Gate Complexity of the Algebraic Torus

Anonymous

Abstract

Let p be a prime and q a prime power with $\operatorname{char}(\mathbb{F}_q) \neq p$. 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. 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 $T = (\mathbb{F}_q^*)^n$.

The answer depends on a divisibility condition:

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

In both cases, the upper bound is a Fourier inversion identity and the lower bound is obtained via Frobenius orbit counting. We also show that the depth-3 case already escapes the exponential barrier: for $n < p$, the torus indicator can be computed with $O(n)$ gates, giving an exponential separation.

1 Introduction

A central open problem in circuit complexity is to prove superpolynomial lower bounds for $\mathsf{AC}^0[6]$. The Razborov–Smolensky method [8, 9] gives exponential lower bounds for $\mathsf{AC}^0[p]$ when p is prime, but breaks down for composite moduli like $6 = 2 \times 3$.

Our work is motivated by this question, though our model lives in arbitrary positive characteristic rather than just the Boolean case. We give a clean result concerning the gate complexity $t(p, q, n)$ at depth 2. Whether our method applies to the actual $\mathsf{AC}^0[6]$ problem remains unclear to the author at this moment.

The model. A (p, q)-gate computes $g \circ \ell$, where $\ell \colon \mathbb{F}_q^n \to \mathbb{F}_q$ is an affine form and $g \colon \mathbb{F}_q \to \mathbb{F}_p$ is an *arbitrary* function—a full lookup table on one affine projection. The gate complexity $t(p, q, n)$ is the minimum number of gates whose $\mathbb{F}_p$-linear combination equals the indicator $\mathbf{1}_T$ of the algebraic torus $T = (\mathbb{F}_q^*)^n$.

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

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

This gate outputs 1 *if and only if* $x_1 + 2x_2 \equiv 0 \pmod 3$. *Our main theorem gives* $t(2, 3, n) = 2^{n-1}$.

1.1 Main Result

Theorem 1.2 (Main Theorem). *Let p be a prime and q a prime power with* $\operatorname{char}(\mathbb{F}_q) \neq p$. *Then*

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

For $p = 2$, the condition $2 \mid (q-1)$ holds for all odd q, so $t(2, q, n) = (q-1)^{n-1}$. For $q = 2$, we have $p \nmid 1$ for all odd primes p, giving $t(p, 2, n) = 2^n - 1$.

We also show that depth-3 circuits escape the exponential barrier:

Theorem 1.3. *For $n < p$, the torus indicator $\mathbf{1}_T$ can be computed by a depth-3 circuit with $n+1$ gates. Moreover, any depth-3 circuit for $\mathbf{1}_T$ requires at least n layer-1 gates (Proposition 9.2), so $t_3(p, q, n) = \Theta(n)$.*

1.2 Techniques

Upper bound. The construction is a Fourier inversion identity decomposed over projective lines. For each $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$, we define a gate $g_{[a]} \circ \ell_a$ where $\ell_a(x) = a \cdot x$. The coefficients 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 $(q-1)^{n-1}$.

Lower bound. The $\mathbb{F}_{p^k}$-Fourier transform (where $k = \mathrm{ord}_r(p)$) has the property that each gate's Fourier support lies on a single $\mathbb{F}_q$-line, and the support is closed under the Frobenius $\alpha \mapsto p\alpha$. The Fourier support of $\mathbf{1}_T$ consists of either all torus orbits or all nonzero orbits. A counting argument—each line contributes at most $(q-1)/k$ orbits, and the factors of k cancel—gives the lower bound.

1.3 Related Work

The polynomial method of Razborov [8] and Smolensky [9] gives exponential lower bounds for $\mathsf{AC}^0[p]$ for prime p, but fails for composite moduli. Barrington, Straubing, and Thérien [3] studied the algebraic structure of ACC^0. Chattopadhyay, Green, and Straubing [4] proved subexponential lower bounds for powering in $\mathbb{F}_{p^n}$ against $\mathsf{ACC}(p)$ circuits using Kopparty's versatility method [7]; their model is Boolean (gates act on bits), while ours is algebraic (gates act on field elements), and we discuss the relationship in Section 10. Viola [11] surveyed the state of small-depth computation. Williams [12] proved nonuniform ACC^0 lower bounds via satisfiability algorithms, but the uniform case remains open.

In the purely linear setting, Alman and Li [1] study depth-2 linear circuits for Kronecker power matrices using asymptotic spectrum theory. A finding in this line of work [2, 6, 1] is that Kronecker products of small matrices are generally not Valiant-rigid. Our setting differs in that gates include nonlinear post-processing $g \colon \mathbb{F}_q \to \mathbb{F}_p$, and the exponential lower bound highlights the role of this nonlinearity.

