Notes for Lecture 15

We continue our proof of the Impagliazzo-Wigderson Theorem [1] stated in Lecture 12. As was discussed there, our proof of the theorem requires sublinear-time list-decoding of error-correcting codes. In today's lecture, we give such a scheme for Reed-Muller codes. This is based on results of [2].

1 Notations and Previous Results

Recall that $\mathbb{F}$ is a field with q elements. We consider a subset H of $\mathbb{F}$ of size h. A Reed-Muller code maps messages in $\mathbb{F}^{h^m}$ to codewords in $\mathbb{F}^{q^m}$ for some m. It will be convenient to think of the message as a function from H^m to $\mathbb{F}$. In a Reed-Muller code, the message is interpreted as the values taken by a multivariate polynomial on the subset H^m of $\mathbb{F}^m$. The codeword corresponds to the values of the polynomial at all points in $\mathbb{F}^m$. We denote M the message and p the encoding. The "corrupted" codeword is denoted f.

We first recall two results from previous lectures.

Proposition 1 *Assume the function $f : \mathbb{F}^m \to \mathbb{F}$ is $\frac{1}{10}$-close to a multivariate polynomial $p : \mathbb{F}^m \to \mathbb{F}$ of degree hm with $q > 5hm$. Given $x \in \mathbb{F}^m$, we can compute $p(x)$ w.h.p. in time* $\text{poly}(|\mathbb{F}|, hm)$.

Proposition 2 *Let $g : \mathbb{F} \to \mathbb{F}$ and $a > 2\sqrt{(d+1)|\mathbb{F}|}$ for some d. Then, we can find a list of all polynomials of degree d that agree with g on at least a points in time* $\text{poly}(|\mathbb{F}|)$. *Moreover, the list has size at most $\frac{a}{2d}$.*

2 Toy Problem

We begin with a toy problem.

- Setup:
  - $p : \mathbb{F}^m \to \mathbb{F}$ polynomial of degree hm
  - $f : \mathbb{F}^m \to \mathbb{F}$ function agreeing with p on ε fraction of inputs
- Given:
  - x, y uniformly random in $\mathbb{F}^m$
  - the value of $p(y)$
  - oracle access to f
- Goal: compute $p(x)$.

The following algorithm is a natural candidate solution to this problem. Consider the line $l(t) = ty+(1-t)x$ for $t \in \mathbb{F}$. It contains $|\mathbb{F}|$ points with $l(0) = x$ and $l(1) = y$. Consider the restrictions of p and f to this line, that is $p_0(t) = p(l(t))$ and $f_0 = f(l(t))$. Apply Sudan's algorithm (Proposition 2) to f_0 with $d = hm$ and $a = \frac{\varepsilon|\mathbb{F}|}{2}$. The list returned has size $\frac{\varepsilon|\mathbb{F}|}{4hm}$. If there is a unique polynomial r in the list with $r(1) = p(y)$ then output $r(0)$, otherwise output FAIL.

We make two claims.

Claim 3 *Assume $|\mathbb{F}| > \frac{20}{\varepsilon^2}$. Then, with probability at least $19/20$ over the choice of x, y, p_0 and f_0 agree on at least $\frac{\varepsilon|\mathbb{F}|}{2}$ points (and, in particular, p_0 appears in the list output by our algorithm).*

PROOF: Because x, y are chosen independently uniformly at random in $\mathbb{F}^m$, the points on the line $\{l(t) : t \in \mathbb{F}\}$ are pairwise independent. For $t \in \mathbb{F}$, define

$$Z_t = \begin{cases} 1, & \text{if } p_0(t) = f_0(t), \\ 0, & \text{o.w.} \end{cases}$$

We have $\mathbb{E}[Z_t] \geq \varepsilon$ because p and f have ε agreement. Let $\mu = \mathbb{E}[\sum_t Z_t]$ and $\mathcal{E}$ be the event

$$\mathcal{E} = \left\{ f_0 \text{ and } p_0 \text{ agree on less than } \frac{\varepsilon|\mathbb{F}|}{2} \text{ points} \right\}.$$

By Chebyshev's inequality,

$$\mathbb{P}[\mathcal{E}] \leq \mathbb{P}\left[\left|\sum_t Z_t - \mu\right| > \frac{\varepsilon|\mathbb{F}|}{2}\right] \leq \frac{4\mathrm{Var}\left[\sum_t Z_t\right]}{\varepsilon^2|\mathbb{F}|^2} \leq \frac{4\sum_t \mathrm{Var}\left[Z_t\right]}{\varepsilon^2|\mathbb{F}|^2} \leq \frac{1}{\varepsilon^2|\mathbb{F}|} \leq \frac{1}{20},$$

where we have used the pairwise independence of the Z_t's to permute Var and $\sum$, and the fact that the variance of a $0-1$ variable is at most $\frac{1}{4}$. □

Claim 4 *Assume $|\mathbb{F}| > \frac{16hm}{\varepsilon^2}$. Then, with probability at least $\frac{19}{20}$, p_0 is the unique polynomial in the list with value $p(y)$ at $t = 1$ (for ε small enough).*

PROOF: We think of x and y as being picked according to the following process. We first pick a random line, that is we choose z, w independently uniformly at random and consider the line $l'(t) = tz + (1-t)w$. We then choose two different uniform points on l', that is we choose t_1, t_2 uniformly without replacement in $\mathbb{F}$ and let $x = t_1 z + (1-t_1)w$ and $y = t_2 z + (1-t_2)w$.

