**Limited independence fools $\mathsf{AC}^0$ (lecture notes)**

Course: Circuit Complexity, Autumn 2024, University of Chicago
Instructor: William Hoza (`williamhoza@uchicago.edu`)

---

**Definition 1** ($k$-wise uniformity)**.** Let $X$ be a distribution over $\{0,1\}^n$, and let $k \in [n]$. We say that $X$ is *$k$-wise uniform* if, for every $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, the substring $X_{i_1} X_{i_2} \dots X_{i_k}$ is distributed uniformly over $\{0,1\}^k$.

Our goal in these notes is to prove the following.

**Theorem 1** (Limited independence fools $\mathsf{AC}^0$)**.** *Let $d \in \mathbb{N}$ be a constant. For every $S \in \mathbb{N}$ and $\varepsilon > 0$, there is a value $k = \operatorname{polylog}(S) \cdot \log(1/\varepsilon)$ such that if $X \in \{0,1\}^n$ is $k$-wise uniform and $S \geq n$, then $X$ fools size-$S$ $\mathsf{AC}^0_d$ circuits with error $\varepsilon$.*

Bazzi proved the $d = 2$ case of Theorem 1 [Baz09], then Razborov simplified the proof [Raz09], and then Braverman proved the general case [Bra10] (albeit with a worse dependence on $\varepsilon$). Consequently, Theorem 1 is sometimes called "Braverman's theorem." There were quantitative improvements after Braverman's work [Tal17; HS19]. For non-constant $d$, the best bound currently known is $k = (\log S)^{O(d)} \cdot \log(1/\varepsilon)$ [HS19]. In these lecture notes, for simplicity, we focus on the constant-depth case. We will present a proof of Theorem 1 due to Hatami and Hoza [HH24].

## 1 Polynomial approximations for $\mathsf{AC}^0$ circuits

**Proposition 1.** *If $X$ is $k$-wise uniform, then $X$ fools degree-$k$ real multilinear polynomials (with error zero).*

*Proof.* This follows from linearity of expectation. □

In this course, we have seen that $\mathsf{AC}^0$ circuits can be "approximated" by low-degree polynomials in two different ways. First, we saw how to simulate $\mathsf{AC}^0$ circuits using probabilistic polynomials. Second, we saw a Fourier tail bound for $\mathsf{AC}^0$ circuits, which implies the following approximation.

**Lemma 1** (Low-degree $L_2$ approximations for $\mathsf{AC}^0$)**.** *Let $C \colon \{0,1\}^n \to \{0,1\}$ be an $\mathsf{AC}^0_d$ circuit of size $S$. Then for every $\varepsilon \in (0,1)$, there exists a polynomial $\widetilde{C} \in \mathbb{R}[x_1, \dots, x_n]$ of degree $O(\log S)^{d-1} \cdot \log(1/\varepsilon)$ such that $\mathbb{E}_{x \in \{0,1\}^n}[(C(x) - \widetilde{C}(x))^2] \leq \varepsilon$. Furthermore, for every $x \in \{0,1\}^n$, we have $|\widetilde{C}(x)| \leq n^{O(\log S)^{d-1} \cdot \log(1/\varepsilon)}$.*[1]

*Proof.* Let $f(x) = (-1)^{C(x)}$. Define $f^{<k}$ by dropping all the terms of degree at least $k$ from the Fourier expansion of $f$:

$$f^{<k}(x) = \sum_{\substack{S \subseteq [n] \\ |S| < k}} \widehat{f}(S) \cdot \chi_S(x).$$

Then define $\widetilde{C}(x) = \frac{1}{2} - \frac{1}{2} f^{<k}(x)$. We have

$$C(x) - \widetilde{C}(x) = \left(\frac{1}{2} - \frac{1}{2} f(x)\right) - \left(\frac{1}{2} - \frac{1}{2} f^{<k}(x)\right) = \frac{1}{2} \cdot \left(f^{<k}(x) - f(x)\right),$$

and hence

$$\mathop{\mathbb{E}}_x[(C(x) - \widetilde{C}(x))^2] = \frac{1}{4} \mathop{\mathbb{E}}_x[(f^{<k}(x) - f(x))^2] = \frac{1}{4} \cdot \sum_{\substack{S \subseteq [n] \\ |S| \geq k}} \widehat{f}(S)^2 \leq \frac{1}{4} \cdot 2 \cdot 2^{-k/O(\log S)^{d-1}},$$

by Parseval's theorem and the Fourier tail bound for $\mathsf{AC}^0$. If we choose a suitable value $k = O(\log S)^{d-1} \cdot \log(1/\varepsilon)$, then the error is at most $\varepsilon$. Finally, note that each Fourier coefficient of $f$ is at most 1, so by the triangle inequality, for every $x$, we have $|\widetilde{C}(x)| \leq \frac{1}{2} + \frac{1}{2}\binom{n}{k} \leq n^{O(k)}$. □

[1] It is possible to slightly improve the bound on $|\widetilde{C}(x)|$ [Tal17].

