1 Today’s Plan

Last lecture investigated the ability of polynomials to represent circuits, culminating in the following upper bound.

**Theorem 1.1.** For any \(m\)-gate, \(d\)-depth, \(n\)-input circuit \(C \in \text{AC}^0 + \text{mod}_p\), there exists a polynomial \(g \in F_p[x]\) of degree \(\log(m)^{O(d)}\) which agrees with \(C\) on all but \(\leq 2^n/m\) (boolean) inputs.

Today’s lecture continues this study by establishing a lower bound for parity functions. For warm-up, the first consideration is of \(\oplus_2\), meaning standard parity or addition mod 2.

**Theorem 1.2.** Any polynomial \(g \in F_p[x]\) which agrees with \(\oplus_2\) on at least \(3 \cdot 2^n/4\) inputs must have degree \(\Omega(\sqrt{n})\).

The proof proceeds by noticing that parity can be used to obtain, from any polynomial, another polynomial of small degree which agrees with the original on most inputs. A counting argument will then show, combined with Theorem 1.1, that this degree can not be too small.

This proof may be refined to show the analogous result for \(\oplus_q\).

**Theorem 1.3.** Any polynomial \(g \in F_p[x]\) which agrees with \(\oplus_q\) on at least \(3 \cdot 2^n/4\) inputs must have degree \(\Omega(\sqrt{n})\).

Finally, combining Theorem 1.1 and Theorem 1.3 will yield the desired hardness statement for parity.

**Corollary 1.4.** For any primes \(p \neq q\) with \(p \geq 3\) and \(q \geq 2\), any circuit \(g \in \text{AC}^0 + \text{mod}_p\) for \(\oplus_q\) has \(2^{n(1/(2d))}\) gates.

2 Background Material

So far in this class, boolean functions have been taken to have domain \(\{0, 1\}^n\). Today, however, this choice will become problematic, as 0 does not have a multiplicative inverse. The solution will be to “Fourier transform” polynomials over the desired field so that now both values have inverses.

**Definition 2.1.** Define the functional \(\tilde{\cdot}\) on polynomials over a field \(F\) with \(q^{\text{th}}\) root of unity \(\omega_q\) for some prime \(q\) to perform the variable substitution

\[x_i \mapsto (\omega_q - 1)x_i + 1.\]
Similarly, define an inverse transform functional \( \hat{\cdot} \), where
\[
y_i \mapsto y_i - \frac{1}{\omega q - 1}.
\]
Note that \( \hat{f} = f \); lastly, this transform is well-defined, since \( q \) prime means \( \omega q \neq 1 \).

Critically, this transform and its inverse do not increase the degree of a polynomial.

**Lemma 2.2.** For any \( f \in F[x] \), the \( \deg(\hat{f}) \leq \deg(f) \) and \( \deg(\tilde{\cdot}) \leq \deg(f) \).

**Proof.** From the definition of \( \tilde{\cdot} \) and \( \hat{\cdot} \), any variable appearance \( x^n \) is replaced by another expression with terms \( x^m \), where \( m \leq n \). Thus, collecting terms, the degree can not increase. \( \square \)

Another crucial fact about the functions in consideration is that they can be represented as low degree polynomials.

**Lemma 2.3.** Let any finite field \( F \) and element \( a \in F \) be given. Then, every function \( g : F^n \to F \) admits a representation \( h_g \in F[x] \) satisfying \( \deg(h_g) \leq n \) and \( h_g(x) = g(x) \) for every \( x \in \{a, 1\}^n \).

Note that possibly \( h_g(y) \neq g(y) \) when \( y \in F^n \setminus \{a, 1\}^n \).