By assumption, $a = \frac{\varepsilon|\mathbb{F}|}{2} > 2\sqrt{|\mathbb{F}|hm}$ so that Sudan's algorithm can be used. By Proposition 2, there are at most $\frac{\varepsilon|\mathbb{F}|}{4hm}$ polynomials of degree at most hm agreeing with f restricted to l' on at least $\frac{\varepsilon|\mathbb{F}|}{2}$ points. Two such polynomials agree on at most $\frac{hm}{|\mathbb{F}|}$ fraction of $\mathbb{F}$ (number of roots of difference). Assume r is a polynomial not equal to p'_0, the restriction of p to l' (in particular $p'_0(t_2) = p(y)$). Then

$$\mathbb{P}[r(t_2) = p(y)] \leq \frac{hm}{|\mathbb{F}|},$$

because y is uniformly random on the line. Therefore,

$$\mathbb{P}[\exists r \neq p_0' \text{ in the list s.t. } r(t_2) = p(y)] \leq \frac{\varepsilon|\mathbb{F}|}{4hm}\frac{hm}{|\mathbb{F}|} \leq \frac{\varepsilon}{4} \leq \frac{1}{20},$$

if ε is small enough.

Notice finally that even though we applied Sudan's algorithm to f restricted to l' rather than l, there is a one-to-one linear map between polynomials such that agreement with f on l corresponds to agreement with f on l'. This concludes the proof.

□

We have proved the following.

Proposition 5 *Consider the setup of the Toy Problem with*

$$|\mathbb{F}| > \max\left\{\frac{20}{\varepsilon^2}, \frac{16hm}{\varepsilon^2}\right\}.$$

Then for ε small enough, we can compute $p(x)$ with probability at least $\frac{9}{10}$.

3 Main Result

Given x, y the algorithm above is deterministic. Let $A_{y,p(y)}(x)$ be the output of the algorithm on inputs $x, y, p(y)$. Then we know from Proposition 5 that

$$\mathbb{P}_{x,y}[A_{y,p(y)}(x) = p(x)] \geq \frac{9}{10}.$$

Therefore, there exists a y such that

$$\mathbb{P}_{x}[A_{y,p(y)}(x) = p(x)] \geq \frac{9}{10}.$$

Fix that y. From Proposition 2, it follows that if f has a circuit of size S then $A_{y,p(y)}$ has a circuit of size $S|\mathbb{F}| + \text{poly}(|\mathbb{F}|)$. Now, apply the algorithm of Proposition 1 to $A_{y,p(y)}$. We get the following result.

Theorem 6 *Let $p : \mathbb{F}^m \to \mathbb{F}$ be a polynomial of degree hm and $f : \mathbb{F}^m \to \mathbb{F}$ a function agreeing with p on an ε fraction of inputs in $\mathbb{F}^m$. Assume furthermore that*

$$|\mathbb{F}| > \max\left\{\frac{20}{\varepsilon^2}, \frac{16hm}{\varepsilon^2}\right\}.$$

If f can be computed by a circuit of size S, then p can be computed by a circuit of size $S\text{poly}(|\mathbb{F}|, hm)$ (a more careful analysis gives $S|\mathbb{F}|\text{poly}(\log|\mathbb{F}|, hm) + \text{poly}(|\mathbb{F}|)$).

4 Back to the Impagliazzo-Wigderson Theorem

We conclude with a discussion of the relevance of Theorem 6 to our (ongoing) proof of the Impagliazzo-Wigderson theorem which we will complete in the next lecture.

Suppose L is a decision problem solvable in time $2^{O(n)}$ that cannot be solved by circuits of size $2^{\delta n}$ on inputs of length n for some $\delta > 0$. Denote $L_n : \{0,1\}^n \to \{0,1\}$ the restriction of L to inputs of size n. Fix $\gamma (= \Omega(\delta))$. Using the notation of the previous sections, take $h = 2^{\gamma n}$, $m = \frac{1}{\gamma}$, $\varepsilon = \frac{1}{2^{\gamma n}}$. From previous results, we need to take $q = 16 \cdot 2^{2\gamma n} \cdot 2^{\gamma n} = 2^{3\gamma n+4}$. We think of H as $\{0,1\}^{\gamma n}$ and L_n as a function from H^m to $\{0,1\}$. Let $p : \mathbb{F}^m \to \mathbb{F}$ a degree hm polynomial that agrees with L_n on H^m. We think of p as a function from $\{0,1\}^{3n+4/\gamma}$ to $\{0,1\}^{3\gamma n+4}$. By a standard interpolation formula, p is computable in time $2^{O(n)}$. From Theorem 6, if there exists a circuit of size S that computes p on a fraction $\varepsilon = \frac{1}{2^{\gamma n}}$ of inputs, then there exists a circuit of size $S2^{\gamma nc}$ for some $c > 0$ that computes p everywhere. In particular, it computes L_n everywhere. This gives a contradiction if γ is such that $S2^{\gamma nc} < 2^{\delta n}$. Therefore, we have constructed a function with exponential average-case complexity.

What we really need is a *decision* problem with exponential average-case complexity. We will construct such a problem in the next lecture.

References

[1] R. Impagliazzo and A. Wigderson. $P = BPP$ unless E has sub-exponential circuits. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, pages 220–229, 1997.

[2] M. Sudan, L. Trevisan, and S. Vadhan. Pseudorandom generators without the XOR lemma. *Journal of Computer and System Sciences*, 62(2):236–266, 2001.