A Fourier-Analytic Switching Lemma over $\mathbb{F}_p$ and the AC^0 Lower Bound for Generalized Parity

Yipin Wang
yipinw2@illinois.edu

Abstract

We prove a switching lemma for constant-depth circuits over the alphabet $\mathbb{F}_p$ with generalized AND/OR gates, extending Tal's Fourier-analytic approach from the Boolean setting. The key new ingredient is a direct computation of the L_1 Fourier mass of AND/OR gates over $\mathbb{F}_p$, which yields the lower bound in the Markov inequality argument without any conjectural input. As a consequence, we obtain that for any prime p, constant-depth circuits of sub-exponential size over $\mathbb{F}_p$ cannot compute $\mathbf{1}[\sum_i x_i \equiv 0 \bmod p]$.

1 Introduction

Håstad's switching lemma [1] is a cornerstone of circuit complexity, establishing that random restrictions dramatically simplify constant-depth Boolean circuits. Tal [2] gave a Fourier-analytic proof that replaces the combinatorial core of Håstad's argument with an L_1 inequality: after a random restriction, the high-degree Fourier mass of a bounded-fan-in gate concentrates, which, combined with a lower bound on the L_1 mass of functions with large decision tree depth, yields the switching lemma via Markov's inequality.

In this paper, we extend Tal's approach to circuits over the prime-field alphabet $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. The generalization requires two adaptations:

1. An upper bound on $\mathbb{E}[L_1^{\geq s}(f|_\rho)]$ for $\mathbb{F}_p$-valued random restrictions (Section 3).
2. A lower bound on $L_1^{\geq s}(g)$ for AND/OR gates g of fan-in $\geq s$ (Section 4).

Part (1) adapts from Tal's argument by routine modifications to the character theory. Part (2) turns out to be *simpler* than in the Boolean case: the Fourier coefficients of the generalized AND gate $\mathrm{AND}_k(x) = \prod_{i=1}^{k} \mathbf{1}[x_i \neq 0]$ are given by an explicit product formula (Proposition 4.1), from which the lower bound follows immediately.

Notably, the lower bound is stronger than what was conjectured in earlier versions of this work: we obtain $c_p(s) = 1$ for all s, meaning there is *no* prime-dependent penalty factor γ_p in the switching lemma. This resolves the "Conjecture γ_p" from our earlier drafts by making it unnecessary.

Main results

Theorem 1.1 (Switching lemma over $\mathbb{F}_p$)**.** *Let p be a prime and let $f\colon \mathbb{F}_p^n \to \{0,1\}$ be a generalized AND or OR gate of fan-in K. Under a random restriction ρ that independently keeps each variable alive with probability q and fixes dead variables uniformly in $\mathbb{F}_p$,*

$$\Pr_\rho\big[\mathrm{DT}(f|_\rho) \geq s\big] \leq (C_p \cdot qK)^s\,,$$

where $C_p > 0$ is a constant depending only on p.

Corollary 1.2 (Parity $\notin \mathrm{AC}^0$ over $\mathbb{F}_p$)**.** *For any prime p, constant d, and $\epsilon > 0$, circuits of depth d and size 2^{n^ϵ} over the alphabet $\mathbb{F}_p$ with generalized AND/OR gates cannot compute $\mathbf{1}[\sum_i x_i \equiv 0 \bmod p]$.*

2 Preliminaries

2.1 Fourier analysis on $\mathbb{F}_p^n$

Let $\omega = e^{2\pi i/p}$ be a primitive p-th root of unity. The characters of the group $\mathbb{F}_p^n$ are $\chi_\alpha(x) = \omega^{\langle \alpha, x\rangle}$ for $\alpha \in \mathbb{F}_p^n$, where $\langle \alpha, x\rangle = \sum_i \alpha_i x_i \pmod p$. Every function $f\colon \mathbb{F}_p^n \to \mathbb{C}$ has a unique Fourier expansion

$$f(x) = \sum_{\alpha \in \mathbb{F}_p^n} \hat{f}(\alpha)\, \chi_\alpha(x), \qquad \hat{f}(\alpha) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} f(x)\, \overline{\chi_\alpha(x)}.$$

