Switching Lemmas over $\mathbb{F}_p$ and Tight AC^0 Lower Bounds

Abstract

We give two switching lemmas over $\mathbb{F}_p$ and derive a tight lower bound for AC^0 circuits computing generalized parity. First, we observe that the single-gate switching lemma of [3] — $\Pr[\mathrm{DT}(f|_\rho) \geq s] \leq (C_p qK/s)^s$ for an AND or OR gate of fan-in K — already suffices for a tight $\exp(\Omega_p(n^{1/(d-1)}))$ lower bound on depth-d circuits, resolving the AC^0 question over $\mathbb{F}_p$. Second, we prove a multi-clause *representability* switching lemma via Håstad's injection: for a width-w CNF with M clauses, $\Pr[\mathrm{C}_1(f|_\rho) > s] \leq (Mwpq/(1-q))^s$, where C_1 is the 1-certificate complexity. For the AC^0 application, the factor of M is absorbed by the union bound. We discuss the open problem of obtaining an M-independent bound matching Håstad's Boolean result.

1 Introduction

1.1 Background

Håstad's switching lemma [1] states that for a width-w CNF f over $\{0,1\}^n$ and a random restriction ρ keeping each variable alive with probability q:

$$\Pr\big[f|_\rho \text{ has no width-}s \text{ DNF}\big] \leq (Cwq)^s,$$

where C is an absolute constant. Two features are essential for the tight AC^0 lower bound: (i) no dependence on the number of clauses M, and (ii) no factor of $1/s^s$.

Over $\mathbb{F}_p$, the recent work [3] proved a switching lemma for single gates:

$$\Pr[\mathrm{DT}(f|_\rho) \geq s] \leq \left(\frac{C_p \cdot qK}{s}\right)^s \tag{1}$$

for an AND or OR gate of fan-in K, where $C_p = O(p)$. The $1/s^s$ factor is *tight* for single gates (it matches the Chernoff bound on the binomial count of surviving variables).

In this note, we make two contributions:

1. We show that the single-gate bound (1) already implies the tight AC^0 lower bound $\exp(\Omega_p(n^{1/(d-1)}))$ over $\mathbb{F}_p$. The $1/s^s$ factor is handled by the union bound in the standard depth-reduction argument, affecting only the constant in the exponent (not the asymptotic form).
2. We prove a multi-clause representability switching lemma over $\mathbb{F}_p$ via Håstad's injection, giving $\Pr[\mathrm{C}_1(f|_\rho) > s] \leq (Mwpq/(1-q))^s$ for width-w CNFs. For the AC^0 application, the M factor is absorbed into the union bound.

1.2 Setup

We work over $\mathbb{Z}_p^n$ for a prime p. A *literal* is $\ell_i(x) = \mathbf{1}[x_i \neq 0]$. A *width-$w$ CNF* is $f = D_1 \wedge \cdots \wedge D_M$ where each clause is $D_j(x) = \bigvee_{i \in S_j} \ell_i(x)$ with $|S_j| \leq w$.

A *random restriction* $\rho \sim \rho_q$ independently sets each variable to: alive with probability q, or dead with value $v \in \mathbb{F}_p$ with probability $(1-q)/p$ each. We write $A(\rho)$ for the alive set and $\sigma(\rho)$ for the dead assignment.

The *1-certificate complexity* $\mathrm{C}_1(f)$ is the maximum over 1-inputs of the minimum certificate size. By a standard equivalence (Proposition 3), f has a width-s DNF if and only if $\mathrm{C}_1(f) \leq s$.

2 Tight AC^0 lower bound from the single-gate lemma

Theorem 1 (AC^0 lower bound over $\mathbb{F}_p$)**.** *For any prime p and constant depth $d \geq 2$, any depth-d circuit over $\mathbb{F}_p$ computing $\mathrm{PAR}_p(x) = \mathbf{1}[\sum_i x_i \not\equiv 0 \pmod{p}]$ has size $\exp(\Omega_p(n^{1/(d-1)}))$.*

Proof. Let C be a depth-d circuit of size S computing PAR_p on $\mathbb{F}_p^n$, where all gates are AND/OR of the $\mathbb{F}_p$ literals ℓ_i.

We apply $d-1$ rounds of random restriction. At round i:

- The circuit has depth $d+1-i$, with bottom-level gates of fan-in at most w_i.
- Apply ρ_i with parameter $q_i = 1/(C_p w_i)$.
- By the single-gate bound (1), each bottom gate g (fan-in $\leq w_i$) satisfies $\Pr[\mathrm{DT}(g|_\rho) \geq s_i] \leq (1/s_i)^{s_i}$.
- Set s_i so that $S \cdot (1/s_i)^{s_i} < 1$. This requires $s_i \cdot \ln s_i > \ln S$, satisfied by $s_i = \lceil \ln S / \ln \ln S \rceil$.
- Union bound: with positive probability, every bottom gate simplifies to DT depth $\leq s_i$.
- Replace each bottom gate by its depth-s_i decision tree. This reduces the circuit depth by 1 and sets the new bottom fan-in to $w_{i+1} = s_i$.