The fact that $\mathsf{AC}^0$ circuits can be "approximated" by low-degree polynomials (in multiple ways!) *suggests* that limited independence ought to fool $\mathsf{AC}^0$ circuits. To actually prove it, we will construct yet another low-degree "approximation" for $\mathsf{AC}^0$ circuits. Specifically, we will show that $\mathsf{AC}^0$ circuits have low-degree *sandwiching polynomials*.

**Definition 2** (Sandwiching)**.** Let $C, C_-, C_+ \colon \{0,1\}^n \to \mathbb{R}$. We say that $C$ is *$\varepsilon$-sandwiched* between $C_-$ and $C_+$ if the following two conditions hold.

1. For every $x \in \{0,1\}^n$, we have $C_-(x) \leq C(x) \leq C_+(x)$.
2. We have $\mathbb{E}_{x \in \{0,1\}^n}[C_+(x) - C_-(x)] \leq \varepsilon$.

**Theorem 2** ($\mathsf{AC}^0$ circuits have low-degree sandwichers)**.** *Let $d \in \mathbb{N}$ be a constant. Let $C \colon \{0,1\}^n \to \{0,1\}$ be an $\mathsf{AC}^0_d$ circuit of size $S \geq n$, and let $\varepsilon \in (0,1)$. Then $C$ is $\varepsilon$-sandwiched between polynomials of degree at most* $\operatorname{polylog}(S) \cdot \log(1/\varepsilon)$.

We will prove Theorem 2 in the next section. First, let us show how to use Theorem 2 to prove Theorem 1.

*Proof of Theorem 1 using Theorem 2.* Let $C_-$, $C_+$ be $\varepsilon$-sandwichers for $C$. Then

$$\mathbb{E}[C(X)] \leq \mathbb{E}[C_+(X)] = \mathbb{E}[C_+(U_n)] \leq \mathbb{E}[C_-(U_n)] + \varepsilon \leq \mathbb{E}[C(U_n)] + \varepsilon,$$

and similarly

$$\mathbb{E}[C(X)] \geq \mathbb{E}[C_-(X)] = E[C_-(U_n)] \geq \mathbb{E}[C_+(U_n)] - \varepsilon \geq \mathbb{E}[C(U_n)] - \varepsilon. \qquad \square$$

In fact, it turns out that Theorems 1 and 2 are equivalent, i.e., a class is fooled by all $k$-wise uniform distributions if and only if it is sandwiched between degree-$k$ polynomials.

## 2 Constructing sandwiching polynomials

We will prove Theorem 2 by induction on $d$, the depth of the circuit.

### 2.1 The base case

Suppose $d = 1$. By negating the circuit if necessary, we may assume that $C$ is a conjunction of literals. If it is a conjunction of at most $\log(1/\varepsilon)$ literals, then $\deg(C) \leq \log(1/\varepsilon)$, so we are done. If it is a conjunction of more than $\log(1/\varepsilon)$ literals, then it is $\varepsilon$-sandwiched between 0 and the product of the first $\log(1/\varepsilon)$ literals.

### 2.2 The inductive step

Suppose $d \geq 2$. By negating the circuit if necessary, we may assume that $C = \bigvee_{i=1}^m C_i$, where each $C_i$ is a depth-$(d-1)$ circuit with "AND" gates on top. For each $i \in [m]$, define $F_i = \bigwedge_{j=1}^{i-1} (\neg C_i)$, so $F_i$ is an $\mathsf{AC}^0_d$ circuit of size at most $S$ and $C = \sum_{i=1}^m C_i \cdot F_i$.