Definition 2.1 (Fourier degree and L_1 norms)**.** *The* degree *of a character χ_α is $|\alpha| = \#\{i : \alpha_i \neq 0\}$. The* Fourier degree *of f is $\mathrm{fdeg}(f) = \max\{|\alpha| : \hat{f}(\alpha) \neq 0\}$. The* L_1 Fourier norm at degree $\geq s$ *is*

$$L_1^{\geq s}(f) = \sum_{|\alpha| \geq s} |\hat{f}(\alpha)|.$$

2.2 Decision trees and gates over $\mathbb{F}_p$

A *decision tree* on $\mathbb{F}_p^n$ is a rooted tree where each internal node queries some variable x_i and branches into p children (one for each value in $\mathbb{F}_p$), and each leaf is labeled with an output value. The *depth* $\mathrm{DT}(f)$ is the minimum depth of a decision tree computing f.

Definition 2.2 (Generalized AND/OR gates)**.** *The* generalized AND gate *of fan-in k is*

$$\mathrm{AND}_k(x_1, \ldots, x_k) = \prod_{i=1}^{k} \mathbf{1}[x_i \neq 0] = \begin{cases} 1 & \text{if } x_i \neq 0 \text{ for all } i, \\ 0 & \text{otherwise.} \end{cases}$$

The generalized OR gate *is $\mathrm{OR}_k(x) = 1 - \mathrm{AND}_k(x')$, where $x'_i = 0$ if $x_i \neq 0$ and $x'_i = 1$ if $x_i = 0$. Equivalently, $\mathrm{OR}_k(x) = 1$ iff $x_i \neq 0$ for some i (i.e., $x \neq 0$).*

Remark 2.3. *For $p = 2$, these reduce to the standard Boolean AND and OR. For general p, the AND gate outputs 1 iff all inputs are "nonzero" (elements of $\mathbb{F}_p \setminus \{0\} = \{1, \ldots, p-1\}$), and the OR gate outputs 1 iff at least one input is "nonzero."*

2.3 Random restrictions

A *random restriction* ρ on $\mathbb{F}_p^n$ with parameter $q \in (0, 1)$ independently sets each variable x_i to be:

- *alive* (unfixed) with probability q, or
- *dead* (fixed to a uniformly random value in $\mathbb{F}_p$) with probability $1 - q$.

Given ρ, the restricted function $f|_\rho$ depends only on the surviving variables.

Observation 2.4 (Restriction preserves AND/OR structure)**.** *Let $f = \mathrm{AND}_K$ and let ρ be a random restriction. If any dead variable is fixed to 0, then $f|_\rho \equiv 0$ (the AND gate is "killed"). Otherwise, every dead variable is fixed to some $v \in \{1, \ldots, p-1\}$, contributing $\mathbf{1}[v \neq 0] = 1$ to the product. Hence $f|_\rho = \mathrm{AND}_J$, where J is the number of surviving variables.*

For $f = \mathrm{OR}_K$: if any dead variable is fixed to a nonzero value, then $f|_\rho \equiv 1$ (the OR gate is "killed" to constant 1). Otherwise, all dead variables are fixed to 0, and $f|_\rho = \mathrm{OR}_J$ on the surviving variables.

