Gate Complexity of the Algebraic Torus: the General Case

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

February 2026

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:

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

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.

1 Introduction

In [1], the gate complexity $t(2, q, n) = (q-1)^{n-1}$ was determined for all odd prime powers q. There, the key tools were the self-duality $\widehat{\mathbf{1}_T} = \mathbf{1}_T$ over $\mathbb{F}_{2^k}$ and an orbit counting argument exploiting the Frobenius $\alpha \mapsto 2\alpha$.

In this companion paper, we extend the result to all primes p, revealing a dichotomy that was invisible in the $p = 2$ case. When $p = 2$, $q - 1$ is always even, so $p \mid (q - 1)$ holds automatically. For general p, the Fourier support of $\mathbf{1}_T$ over $\mathbb{F}_{p^k}$ depends on whether $q - 1 \equiv 0 \pmod{p}$:

- If $p \mid (q-1)$: the per-coordinate factor $q - 1$ vanishes in $\mathbb{F}_{p^k}$, giving $\mathrm{supp}(\widehat{\mathbf{1}_T}) = T$.
- If $p \nmid (q-1)$: the factor $q - 1$ is invertible, giving $\mathrm{supp}(\widehat{\mathbf{1}_T}) = \mathbb{F}_q^n \setminus \{0\}$.

The orbit counting lower bound reflects this: in the first case, only torus orbits need covering; in the second, all of $(\mathbb{F}_q^n \setminus \{0\})$ does. The upper bound in both cases comes from a unified construction via Fourier inversion decomposed over projective lines.

Main result

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

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

For $p = 2$, the condition $2 \mid (q-1)$ holds for all odd q, recovering the result of [1]. The case $q = 2$ (so $q - 1 = 1$, $p \nmid 1$ for all $p \geq 3$) gives $t(p, 2, n) = 2^n - 1 = |\mathbb{P}^{n-1}(\mathbb{F}_2)|$, also matching [1].

2 Setup

We briefly recall the framework from [1]. Let $T = (\mathbb{F}_q^*)^n$ denote the algebraic torus and $Z = \mathbb{F}_q^n \setminus T$ the boundary. A (p, q)-*gate* is a function $g \circ \ell \colon \mathbb{F}_q^n \to \mathbb{F}_p$ where $\ell(x) = a \cdot x + b$ is affine and $g \colon \mathbb{F}_q \to \mathbb{F}_p$ is arbitrary. The gate complexity $t(p, q, n)$ is the minimum w such that

$$\mathbf{1}_T = \sum_{i=1}^{w} c_i \, (g_i \circ \ell_i), \qquad c_i \in \mathbb{F}_p^*,$$

as functions $\mathbb{F}_q^n \to \mathbb{F}_p$.

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

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. Define the additive character

$$\chi \colon \mathbb{F}_q \to \mathbb{F}_{p^k}^*, \qquad \chi(x) = \zeta^{\mathrm{Tr}(x)},$$

where $\mathrm{Tr} \colon \mathbb{F}_q \to \mathbb{F}_r$ is the field trace. The $\mathbb{F}_{p^k}$-Fourier transform of $f \colon \mathbb{F}_q^n \to \mathbb{F}_{p^k}$ is

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

Since $\mathbb{F}_p \subset \mathbb{F}_{p^k}$, any function $f \colon \mathbb{F}_q^n \to \mathbb{F}_p$ has a well-defined $\mathbb{F}_{p^k}$-Fourier transform. The Frobenius $\sigma \colon x \mapsto x^p$ acts on $\mathbb{F}_{p^k}$ with order k, and for $\mathbb{F}_p$-valued f:

$$\hat{f}(p\alpha) = \hat{f}(\alpha)^p. \tag{1}$$

In particular, $\hat{f}(\alpha) \neq 0$ if and only if $\hat{f}(p\alpha) \neq 0$, so the Fourier support is a union of orbits under $\alpha \mapsto p\alpha$.