By Lemma 1, for each $i \in [m]$, there exists a polynomial $\widetilde{F}_i$ of degree $\operatorname{polylog}(S) \cdot \log(1/\varepsilon)$ such that $\mathbb{E}_x[(F_i(x) - \widetilde{F}_i(x))^2] \leq \varepsilon/(2m^3)$. Furthermore, for every $x \in \{0,1\}^n$, we have $|\widetilde{F}_i(x)| \leq 2^{\operatorname{polylog}(S) \cdot \log(1/\varepsilon)}$. Define

$$\begin{aligned}
\widetilde{C} &= \sum_{i=1}^m C_i \cdot \widetilde{F}_i \\
C_- &= C - (C - \widetilde{C})^2 \\
C_+ &= C + (C - \widetilde{C})^2 \cdot \left( \left( \sum_{i=1}^m C_i \right) - C \right).
\end{aligned}$$

First, we will show that $C$ is sandwiched between $C_-$ and $C_+$. Then, we will use our induction hypothesis to show that $C_-$ and $C_+$ are sandwiched between low-degree polynomials.

### 2.2.1 $C$ is sandwiched between $C_-$ and $C_+$

From the definitions, it is clear that $C_- \leq C \leq C_+$. Furthermore,

$$\begin{aligned}
\mathop{\mathbb{E}}_x[C_+(x) - C_-(x)] &= \mathop{\mathbb{E}}_x\left[(C(x) - \widetilde{C}(x))^2 \cdot \left(\left(\sum_{i=1}^m C_i(x)\right) - C(x) + 1\right)\right] \\
&\leq m \cdot \mathop{\mathbb{E}}_x\left[(C(x) - \widetilde{C}(x))^2\right] \\
&= m \cdot \mathop{\mathbb{E}}_x\left[\left(\sum_{i=1}^m C_i(x) \cdot (F_i(x) - \widetilde{F}_i(x))\right)^2\right] \\
&\leq m^2 \cdot \sum_{i=1}^m \mathop{\mathbb{E}}_x[(F_i(x) - \widetilde{F}_i(x))^2] \\
&\leq \varepsilon/2.
\end{aligned}$$

### 2.2.2 $C_-$ and $C_+$ have low-degree sandwichers

By case analysis (either $C = 1$ or $C = 0$), one can show that

$$\begin{aligned}
C_- &= 1 - (1 - \widetilde{C})^2 \\
C_+ &= 1 + (1 - \widetilde{C})^2 \cdot \left(\left(\sum_{i=1}^m C_i\right) - 1\right).
\end{aligned}$$

From here, let us focus on $C_+$ for simplicity (the analysis of $C_-$ is similar). Plugging the definition of $\widetilde{C}$ into the formula above gives us

$$C_+ = 1 + \left(1 - \sum_{i=1}^m C_i \cdot \widetilde{F}_i\right)^2 \cdot \left(-1 + \sum_{i=1}^m C_i\right).$$

If we define $C_0 = \widetilde{F}_0 = 1$ and we suitably define $c_{i,j,k} \in \{-1, 0, 1\}$ for $0 \leq i, j, k \leq m$, then we can expand the formula above as follows.

$$C_+ = \sum_{i=0}^m \sum_{j=0}^m \sum_{k=0}^m c_{i,j,k} \cdot C_i \cdot C_j \cdot C_k \cdot \widetilde{F}_i \cdot \widetilde{F}_j.$$

Let us focus on a single term $c_{i,j,k} \cdot C_i \cdot C_j \cdot C_k \cdot \widetilde{F}_i \cdot \widetilde{F}_j$ in the sum above.

- The function $C_i \cdot C_j \cdot C_k$ is an $\mathsf{AC}^0_{d-1}$ circuit of size at most $S$. (Recall that each $C_i$ has an "AND" gate on top.) Therefore, by induction, it is sandwiched between low-degree polynomials.
- The function $c_{i,j,k} \cdot \widetilde{F}_i \cdot \widetilde{F}_j$ is a polynomial of degree at most $\mathrm{polylog}(S) \cdot \log(1/\varepsilon)$, and it takes values in the interval $[-L, L]$ where $L = 2^{\mathrm{polylog}(S) \cdot \log(1/\varepsilon)}$.

We will now prove that the two facts above imply that the term $c_{i,j,k} \cdot C_i \cdot C_j \cdot C_k \cdot \widetilde{F}_i \cdot \widetilde{F}_j$ is sandwiched between low-degree polynomials.