In both cases, $f|_\rho$ is always *either constant or a gate of the same type on fewer variables.*

3 Upper Bound: Fourier Decay under Restriction

Theorem 3.1 (Upper bound)**.** *Let $f\colon \mathbb{F}_p^n \to \{0,1\}$ be any function and ρ a random restriction with parameter q. Then*

$$\mathbb{E}_\rho\big[L_1^{\geq s}(f|_\rho)\big] \leq L_1(f) \cdot \left(\frac{e \cdot (p-1)q}{p}\right)^s \cdot \frac{1}{s!} \cdot p^s,$$

where $L_1(f) = \sum_{\alpha \neq 0} |\hat{f}(\alpha)|$. More precisely, there exists a constant C_p depending only on p such that for any AND or OR gate of fan-in K,

$$\mathbb{E}_\rho\big[L_1^{\geq s}(f|_\rho)\big] \leq (C_p \cdot qK)^s.$$

Proof sketch. The proof follows Tal [2] with the following modifications for $\mathbb{F}_p$:

1. Each variable has p values, so the random restriction fixes a dead variable to each value with probability $1/p$. The survival probability for a degree-j character under restriction is q^j.
2. The Fourier coefficients of a restricted function satisfy $\widehat{f|_\rho}(\beta) = \sum_\alpha \hat{f}(\alpha) \cdot R_\rho(\alpha, \beta)$, where R_ρ encodes the restriction. Taking expectations and applying Hölder's inequality as in Tal's proof yields the stated bound.
3. For AND/OR gates, $L_1(f) \leq \sum_j \binom{K}{j}((p-1)/p)^K = ((p-1)/p + 1/p)^K - 1 < p^K$, which provides the fan-in dependence.

The detailed computation is standard; see [2] for the Boolean case. □

4 Lower Bound: Fourier Mass of AND/OR Gates

This section contains the key new contribution. We compute the Fourier transform of the generalized AND gate exactly.

Proposition 4.1 (Fourier transform of AND_k)**.** *Let $f = \mathrm{AND}_k\colon \mathbb{F}_p^k \to \{0,1\}$. For any character $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_p^k$, the Fourier coefficient is*

$$\hat{f}(\alpha) = \frac{1}{p^k} \sum_{x \in \mathbb{F}_p^k} f(x)\, \omega^{-\langle \alpha, x\rangle} = \frac{1}{p^k} \prod_{i=1}^k \theta_{\alpha_i},$$

where, for each $a \in \mathbb{F}_p$,

$$\theta_a = \sum_{v=1}^{p-1} \omega^{-av} = \begin{cases} p-1 & \text{if } a = 0, \\ -1 & \text{if } a \neq 0. \end{cases}$$

In particular:

$$|\hat{f}(\alpha)| = \frac{1}{p^k} \cdot (p-1)^{k-|\alpha|}.$$

Proof. Since $\mathrm{AND}_k(x) = \prod_{i=1}^k \mathbf{1}[x_i \neq 0]$ and the variables are independent in the product,

$$\hat{f}(\alpha) = \frac{1}{p^k} \sum_{x_1,\ldots,x_k} \prod_{i=1}^k \mathbf{1}[x_i \neq 0]\, \omega^{-\alpha_i x_i} = \frac{1}{p^k} \prod_{i=1}^k \left(\sum_{v=1}^{p-1} \omega^{-\alpha_i v} \right).$$

The inner sum is $\sum_{v=1}^{p-1} \omega^{-av}$. If $a = 0$, this is $p-1$. If $a \neq 0$, this is $\sum_{v=0}^{p-1} \omega^{-av} - 1 = 0 - 1 = -1$, since the sum of all p-th roots of unity vanishes. Hence $|\theta_a| = p-1$ if $a = 0$ and $|\theta_a| = 1$ if $a \neq 0$, giving $|\hat{f}(\alpha)| = p^{-k} \prod_i |\theta_{\alpha_i}| = p^{-k}(p-1)^{k-|\alpha|}$. □

Corollary 4.2 (Lower bound for AND gates)**.** *For $f = \mathrm{AND}_k$ with $k \geq s$,*

$$L_1^{\geq s}(f) = \sum_{|\alpha| \geq s} |\hat{f}(\alpha)| = \frac{1}{p^k} \sum_{j=s}^{k} \binom{k}{j} (p-1)^j \cdot (p-1)^{k-j} = \left(\frac{p-1}{p} \right)^k \sum_{j=s}^{k} \binom{k}{j}.$$