**Proof.** Dispense with the case that \( a = 1 \), which entails that \( g \) is constant over \( \{a, 1\}^n \) (and \( h_g \) has degree zero). For any \( u, v \in \{a, 1\} \),
\[
\frac{uv + uv - (1 + a)(u + v) + 1 + aa}{(1 - a)(1 - a)} = 1(u = v) = \begin{cases} 1 & \text{when } u = v, \\ 0 & \text{otherwise}. \end{cases}
\]

Furthermore, holding either of \( u \) or \( v \) to be constant, this expression is a polynomial of degree 1 with respect to the other variable (and well defined since \( 1 - a \neq 0 \), it has an inverse in \( F \)). As such,
\[
g(x) = \sum_{y \in \{a, 1\}^n} g(y) \mathbb{1}(x = y) = \sum_{y \in \{a, 1\}^n} g(y) \prod_{i=1}^n \mathbb{1}(x_i = y_i) = \sum_{y \in \{a, 1\}^n} g(y) \prod_{i=1}^n \frac{2x_i y_i - (1 + a)(x_i + y_i) + a^2}{(1 - a)^2},
\]
where “\( 2^n \)” is used for convenience. Collecting terms yields the desired \( h_g \). \( \square \)

Finally, the counting argument of the proofs of Theorem 1.2 and Theorem 1.3 will need the following.

**Lemma 2.4.** For any \( c \geq 0 \) and \( n \geq 1 \),
\[
\sum_{i=0}^{n/2 + \sqrt{n}} \binom{n}{i} \leq 2^n \left( \frac{1}{2} + (c + n^{-1/2}) \sqrt{\frac{2}{\pi}} \right).
\]

**Proof.** To start,
\[
\sum_{i=0}^{n/2 + \sqrt{n}} \binom{n}{i} = \sum_{i=0}^{\lfloor n/2 \rfloor - 1} \binom{n}{i} + \sum_{i=\lfloor n/2 \rfloor}^{n} \binom{n}{i}. \tag{2.5}
\]
To bound the first term, the symmetry \((\binom{n}{i} = \binom{n}{n-i})\) grants
\[
\sum_{i=0}^{[n/2]-1} \left(\binom{n}{i}\right) = \frac{1}{2} \left( \sum_{i=0}^{[n/2]-1} \binom{n}{i} + \sum_{i=0}^{[n/2]-1} \binom{n}{n-i} \right) \leq \frac{1}{2} \sum_{i=0}^{n} \binom{n}{i} = 2^{n-1}.
\]

For the second term of (2.5), first recall Feller’s form of Stirling’s inequality:
\[
\sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{1/(12m+1)} < m! < \sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{1/(12m)}.
\]

Consequently
\[
\binom{n}{2} = \frac{n!}{(n/2)!^2} < \frac{n^n \sqrt{2\pi n}}{((n/2)^{n/2} \sqrt{2\pi (n/2)})^2} \exp\left(\frac{1}{(12n)} - \frac{2}{(6n + 1)}\right) < \frac{e^{n/2}}{\sqrt{2\pi}}.
\]

Therefore the second term of (2.5) may be bounded as
\[
\sum_{i=\lfloor n/2 \rfloor}^{c\sqrt{n}} \binom{n}{i} \leq \left( c\sqrt{n} + 1 \right) \binom{n}{n/2} \leq 2^n (c + 1/\sqrt{n}) \sqrt{2/\pi}.
\]

Combining the bounds on the two terms of (2.5), the result follows. \(\square\)

3 Proof for \(\oplus_2\)

The stage is now set for the warmup case \(\oplus_2\).

**Proof of Theorem 1.2.** Let \(g \in F[x]\) be a polynomial for \(\oplus_2\) which is correct on all but a set of at most \(2^n/4\) inputs, where \(g\) has minimal degree among all polynomials satisfying this constraint. Furthermore, let \(S\) be the set of bad inputs. Lastly, note that for any input \(y \in \{-1,+1\}^n\), \(\oplus_2(y) = \prod_{i=1}^n y_i\).