Initial fan-in: $w_1 = w \leq S$. After round 1: $w_2 = s_1 = \Theta(\ln S / \ln \ln S)$. For $i \geq 2$: $w_i = s_{i-1} = \Theta(\ln S / \ln \ln S)$ (since S doesn't change much between rounds).

After $d-1$ rounds, the number of surviving alive variables is:

$$n' = n \cdot \prod_{i=1}^{d-1} q_i = \frac{n}{C_p^{d-1} \cdot \prod_{i=1}^{d-1} w_i} = \frac{n}{C_p^{d-1} \cdot w \cdot s^{d-2}}$$

where $s = \Theta(\ln S / \ln \ln S)$.

For PAR_p to survive (remain non-constant), we need $n' \geq 1$, giving:

$$w \leq \frac{n}{C_p^{d-1} \cdot s^{d-2}}.$$

Since $w \le S$ and $s = \Theta(\ln S/\ln\ln S)$, substituting $S = \exp(\alpha \cdot n^{1/(d-1)})$ for some constant α:

$$\begin{aligned} s &= \Theta\left(\frac{\alpha \cdot n^{1/(d-1)}}{\ln(\alpha \cdot n^{1/(d-1)})}\right) = \Theta\left(\frac{n^{1/(d-1)}}{\ln n}\right), \\ w \cdot s^{d-2} &\le \frac{n}{C_p^{d-1}}, \\ \exp(\alpha \cdot n^{1/(d-1)}) \cdot \left(\frac{n^{1/(d-1)}}{\ln n}\right)^{d-2} &\le \frac{n}{C_p^{d-1}}. \end{aligned}$$

For α sufficiently small (depending on p and d), the left side grows as $\exp(\Omega(n^{1/(d-1)}))$ while the right side is polynomial. This gives a contradiction, proving $S \ge \exp(\Omega_p(n^{1/(d-1)}))$. $\square$

Remark 2 (Comparison with multi-clause switching). Using a multi-clause switching lemma *without* $1/s^s$ would give $s = \Theta(\ln S)$ instead of $\Theta(\ln S/\ln\ln S)$. This improves the constant in the exponent by a factor of $(\ln\ln S)^{d-2} = (\ln n)^{O(1)}$, yielding $S \ge \exp(c_p \cdot n^{1/(d-1)})$ with a better constant c_p. The *asymptotic* form $\exp(\Omega(n^{1/(d-1)}))$ is the same either way.

3 Multi-clause representability switching lemma

We now prove a switching lemma for multi-clause CNFs over $\mathbb{F}_p$.

Proposition 3. *$f\colon \mathbb{F}_p^n \to \{0,1\}$ has a width-s DNF iff* $\mathrm{C}_1(f) \le s$.

Proof. Standard: a width-s DNF gives 1-certificates of size $\le s$ (from satisfying terms), and conversely, 1-certificates of size $\le s$ define width-s terms. $\square$

3.1 Clause survival and certificates

For a CNF $f = D_1 \wedge \cdots \wedge D_M$, clause D_j *survives* ρ if no dead variable in S_j has a nonzero value. Killed clauses are identically 1 after restriction.

Proposition 4. $\mathrm{C}_1(f|_\rho)$ *equals the minimum number of alive variables needed to hit every surviving clause (by assigning nonzero values).*

Theorem 5 (Multi-clause switching lemma)**.** *Let $f = D_1 \wedge \cdots \wedge D_M$ be a width-w CNF over $\mathbb{F}_p^n$. For $\rho \sim \rho_q$:*

$$\Pr[\mathrm{C}_1(f|_\rho) > s] \le \binom{M}{s} \cdot \left(\frac{wpq}{1-q}\right)^s \le \left(\frac{eMwpq}{s(1-q)}\right)^s.$$

Proof. Let $\mathrm{BAD} = \{\rho : \mathrm{C}_1(f|_\rho) > s\}$.

Canonical staircase. For $\rho \in \mathrm{BAD}$, define the staircase by processing surviving clauses in index order. For each unhit surviving clause D_j (in order $j = 1, 2, \ldots, M$), select the smallest-index alive variable $i \in S_j$ not already selected. Since $\mathrm{C}_1 > s$, this produces s variables $i_1, \ldots, i_s$ from s distinct clauses $j_1 < j_2 < \cdots < j_s$, with $i_t \in S_{j_t}$.

Write $p_t = \mathrm{pos}(i_t, S_{j_t}) \in \{0, \ldots, w-1\}$ for the position of i_t in S_{j_t} (sorted order).

Injection. Define $\Phi(\rho) = (\tilde\rho, \tau)$ where:

- $\tilde\rho$ agrees with ρ except $i_1, \ldots, i_s$ are dead with value 0.