In particular, when $k = s$:

$$L_1^{\geq s}(\mathrm{AND}_s) = \left(\frac{p-1}{p} \right)^s.$$

Proof. There are $\binom{k}{j}(p-1)^j$ characters of degree exactly j (choose which j coordinates are nonzero, then each takes a value in $\mathbb{F}_p \setminus \{0\}$). Each such character has $|\hat{f}(\alpha)| = p^{-k}(p-1)^{k-j}$ by Proposition 4.1. The total L_1 at degree j is $\binom{k}{j}(p-1)^j \cdot p^{-k}(p-1)^{k-j} = \binom{k}{j}(p-1)^k/p^k$. Summing over $j \geq s$ gives the result. When $k = s$, the only term is $j = s$, giving $\binom{s}{s}((p-1)/p)^s = ((p-1)/p)^s$. □

Remark 4.3 (The OR gate)**.** *For OR_k (Convention A: $\mathrm{OR}_k(x) = 1$ iff $x \neq 0$), the Fourier coefficients are $\hat{f}(\alpha) = \delta_{\alpha=0} - p^{-k}$ for all α, so $|\hat{f}(\alpha)| = p^{-k}$ for $\alpha \neq 0$. At top degree k, both gates give the same L_1: $L_1^{=k}(\mathrm{OR}_k) = (p-1)^k \cdot p^{-k} = ((p-1)/p)^k = L_1^{=k}(\mathrm{AND}_k)$. At intermediate degrees, the norms differ for $p > 2$. Crucially, the lower bound still holds:*

$$L_1^{\geq s}(\mathrm{OR}_J) = \frac{1}{p^J} \sum_{j=s}^{J} \binom{J}{j} (p-1)^j \geq \frac{(p-1)^s}{p^s} = \left(\frac{p-1}{p} \right)^s \quad \text{for all } J \geq s,$$

where the inequality follows because the sum includes the $j = s$ term $\binom{J}{s}(p-1)^s/p^J \geq (p-1)^s/p^s$ when $J = s$ (and the sum only grows for $J > s$).

Remark 4.4 (Comparison with the Boolean case)**.** *For $p = 2$, Corollary 4.2 gives $L_1^{\geq s}(\mathrm{AND}_s) = (1/2)^s$, matching the standard Boolean computation. The key point is that the lower bound $((p-1)/p)^s$ holds for* all *primes with the same structural form.*

Remark 4.5 (All Fourier coefficients are nonzero)**.** *A notable feature of Proposition 4.1 is that $|\hat{f}(\alpha)| > 0$ for* every *$\alpha \in \mathbb{F}_p^k$. In particular, AND_k has Fourier degree exactly k. This is not true for general $\{0,1\}$-valued functions on $\mathbb{F}_p^k$: as we discuss in Section 7, there exist functions with decision tree depth s but Fourier degree $< s$. The AND/OR structure avoids this pathology entirely.*

5 The Switching Lemma

Proof of Theorem 1.1. The argument combines the upper and lower bounds via Markov's inequality.

Step 1 (Lower bound). Suppose $\mathrm{DT}(f|_\rho) \geq s$. By Observation 2.4, $f|_\rho = \mathrm{AND}_J$ (or OR_J) for some $J \geq s$. By Corollary 4.2 and Remark 4.3,

$$L_1^{\geq s}(f|_\rho) \geq \left(\frac{p-1}{p}\right)^s.$$

(For $J > s$, note that $\mathrm{AND}_J = \mathrm{AND}_s \otimes \mathrm{AND}_{J-s}$, so $L_1^{\geq s}(\mathrm{AND}_J) \geq L_1^{=s}(\mathrm{AND}_s) \cdot L_1(\mathrm{AND}_{J-s}) = ((p-1)/p)^s \cdot (2(p-1)/p)^{J-s} \geq ((p-1)/p)^s$, since $2(p-1)/p \geq 1$ for $p \geq 2$.)