Now let any (Fourier transformed) Boolean function \(f : \{-1,+1\}^n \to F\) be given; invoking Lemma 2.3 (where \(-1 = \omega_2\)), for any \(x \in \{-1,+1\}^n \setminus S\),
\[
f(x) = \sum_{U \subseteq [n]} \alpha_U \prod_{i \in U} x_i
\]
\[
= \sum_{U \subseteq [n]} \alpha_U \prod_{i \in U} x_i + \sum_{|U| > n/2} \alpha_U \prod_{i \in U} x_i + \left( \prod_{i \in [n]} x_i \right) \left( \prod_{i \in [n]} \right)_{i=1}^y
\]
\[
= \sum_{U \subseteq [n]} \alpha_U \prod_{i \in U} x_i + \tilde{g}(x) \sum_{|U| > n/2} \alpha_U \prod_{i \in U} x_i.
\]

Note that this final expression implies that every \(f\) admits a representation \(h_f\) which is correct on \(\{-1,+1\}^n \setminus S\), has degree at most \(n/2 + \deg(g)\) (by assumption on \(g\)), and is multilinear (since
any quadratic in the second expression can be replaced with 1). And recall by Lemma 2.2 that 
\(\hat{f} : \{0, 1\}^n \to F\) will have at most the same degree.

Now suppose contradictorily that \(\deg(g) \leq \sqrt{n}/4\) for all \(n\). Then the total number of such
representations, by Lemma 2.4 is at most
\[
p^{\sum_{i=0}^{n/2 + \sqrt{n}/4} \binom{n}{i}} \leq p^{2^n (1/2 + (1/4 + 1/\sqrt{n})\sqrt{2}/\pi)}.
\]

On the other hand, the number of functions with domain \([-1, +1]^n \setminus S\) and range \(F_p\) is
\[
p^{2^n - |S|} \geq p^{2^n (3/4)}.
\]

This yields a contradiction (since the representation was exact off \(S\) for every function), thus \(\deg(g) \in \Omega(\sqrt{n})\). The result follows since \(\deg(g)\) was minimal. \(\square\)

4 Proof for \(\oplus_q\)

**Proof of Theorem 1.3.** Similarly to before, let \(g \in F[x]\) be a polynomial for \(\oplus_q\) which is correct on all but a set of at most \(2^{n/4}\) inputs, where \(g\) has minimal degree among all polynomials satisfying this constraint. Again, let \(S\) be the set of bad inputs.

For this proof, the Fourier representation will be over the extension field \(F_p(\omega_q)\); correspondingly, for any input \(y \in \{\omega_q, 1\}^n\), \(\oplus_q(y) = \prod_{i=1}^n y_i\).

Now let any \(f : F_p(\omega_q)^n \to F_p(\omega_q)\) be given; making use of Lemma 2.3 applied to \(\{\omega_q, 1\}\), for any \(x \in \{\omega_q, 1\}^n \setminus S\),
 \[
f(x) = \sum_{U \subseteq [n]} \alpha_U \prod_{i \in U} x_i
\]
 \[
= \sum_{|U| \leq n/2} \alpha_U \prod_{i \in U} x_i + \sum_{|U| > n/2} \alpha_U \prod_{i \in U} \left(\prod_{i \in [n]} x_i^{q^{-1}}\right) = 1 \left(\prod_{i \in [n]} x_i^{q^{-1}}\right)
\]
 \[
= \sum_{|U| \subseteq [n]} \alpha_U \prod_{i \in U} x_i + g(x) \sum_{|U| \subseteq [n]} \alpha_U \prod_{i \in U} x_i^{q^{-1}}.
\]

Applying Lemma 2.3 to the last product (separately for each \(U\)), it follows again that this expression is a polynomial with degree at most \(n/2 + \deg(g)\). The rest of the proof follows as before, with the exception that the base of the exponents is \(|F_p(\omega_q)|\) rather than \(p\). \(\square\)

5 Proof of Parity Circuit Hugeness

**Proof of Corollary 1.4.** By Theorem 1.1, parity has an approximate polynomial of degree \(\log(m)^{O(d)}\), and by Theorem 1.2, this degree is \(\Omega(\sqrt{n})\). As such,
\[
\log(m)^{O(d)} \geq \Omega(\sqrt{n})
\]
\[
\implies m \geq 2^{n^{O(1/2d)}}. \square
\]