4 Fourier Support Dichotomy

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

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

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 factorises as $\mathbf{1}_T(x) = \prod_j \mathbf{1}_{x_j \neq 0}$, so the Fourier transform factorises. 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. For $a \notin T \cup \{0\}$, the line $\mathbb{F}_q \cdot a$ meets $\mathbb{F}_q^n \setminus \{0\}$ in $(q-1)/k$ Frobenius orbits (all lying in $\mathbb{F}_q^* \cdot a$).

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

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

6 Upper Bound

The upper bound in both cases follows from a single Fourier inversion construction.

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 parametrise $\mathbb{F}_q^n \setminus \{0\}$:

$$\begin{aligned} F(x) &= \frac{1}{q} \sum_{[a]} c_{[a]} + \frac{1}{q} \sum_{[a] \in \mathbb{P}^{n-1}} c_{[a]} \sum_{s \in \mathbb{F}_q^*} \chi(sa \cdot x) \\ &= C_0 + \frac{1}{q} \sum_{\alpha \in \mathbb{F}_q^n \setminus \{0\}} \frac{c_{[\alpha]}}{q-1} \chi(\alpha \cdot x), \end{aligned} \tag{3}$$

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.

Now $c_{[\alpha]}/(q(q-1)) = (-1)^{n-m(\alpha)}(q-1)^{m(\alpha)}/(q^n(q-1))$. But $q^{-n}(-1)^{n-m(\alpha)}(q-1)^{m(\alpha)} = \widehat{\mathbf{1}_T}(\alpha)/q^n$ is the normalised Fourier coefficient. More precisely:

$$\frac{c_{[\alpha]}}{q(q-1)} = \frac{(-1)^{n-m(\alpha)}(q-1)^{m(\alpha)}}{q^n \cdot (q-1)} = \frac{\widehat{\mathbf{1}_T}(\alpha)}{q^n(q-1)}.$$

Wait — let us redo this directly. By Proposition 4.1:

$$\mathbf{1}_T(x) = \frac{1}{q^n} \sum_{\alpha \in \mathbb{F}_q^n} \widehat{\mathbf{1}_T}(\alpha)\, \chi(\alpha \cdot x) = \widehat{\mathbf{1}_T}(0)/q^n + \frac{1}{q^n} \sum_{\alpha \neq 0} (-1)^{n-m(\alpha)}(q-1)^{m(\alpha)} \chi(\alpha \cdot x).$$

Grouping terms by projective class: each class $[a]$ contributes $q-1$ terms (for $s \in \mathbb{F}_q^*$), all with the same coefficient $(-1)^{n-m(a)}(q-1)^{m(a)}$ since $m(sa) = m(a)$:

$$\mathbf{1}_T(x) = \frac{(q-1)^n}{q^n} + \frac{1}{q^n} \sum_{[a]\in\mathbb{P}^{n-1}} (-1)^{n-m(a)}(q-1)^{m(a)} \sum_{s\in\mathbb{F}_q^*} \chi(sa\cdot x).$$

Since $\sum_{s\in\mathbb{F}_q^*} \chi(sa\cdot x) = q\cdot \mathbf{1}[a\cdot x = 0] - 1$:

$$\begin{aligned}\mathbf{1}_T(x) &= \frac{(q-1)^n}{q^n} + \frac{1}{q^n}\sum_{[a]}(-1)^{n-m(a)}(q-1)^{m(a)}\big(q\cdot \mathbf{1}[a\cdot x=0]-1\big)\\ &= \frac{(q-1)^n}{q^n} + \frac{1}{q^{n-1}}\sum_{[a]}(-1)^{n-m(a)}(q-1)^{m(a)}\mathbf{1}[a\cdot x=0]\\ &\qquad - \frac{1}{q^n}\sum_{[a]}(-1)^{n-m(a)}(q-1)^{m(a)}. \end{aligned} \tag{4}$$

The middle term is $\sum_{[a]} c_{[a]}\mathbf{1}[a\cdot x = 0] = F(x)$. The first and third terms are constants (independent of x). Therefore $\mathbf{1}_T(x) = F(x) + C$ for some constant $C \in \mathbb{F}_p$.

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.

This completes the proof. □

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

7 The Construction Explicitly

The proof of Theorem 6.1 yields a concrete gate representation, which we record here.