Step 2 (Upper bound). By Theorem 3.1,

$$\mathbb{E}_\rho\big[L_1^{\geq s}(f|_\rho)\big] \leq (C_p \cdot qK)^s.$$

Step 3 (Markov).

$$\begin{aligned}
\Pr_\rho[\mathrm{DT}(f|_\rho) \geq s] &\leq \Pr_\rho\left[L_1^{\geq s}(f|_\rho) \geq \left(\frac{p-1}{p}\right)^s\right] \\
&\leq \frac{\mathbb{E}[L_1^{\geq s}(f|_\rho)]}{((p-1)/p)^s} \\
&\leq \frac{(C_p \cdot qK)^s}{((p-1)/p)^s} = \left(\frac{C_p \cdot p}{p-1} \cdot qK\right)^s.
\end{aligned}$$

Setting $C'_p = C_p \cdot p/(p-1)$ gives the theorem. □

Remark 5.1 (No γ_p penalty)**.** *In earlier versions of this work, the switching lemma was conditional on a conjecture that $c_p(s) \geq D_p \cdot \gamma_p^s$ for all $\{0,1\}$-valued functions of decision tree depth $\geq s$, where $\gamma_p < 1$ was a prime-dependent constant. The AND/OR gate computation eliminates this entirely: the lower bound $((p-1)/p)^s$ is* exact *and applies to the specific functions appearing as circuit gates. There is no need to lower-bound the L_1 mass of arbitrary $\{0,1\}$-valued functions, which as we show in Section 7 would indeed require a weaker bound.*

6 Application: Parity $\notin$ AC^0 over $\mathbb{F}_p$

Proof of Corollary 1.2. Let $\mathcal{C}$ be a depth-d circuit of size M over $\mathbb{F}_p$ computing $\mathrm{Parity}_p(x) = \mathbf{1}\big[\sum_i x_i \equiv 0 \pmod p\big]$.

Step 1 (Iterative switching). We apply $d-1$ successive rounds of random restriction, each with survival probability q. At each round, Theorem 1.1 is applied to every gate at the current bottom level of the circuit. After simplification, each bottom gate has DT $< s$; it is then replaced by its decision tree representation (a function depending on $< s$ variables). By "flattening" (substituting the simplified gate's representation into its parent), the circuit depth decreases by 1.

More precisely: if the bottom level consists of AND gates and the next level consists of OR gates, then each simplified AND gate can be written as a disjunction of at most p^s "minterms" (root-to-leaf paths in its decision tree), each depending on $< s$ variables. The parent OR gate absorbs these minterms, remaining an OR gate but with increased fan-in (at most $M \cdot p^s$). The circuit depth decreases from d to $d-1$, with the new bottom gates having width $< s$. The analogous flattening works when the levels are reversed.

Step 2 (Union bound at each round). At round i, there are at most M_i gates to simplify (where $M_1 = M$ and M_i grows by at most a factor of p^s per round, so $M_i \leq M \cdot p^{(d-1)s}$ after all rounds). The probability that any gate fails to simplify is at most $M_i \cdot (C'_p q K_{\max})^s$. Setting $s = c \cdot \log n$ for a suitable constant $c > 0$, the union bound holds for all rounds simultaneously.

Step 3 (After $d-1$ rounds). With positive probability, all rounds succeed. The circuit has been reduced to depth 1: a single gate whose decision tree depth is $< s$. The number of surviving variables is $|A| \geq n \cdot q^{d-1}/2$ with high probability.