**Lemma 2.** *Let $f \colon \{0,1\}^n \to \mathbb{R}$ and $g \colon \{0,1\}^n \to [-L, L]$. If $f$ has $\delta$-sandwiching polynomials of degree $k$, then $f \cdot g$ has $(3\delta L)$-sandwiching polynomials of degree $k + \deg(g)$.*

*Proof.* Let $f_-, f_+$ be the $\delta$-sandwiching polynomials for $f$. Let $h = f \cdot g$. Our sandwichers are given by

$$\begin{aligned}
h_- &= f_- \cdot g - L \cdot (f_+ - f_-) \\
h_+ &= f_+ \cdot g + L \cdot (f_+ - f_-).
\end{aligned}$$

To prove that this works, observe that

$$\begin{aligned} fg - h_- &= L \cdot (f_+ - f_-) + (f - f_-)g \geq L \cdot (f_+ - f_-) - L \cdot (f - f_-) = L \cdot (f_+ - f) \geq 0 \\ h_+ - fg &= L \cdot (f_+ - f_-) + (f_+ - f)g \geq L \cdot (f_+ - f_-) - L \cdot (f_+ - f) = L \cdot (f - f_-) \geq 0 \\ \mathbb{E}_x[h_+(x) - h_-(x)] &= \mathbb{E}_x[(f_+(x) - f_-(x)) \cdot (g(x) + 2L)] \leq 3L \cdot \mathbb{E}_x[f_+(x) - f_-(x)] = 3L\delta. \end{aligned}$$

□

Consequently, each term $c_{i,j,k} \cdot C_i \cdot C_j \cdot C_k \cdot \widetilde{F}_i \cdot \widetilde{F}_j$ has $(\frac{\varepsilon}{4(m+1)^3})$-sandwichers of degree $\mathrm{polylog}(S) \cdot \log(1/\varepsilon)$. To construct low-degree sandwichers for $C_+$, we use the following trivial lemma.

**Lemma 3.** *Let $f, g\colon \{0,1\}^n \to \mathbb{R}$. If $f$ has $\delta$-sandwiching polynomials of degree at most $k$ and $g$ has $\gamma$-sandwiching polynomials of degree at most $k$, then $f + g$ has $(\delta + \gamma)$-sandwiching polynomials of degree at most $k$.*

*Proof.* The sandwiching polynomials are $f_- + g_-$ and $f_+ + g_+$. □

Thus, $C_+$ is $(\varepsilon/4)$-sandwiched between two polynomials $C_{+-}$ and $C_{++}$ of degree $\mathrm{polylog}(S) \cdot \log(1/\varepsilon)$. Similarly, $C_-$ is $(\varepsilon/4)$-sandwiched between two polynomials $C_{--}$ and $C_{-+}$ of degree $\mathrm{polylog}(S) \cdot \log(1/\varepsilon)$.

### 2.2.3 Finishing the proof

Observe that $C_{--} \leq C \leq C_{++}$ and

$$\begin{aligned} \mathbb{E}[C_{++} - C_{--}] &\leq \mathbb{E}[C_{++} - C_+] + \mathbb{E}[C_+ - C_-] + \mathbb{E}[C_- - C_{--}] \\ &\leq \mathbb{E}[C_{++} - C_{+-}] + \mathbb{E}[C_+ - C_-] + \mathbb{E}[C_{-+} - C_{--}] \\ &\leq \varepsilon/4 + \varepsilon/2 + \varepsilon/4. \end{aligned}$$

## References


[Baz09] Louay M. J. Bazzi. "Polylogarithmic independence can fool DNF formulas". In: *SIAM J. Comput.* 38.6 (2009), pp. 2220–2272. ISSN: 0097-5397. DOI: 10.1137/070691954.

[Bra10] Mark Braverman. "Polylogarithmic independence fools $\mathrm{AC}^0$ circuits". In: *J. ACM* 57.5 (2010), Art. 28, 10. ISSN: 0004-5411. DOI: 10.1145/1754399.1754401.

[HH24] Pooya Hatami and William Hoza. "Paradigms for Unconditional Pseudorandom Generators". In: *Foundations and Trends in Theoretical Computer Science* 16.1-2 (2024), pp. 1–210. ISSN: 1551-305X. DOI: 10.1561/0400000109.

[HS19] Prahladh Harsha and Srikanth Srinivasan. "On polynomial approximations to $\mathrm{AC}^0$". In: *Random Structures Algorithms* 54.2 (2019), pp. 289–303. DOI: 10.1002/rsa.20786.

[Raz09] Alexander Razborov. "A Simple Proof of Bazzi's Theorem". In: *ACM Trans. Comput. Theory* 1.1 (Feb. 2009). ISSN: 1942-3454. DOI: 10.1145/1490270.1490273.

[Tal17] Avishay Tal. "Tight Bounds on the Fourier Spectrum of AC0". In: *Proceedings of the 32nd Computational Complexity Conference (CCC)*. Ed. by Ryan O'Donnell. Vol. 79. 2017, 15:1–15:31. DOI: 10.4230/LIPIcs.CCC.2017.15.