The connection between gate complexity and coding theory parallels work on toric codes [5, 10].

1.4 Organization

Section 2 establishes the basic setup. Section 3 gives a proof for the gate span completeness result. 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 $q = 3$. Section 8 gives the alternative Vandermonde induction proof for $q = 3$ and shows why it fails for $q \geq 5$. Section 9 shows that depth-3 circuits already escape the exponential barrier. Section 10 discusses connections to Boolean lower bounds.

2 Setup

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

Definition 2.2. *The gate complexity is*

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

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

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

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* $\mathrm{span}_{\mathbb{F}_p}(\mathcal{G}) = \mathbb{F}_p^{\mathbb{F}_q^n}$, *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.*

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 exactly 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 exactly $k = \operatorname{ord}_r(p)$ (since $p^j \alpha = \alpha$ with $\alpha \neq 0$ implies $p^j = 1$ in $\mathbb{F}_q$), 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 $\operatorname{char}(\mathbb{F}_q) \neq p$:*

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

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

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

□

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. The tightness of the lower bound (Theorem 5.3) forces each of the 2^{n-1} gates to cover a distinct Frobenius orbit in T, so the 2^{n-1} linear forms used must be exactly one representative per projective class in T. Up to a choice of distinguished coordinate, these are $\{\ell_s : s \in (\mathbb{F}_3^*)^{n-1}\}$.

Given these forms, 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 $\omega \in \mathbb{F}_4$ is a primitive cube root of unity (satisfying $\omega^2 + \omega + 1 = 0$).

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* $\operatorname{supp}(f) \subseteq T$*. Then* $|\operatorname{supp}(\widehat{f})| \geq 2^n$*.*

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

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

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

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

Proof. For $f \in C \setminus C_0$, Theorem 8.2 gives $|\operatorname{supp}(\widehat{f})| \geq 2^n$, hence $|\operatorname{supp}(\widehat{f}) \setminus \{0\}| \geq 2^n - 1$. 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 that 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 obstruction is the Vandermonde structure: the 5×4 Vandermonde matrix over $\mathbb{F}_{16}$ has singular 4×4 submatrices, so the coordinate slicing induction yields only $|\mathrm{supp}(\widehat{f})| \geq 2 \cdot 4^{n-1}$, a factor of 2 short. This failure motivated the orbit counting argument of Section 5.*

9 The Depth-3 Case

The exponential lower bound of Theorem 1.2 applies to depth-2 circuits. We show that depth-3 suffices to reduce the gate complexity from exponential to linear.

9.1 The Depth-3 Construction

Proof of Theorem 1.3. We construct a two-layer circuit.

Layer 1 (n gates): For each coordinate $i \in [n]$, define the gate $b_i = g_i(x_i) \in \mathbb{F}_p$ where

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

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

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

Correctness: We have $x \in T$ if and only if all $b_i = 1$, if and only if $\sum_i b_i = n$. The condition $n < p$ ensures no wraparound in $\mathbb{F}_p$, so $h(\sum_i b_i) = 1$ if and only if all coordinates are nonzero. The total gate count is $n + 1$. □

Remark 9.1. *The constraint $n < p$ is necessary for the construction: when $n \geq p$, the sum $\sum_i b_i$ can equal $n \bmod p$ without all $b_i = 1$.*

9.2 A Lower Bound at Depth 3

Proposition 9.2. *Any depth-3 circuit computing $\mathbf{1}_T$ uses at least n layer-1 gates.*

Proof. A depth-3 circuit computes $h(\sum_{j=1}^w c_j g_j(a_j \cdot x))$ for direction vectors $a_1, \ldots, a_w \in \mathbb{F}_q^n$. The output depends on x only through the map $L \colon x \mapsto (a_1 \cdot x, \ldots, a_w \cdot x)$. Let $V = \mathrm{span}(a_1, \ldots, a_w)$ with $d = \dim V$.

Suppose $d < n$. Choose $a \notin V$ and set $\ell(x) = a \cdot x$. For each $t \in \mathbb{F}_q$, the affine hyperplane $H_t = \{x : \ell(x) = t\}$ has $|H_t| = q^{n-1}$. The restriction of L to H_t maps onto $\mathbb{F}_q^d$ with fibers of constant size q^{n-1-d} (since ℓ is independent of $a_1, \ldots, a_w$). In particular, for any value $v \in \mathbb{F}_q^d$:

$$|\{x \in H_t : L(x) = v\}| = q^{n-1-d}, \quad \text{independent of } t.$$

Since the circuit's output at x is determined by $L(x)$, the number of $x \in H_t$ where the circuit outputs 1 is independent of t. If the circuit computes $\mathbf{1}_T$, this gives $|H_t \cap T| = |H_0 \cap T|$ for all t.