7.1 Case $p \mid (q-1)$

The gates are indexed by $s \in (\mathbb{F}_q^*)^{n-1}$. For each s, define

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

where $\lambda = ((q-1)^n - (-1)^n)^{-1}\cdot q^{-1} \in \mathbb{F}_p^*$ is a normalisation constant. Then $\sum_s g_s(\ell_s(x)) = \mathbf{1}_T(x)$ in $\mathbb{F}_p$.

Remark 7.1. The gate function $g_s(v) = \lambda\cdot\mathbf{1}[v\neq 0]$ is independent of s: all gates use the same nonlinear function. Only the affine map ℓ_s varies. This matches the $p = 2$ construction of [1], where the XOR of $\mathbf{1}[\ell_s \neq 0]$ over $s \in (\mathbb{F}_q^*)^{n-1}$ computes $\mathbf{1}_T$.

7.2 Case $p \nmid (q-1)$

The gates are indexed by projective points $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$. There are two types:

(i) *Torus directions* ($a \in T$, so $m(a) = 0$): $g_{[a]}(v) = c_{[a]} \cdot \mathbf{1}[v = 0]$ with $c_{[a]} = (-1)^n/q^{n-1}$.

(ii) *Boundary directions* ($a \notin T$, so $m(a) \geq 1$): $g_{[a]}(v) = c_{[a]} \cdot \mathbf{1}[v = 0]$ with $c_{[a]} = (-1)^{n-m(a)}(q-1)^{m(a)}/q^{n-1}$.

Both types use $g(v) = c \cdot \mathbf{1}[v = 0]$ with different constants. The boundary directions contribute to the representation because $q-1$ is nonzero in $\mathbb{F}_p$, so these gates are non-constant.

8 Remarks

8.1 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.

8.2 Phase transition at $p \mid (q-1)$

The ratio of the two formulas is

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

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 $(3/2)^{n-1}$.

8.3 Unification with $q = 2$

For $q = 2$, the torus $T = \{1\}^n$ is a single point and $q - 1 = 1$. Since $p \nmid 1$ for all primes $p \geq 2$, we are always in Case 2: $t(p, 2, n) = (2^n - 1)/1 = 2^n - 1$. This matches the known formula from [1], which was proved by Walsh–Fourier analysis. The present result gives a uniform explanation: every projective direction in $\mathbb{P}^{n-1}(\mathbb{F}_2)$ is needed because the Fourier transform has full support.

9 Computational Verification

We verify Theorem 1.1 computationally for all primes $p \leq 11$ and prime powers $q \leq 11$ with $\text{char}(\mathbb{F}_q) \neq p$, and dimensions $n \leq 4$ (subject to $q^n \leq 300$). The verification uses two independent methods:

(i) *Construction check*: for each (p, q, n), verify that the Fourier inversion construction with $(q-1)^{n-1}$ or $(q^n-1)/(q-1)$ gates produces $\mathbf{1}_T$ in $\mathbb{F}_p$.

(ii) *Optimality check*: for small cases, verify via linear algebra over $\mathbb{F}_p$ that no representation with fewer gates exists.

p	q	Case	$n=1$	$n=2$	$n=3$
2	3	$p \mid (q{-}1)$	1	2	4
2	5	$p \mid (q{-}1)$	1	4	16
3	7	$p \mid (q{-}1)$	1	6	36
5	11	$p \mid (q{-}1)$	1	10	100
3	2	$p \nmid (q{-}1)$	1	3	7
5	3	$p \nmid (q{-}1)$	1	4	13
7	3	$p \nmid (q{-}1)$	1	4	13
3	5	$p \nmid (q{-}1)$	1	6	31
5	7	$p \nmid (q{-}1)$	1	8	57

All values match the formula in Theorem 1.1. Both upper and lower bounds are verified independently.

Acknowledgments

I thank Prof. Makrand Sinha for lecturing on analysis of Boolean functions, which initiated this line of work.

References

[1] Y. Wang. Cross-characteristic gate complexity of the algebraic torus. *ECCC*, 2026.

[2] 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.

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

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

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