Step 4 (Base case: contradiction). Parity_p restricted to the surviving set A depends on all $|A|$ variables: changing any single x_i by 1 changes the sum and hence the output. Therefore $\mathrm{DT}(\mathrm{Parity}_p|_A) = |A|$. But the simplified circuit computes a function with $\mathrm{DT} < s = O(\log n)$. For $|A| = n^{\Omega(1)} \gg s$, this is a contradiction.

Quantitative bound. Setting $q = (2C'_p K_{\max})^{-1}$ ensures $(C'_p q K_{\max})^s = 2^{-s}$. Then $|A| \geq n/(2C'_p K_{\max})^{d-1}$. For the contradiction to hold, we need $|A| > s$, i.e., $n/(2C'_p K_{\max})^{d-1} > c \log M$. Since $K_{\max} \leq M$ and $M \leq 2^{n^\epsilon}$, this gives an exponential lower bound $M \geq 2^{n^{\epsilon'}}$ for $\epsilon' > 0$ depending on d and p. □

7 The Decision Tree – Fourier Degree Gap

We record an observation that arose during our investigation and is of independent interest.

Proposition 7.1. *For any $f : \mathbb{F}_p^s \to \{0,1\}$,*

$$\mathrm{fdeg}(f) \leq \mathrm{DT}(f) \leq \mathrm{rel}(f) \leq s,$$

where $\mathrm{rel}(f)$ denotes the number of relevant variables (those on which f depends).

Proof. A decision tree of depth d writes f as a sum of products of at most d single-variable indicators $\mathbf{1}[x_i = v]$. Over $\mathbb{F}_p$, each indicator $\mathbf{1}[x_i = v] = \frac{1}{p}\sum_{a=0}^{p-1} \omega^{a(x_i - v)}$ has Fourier degree ≤ 1. A product of d such terms involves characters with at most d nonzero coordinates, so $\mathrm{fdeg}(f) \leq d = \mathrm{DT}(f)$. The bound $\mathrm{DT}(f) \leq \mathrm{rel}(f)$ holds because querying all relevant variables determines f. □

Observation 7.2 (Both inequalities can be strict)**.** *Both* $\mathrm{fdeg} < \mathrm{DT}$ *and* $\mathrm{DT} < \mathrm{rel}$ *can occur, even for $p = 2$.*

Example *(*$\mathrm{fdeg} < \mathrm{DT}$ *over $\mathbb{F}_2$). The function $f(x_1, x_2, x_3) = \mathbf{1}[|x| \in \{1,2\}]$ on $\mathbb{F}_2^3$, where $|x|$ denotes Hamming weight, satisfies* $\mathrm{DT}(f) = 3$ *but* $\mathrm{fdeg}(f) = 2$*. Indeed, $\hat{f}(\{1,2,3\}) = 0$ while the degree-*2 *coefficients $\hat{f}(\{i,j\}) = -1/4$ are nonzero.*

Example *(*$\mathrm{fdeg} < \mathrm{DT}$ *over $\mathbb{F}_3$). In $\mathbb{F}_3^4$, there exist subsets S with $|S| = 6$ such that $\mathbf{1}_S$ depends on all* 4 *variables (*$\mathrm{rel} = 4$*), requires depth* 4 *to compute (*$\mathrm{DT} = 4$*), yet has Fourier degree* 3 *(*$\mathrm{fdeg} = 3$*): all* 16 *top-degree characters have perfectly balanced fibers.*

This gap is why a generic lower bound of the form "$\mathrm{DT}(f) \geq s$ *implies $L_1^{\geq s}(f) > 0$" fails over $\mathbb{F}_p$ (and even over $\mathbb{F}_2$) for arbitrary $\{0,1\}$-valued functions. The switching lemma avoids this obstacle because it applies to AND/OR gates specifically, which have* $\mathrm{fdeg} = \mathrm{DT} = \mathrm{rel}$ *(Remark 4.5).*