We show this fails by explicit computation. Write $\ell(x) = \sum_i a_i x_i$ and let $m = |\{i : a_i = 0\}|$. Using additive characters:

$$|H_t \cap T| = \sum_{x \in T} \frac{1}{q} \sum_{s \in \mathbb{F}_q} \chi\big(s(\ell(x) - t)\big) = \frac{1}{q}\left[(q-1)^n + \sum_{s \neq 0} \chi(-st) \sum_{x \in T} \chi(sa \cdot x)\right].$$

The inner sum factorizes over coordinates: $\sum_{x \in T} \chi(sa \cdot x) = \prod_i \sum_{c \in \mathbb{F}_q^*} \chi(sa_i c)$. For $a_i \neq 0$ and $s \neq 0$, the map $c \mapsto sa_i c$ is a bijection on $\mathbb{F}_q^*$, so $\sum_c \chi(sa_i c) = \sum_{u \in \mathbb{F}_q^*} \chi(u) = -1$. For $a_i = 0$, the sum is $q - 1$. Thus $\sum_{x \in T} \chi(sa \cdot x) = (-1)^{n-m}(q-1)^m$ for all $s \neq 0$.

For $t = 0$: $\sum_{s \neq 0} \chi(0) = q - 1$. For $t \neq 0$: $\sum_{s \neq 0} \chi(-st) = -1$. Therefore:

$$|H_0 \cap T| = \frac{1}{q}\left[(q-1)^n + (q-1)(-1)^{n-m}(q-1)^m\right],$$
$$|H_t \cap T| = \frac{1}{q}\left[(q-1)^n - (-1)^{n-m}(q-1)^m\right] \quad (t \neq 0).$$

The difference is

$$|H_0 \cap T| - |H_t \cap T| = (-1)^{n-m}(q-1)^m \neq 0,$$

since ℓ is nonconstant (so $m \leq n - 1$) and $(q-1)^m \geq 1$. This contradicts $|H_t \cap T|$ being constant in t, so $d = n$ and $w \geq n$. □

9.3 The Depth Gap

Corollary 9.3 (Exponential Depth Gap)**.** *For fixed p and q with $p \mid (q-1)$ and $n < p$:*

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

Remark 9.4. *The lower bound of Section 5 relied on each depth-2 gate having Fourier support on a single $\mathbb{F}_q$-line. At depth 3, the intermediate layer combines Fourier modes nonlinearly, defeating this covering argument.*

10 Discussion

10.1 Relation to Boolean Lower Bounds

It is worth clarifying the relationship between our results and the Boolean circuit lower bounds of Chattopadhyay, Green, and Straubing [4], who prove subexponential lower bounds for powering in $\mathbb{F}_{p^n}$ against $\mathsf{ACC}(p)$ circuits.

The two results concern different models. In Boolean $\mathsf{ACC}(p)$, each gate computes a weighted sum of input *bits* modulo p; field elements are encoded as bit strings, and extracting even a single field element's value requires many gates. In our model, a single (p,q)-gate applies an arbitrary function to an $\mathbb{F}_q$-linear form. The CGS lower bound relies on polynomial approximation via the Razborov–Smolensky method, combined with Kopparty's versatility argument [7]; this has no analogue in our setting, since our gates already compute arbitrary functions of their inputs. The models probe different aspects of the cross-characteristic barrier, and neither subsumes the other.

10.2 Open Question

Our depth-3 construction (Theorem 1.3) requires $n < p$ so that the sum $\sum b_i$ does not wrap around in $\mathbb{F}_p$. The lower bound $t_3 \geq n$ (Proposition 9.2) has no such restriction. Extending the upper bound to all n—or finding a different construction that avoids the $n < p$ condition—would close the gap.

References

[1] J. Alman and B. Li. Kronecker powers, orthogonal vectors, and the asymptotic spectrum. In *Proc. 66th IEEE FOCS*, 2025.

[2] J. Alman. Kronecker products, low-depth circuits, and matrix rigidity. In *Proc. 53rd ACM STOC*, pages 772–785, 2021.

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

[4] A. Chattopadhyay, F. Green, and H. Straubing. Circuit complexity of powering in fields of odd characteristic. *Chicago J. Theor. Comput. Sci.*, 2016(10):1–18, 2016.

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

[6] B. Kivva. Improved upper bounds for the rigidity of Kronecker products. In *Proc. 46th MFCS*, LIPIcs vol. 202, 2021.

[7] S. Kopparty. On the complexity of powering in finite fields. In *Proc. 44th ACM STOC*, pages 489–498, 2012.

[8] 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.

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

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

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

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

Acknowledgment. Gen AI (Claude, Anthropic) was used for coding assistance and language polishing. Yet the major intellectural work is done by the author himself.