- $\tau = (j_1, p_1, \ldots, j_s, p_s)$ is the *encoding.*

Clause preservation. Since we kill to value 0, no clause gains a nonzero dead variable: the surviving clauses of $\tilde{\rho}$ are the same as those of ρ.

Injectivity. Given $(\tilde{\rho}, \tau)$, the variables i_t are determined by (j_t, p_t) (as the p_t-th element of S_{j_t}), and ρ is recovered by making $i_1, \ldots, i_s$ alive. This uniquely determines ρ.

Probability ratio. $\Pr[\rho]/\Pr[\tilde{\rho}] = (pq/(1-q))^s$, since each i_t changes from alive (prob q) to dead-with-0 (prob $(1-q)/p$).

Encoding count. Partition $\mathrm{BAD} = \bigsqcup_\tau \mathrm{BAD}_\tau$ by encoding. For fixed τ, the map $\rho \mapsto \tilde{\rho}$ is injective on BAD_τ, so:

$$\Pr[\mathrm{BAD}_\tau] = \left(\frac{pq}{1-q}\right)^s \sum_{\rho \in \mathrm{BAD}_\tau} \Pr[\tilde{\rho}] \leq \left(\frac{pq}{1-q}\right)^s.$$

The number of distinct encodings τ: the clause indices $j_1 < \cdots < j_s$ range over $\binom{M}{s}$ subsets of $[M]$, and each position p_t takes at most w values. Total:

$$|\{\tau\}| \leq \binom{M}{s} \cdot w^s.$$

Combining:

$$\Pr[\mathrm{BAD}] \leq \binom{M}{s} \cdot w^s \cdot \left(\frac{pq}{1-q}\right)^s = \binom{M}{s} \cdot \left(\frac{wpq}{1-q}\right)^s. \qquad \square$$

Remark 6 (Comparison with Håstad). In the Boolean case ($p = 2$), Håstad achieves the stronger bound $(Cwq)^s$ with *no* factor of M or $\binom{M}{s}$. This is proved via the canonical decision tree (CDT) approach, where the encoding at each step records the "branching direction" within a clause (at most w choices), and the clause index is determined by the CDT state. Adapting the CDT approach to $\mathbb{F}_p$ to obtain an M-independent bound is an interesting open problem; the difficulty lies in the p-ary branching structure of decision trees over $\mathbb{F}_p$.

3.2 Application to AC^0

The multi-clause bound of Theorem 5, despite the M factor, also gives the tight AC^0 lower bound:

Corollary 7. *Theorem 5 implies Theorem 1 with an improved constant in the exponent.*

Proof sketch. In the depth-reduction argument, at each round we apply Theorem 5 with $M \leq S$ (circuit size) and w the current bottom fan-in. Setting $q = c/(wpS^{1/s})$ for small c:

$$\binom{M}{s}\left(\frac{wpq}{1-q}\right)^s \leq \left(\frac{eM}{s}\right)^s \cdot c^s \leq \left(\frac{eS}{s}\right)^s \cdot c^s.$$

Choosing $s = \Theta(\ln S)$ and c sufficiently small, this is $< 1/S$, allowing a union bound.

Since $s = \Theta(\ln S)$ (rather than $\Theta(\ln S / \ln\ln S)$ from the single-gate lemma), the surviving variable count improves by a factor of $(\ln\ln S)^{d-2} = (\ln n)^{O(1)}$ in the exponent. $\square$

4 Discussion and open problems

1. **M-independent multi-clause bound.** The main gap between our result and Håstad's Boolean bound is the factor of $\binom{M}{s}$. In the Boolean case, this is eliminated via the CDT approach. Over $\mathbb{F}_p$, the CDT has p-ary branching, and extracting a w-bounded encoding at each step requires new ideas. We conjecture that $\Pr[\mathrm{C}_1(f|_\rho) > s] \leq (C_p wq)^s$ holds without M-dependence.

2. **DT-depth multi-clause bound.** A stronger result would be $\Pr[\mathrm{DT}(f|_\rho) \geq s] \leq (C_p wq)^s$ for width-w CNFs. This would require adapting either the CDT approach or Tal's Fourier-analytic method [2] to $\mathbb{Z}_p^n$.

3. **Optimal constant C_p.** Our bounds give $C_p = O(p)$. In the Boolean case, $C_p \approx 7$ (optimized by various authors). It is unclear whether C_p can be made $O(1)$ independent of p.

4. **Beyond $\mathbf{AC}^0$.** The switching lemma over $\mathbb{F}_p$ is a step toward understanding the interaction between p-ary arithmetic and Boolean circuit complexity, relevant to lower bounds for ACC^0 and related classes.

References

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

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

[3] *A switching lemma for AND/OR gates over* $\mathbb{F}_p$ *and the* AC^0 *lower bound for generalized parity*, submitted to CCC 2026.

[4] P. Beame, *A switching lemma primer*, Technical Report UW-CSE-95-07-01, University of Washington, 1994.