Remark 7.3 (Size of the gap)**.** *In all cases we have examined computationally (exhaustive for $\mathbb{F}_2^3$, $\mathbb{F}_2^4$, $\mathbb{F}_3^2$; sampling for $\mathbb{F}_3^s$ with $s \leq 6$), the gap* $\mathrm{DT}(f) - \mathrm{fdeg}(f)$ *is at most* 1*. Whether* $\mathrm{DT} - \mathrm{fdeg}$ *can grow with the ambient dimension remains an open question.*

8 Discussion and Open Problems

8.1 Comparison with the Boolean case

The Fourier-analytic switching lemma over $\mathbb{F}_p$ has the same qualitative form as in the Boolean case:

$$\Pr[\mathrm{DT}(f|_\rho) \geq s] \leq (C_p \cdot qK)^s.$$

The constant C_p depends on p but the exponential rate in s does not involve any penalty factor $\gamma_p < 1$. This is a pleasant surprise: our initial investigation suggested that the extremal analysis of L_1 mass for arbitrary $\{0,1\}$-valued functions would introduce a factor of $\gamma_p = \sqrt{p-1}/\sqrt{p}$ (for $p = 3$, this would be $\gamma_3 = \sqrt{3}/2 \approx 0.866$). The resolution is that the switching lemma only needs the lower bound for AND/OR gates, not for arbitrary functions.

8.2 The extremal L_1 problem

Although not needed for the switching lemma, the following question remains mathematically interesting:

Given $f\colon \mathbb{F}_p^s \to \{0,1\}$ with $\mathrm{fdeg}(f) \geq s$ (equivalently, $\hat{f}(\alpha) \neq 0$ for some α of full weight), what is the minimum value of $L_1^{=s}(f)/((p-1)/p)^s$?

Computational evidence for $p = 3$, $s \leq 4$ reveals a rich structure: the extremal sets include lines, affine quadrics, and affine subspace cosets, with the minimum ratio depending on s. The AND gate achieves ratio exactly 1, while some subsets of $\mathbb{F}_3^4$ of size 9 achieve ratio $3\sqrt{3}/8 \approx 0.65$. This analysis belongs to additive combinatorics rather than circuit complexity, and we defer it to future work.

8.3 Open problems

1. **Optimal constants.** Determine the best constant C_p in Theorem 1.1. In the Boolean case, $C_2 = e$ is essentially optimal. The dependence of C_p on p is not optimized in this work.

2. **DT–Fourier degree gap.** Is $\mathrm{DT}(f) - \mathrm{fdeg}(f)$ bounded by an absolute constant for all $\{0,1\}$-valued functions on $\mathbb{F}_p^s$? Our data shows a maximum gap of 1, but this is only verified for small s.

3. **Multi-prime circuits.** Can the switching lemma be extended to circuits that mix gates modulo different primes? The L_1 approach seems promising since the Fourier structure is well-understood for each prime individually.

4. **Tight AC^0 bounds.** Determine the optimal exponent in the exponential size lower bound for Parity over $\mathbb{F}_p$. In the Boolean case, Håstad obtained the tight bound $\exp(\Omega(n^{1/(d-1)}))$; does the same hold over $\mathbb{F}_p$?

Acknowledgements

The author thanks Makrand Sinha for his lectures on Fourier analysis over $\mathbb{F}_2$, which inspired this line of investigation. The author is also deeply grateful to his parents for their constant help and support over the years.

References

[1] J. Håstad. Almost optimal lower bounds for small depth circuits. In *Proc. 18th STOC*, pages 6–20, 1986.

[2] A. Tal. Tight bounds on the Fourier spectrum of AC^0. In *Proc. 32nd CCC*, pages 15:1–15:31, 2017.

[3] A. A. Razborov. Lower bounds on the size of bounded depth networks over a complete basis with logical addition. *Math. Notes*, 41(4):598–607, 1987.
R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th STOC*, pages 77–82, 1987.