{-1}\mathbf{w}$ as a delta function at the inversion-fixed point $-1 \in \mathbb{F}_p^*$.

The twisted circulant C is the concrete $(p-1) \times (p-1)$ matrix that encodes the cross-characteristic interaction between $\mathbb{F}_p$ and $\mathbb{F}_q$ at $n = 2$. Its spectral theory, discussed next, constrains how efficiently this interaction can be decomposed.

11.4 The Spectral Gap

The eigenvalues of C split sharply at the threshold $|1 - \lambda| = 1$: exactly $(p+1)/2$ lie in the "small" sector and $(p-3)/2$ in the "large" sector. This splitting follows from the Weil bound $|G(a, \chi)| = \sqrt{p}$ for Gauss sums, which bounds the even–odd mixing in the multiplicative character basis by $O(1/\sqrt{p})$ [10]. This is a finite-field analogue of the Ramanujan property for expander graphs, and implies that the $n = 2$ gate complexity cannot be improved by local perturbations of the gate functions. The further arithmetic of $n_p(q)$ is developed in [9, 10].

12 Discussion

12.1 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
$\lvert T\rvert$	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. Note that the ratio between the two regimes is $(q^n-1)/((q-1)^n) \sim (q/(q-1))^{n-1}$, so for small q the phase transition at $p \mid (q-1)$ is significant: for $q = 3$, the jump from $p = 2$ to $p = 5$ is a factor of roughly $(3/2)^{n-1}$.

12.2 Matrix Rigidity and 2-Adic Obstructions

The twisted circulant C of [10] gives rise to a natural *exponent matrix* $E \in \mathbb{Z}^{(p-1)\times(p-1)}$ defined by $E[j, j'] = (j^{-1} - j') \bmod p$, which has rank 2 over $\mathbb{F}_p$. The divisibility dichotomy controls a rank explosion in the lifted matrix q^E: when $p \mid (q-1)$, the matrix q^E collapses to rank 1, but when $p \nmid (q-1)$, it generically has full rank $p-1$. At $q = 2$, the matrix 2^E is maximally rigid in the sense of Valiant [8]—reducing its rank to r requires changing $\Omega((p-1)^2)$ entries—verified for $p \leq 47$ in [10]. This connects to Valiant's program: rigid matrices cannot be computed by bounded-depth linear circuits, suggesting a possible approach to extending lower bounds beyond depth 2.

The Boolean specialization $q = 2$ also reveals arithmetic constraints. The Steinberg polynomial value $n_p(2) \equiv 1 \pmod 8$ for all primes $p \geq 7$ [10]. This is forced by the group structure of $\mathbb{F}_p^*$ (not a random-matrix phenomenon—a random matrix with $M \equiv I \pmod 2$ satisfies this only with probability $\approx 1/4$). The *discriminant cascade* of [10] extends this to a hierarchy of obstructions at successive 2-adic levels, each controlled by a Legendre symbol $\left(\frac{\Delta_k}{p}\right)$ with $\Delta_k = k^2 + 4$, suggesting an infinite sequence of arithmetic constraints on cross-characteristic computation at $q = 2$.

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

In a depth-2 circuit with MOD-q bottom gates and a MOD-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 1.2 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.

However, Theorem 10.1 shows that depth-3 escapes this barrier with $O(n)$ gates when $n < p$. The central open problem for $\mathsf{AC}^0[6]$ is to understand how cross-characteristic interactions compose across multiple layers.

The results of §12.2 suggest two complementary approaches to extending lower bounds beyond depth 2:

- **Rigidity-based.** The maximal rigidity of q^E at $q = 2$ gives a structural reason why the depth-2 lower bound is exponential. Since matrix rigidity lower bounds apply to log-depth linear circuits [8], the rigidity of q^E might yield lower bounds for circuits of depth greater than 2, provided the nonlinear gate functions can be incorporated into the framework.

- **2-adic.** The discriminant cascade provides a sequence of arithmetic obstructions at $q = 2$. At depth 2, all obstructions are present simultaneously. The depth-3 escape $t_3 = O(n)$ must violate these obstructions by mixing Fourier modes across the intermediate layer. Understanding *which* obstructions depth-3 circuits can circumvent—and which persist—would clarify the depth hierarchy for cross-characteristic computation.

12.4 Further Directions

1. **Exact depth-3 complexity.** Determine $t_3(p, q, n)$ precisely for all n, including the regime $n \geq p$. The depth-3 escape (Theorem 10.1) requires $n < p$ to avoid wraparound in $\mathbb{F}_p$. When $n \geq p$, does $t_3(p, q, n)$ remain $O(n)$, or does it grow faster?

2. **Rigidity and depth.** The maximal rigidity of q^E at $q = 2$ (§12.2) is verified only for $p \leq 47$ in [10]. Establish this for all primes p. More broadly, can the rigidity of q^E, combined with the nonlinear gate structure, yield lower bounds for depth-d cross-characteristic circuits for $d \geq 3$?

3. **Cross-characteristic codes.** The quotient C/C_0 is a linear code over $\mathbb{F}_p$ whose structure arises from $\mathbb{F}_q$. It would be interesting to understand its basic properties (minimum distance, weight distribution) and whether standard coding-theoretic tools adapt to this cross-characteristic setting.

References

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

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

[3] 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.

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

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

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

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

[8] L. G. Valiant. Graph-theoretic arguments in low-level complexity. *Math. Found. Comput. Sci.*, Lecture Notes in Comput. Sci. **53** (1977), 162–176.

[9] Author. Steinberg polynomials from weighted random walks: decomposition, Weil weights, and motivic factorization. Preprint, 2026.

[10] Author. Gibbs intertwining operators and the Steinberg polynomial. Preprint, 2026.

Acknowledgment. Generative AI (Claude, Anthropic) was used for coding assistance and language polishing.