CSE599s: Extremal Combinatorics November 9, 2011

Lecture 12 Construction by Polynomial, and Pseudorandomness

Lecturer: Anup Rao

1 Constructions Based on Polynomials

We continue our tour of combinatorial constructions based on polynomials. Recall:

Fact 1. *Given any $d+1$ points, evaluating univariate degree d polynomials on those points defines a linear bijection between the coefficients of the polynomial and the evaluations.*

1.1 Error Correcting Codes

Goal: An encoding $E : \{0,1\}^n \to \{0,1\}^{O(n)}$ such that for $x \neq y$, $E(x)$ disagrees with $E(y)$ in many coordinates.

The Reed-Solomon code $E : \mathbb{F}^k \to \mathbb{F}^n$ is defined as follows. Interpret each message as a degree k polynomial $p(X)$, and define

$$E(p(X)) = E(\alpha_1), \ldots, E(\alpha_n),$$

for distinct field elements $\alpha_1, \ldots, \alpha_n$. Two distinct polynomials $p(X), q(X)$ can agree on at most k points by Fact 1, so they must disagree on $n-k$ points. This bound is in fact tight (Singleton Bound), since if the encoding ensured that every two inputs disagreed on $n-k+1$ points, the map from $\mathbb{F}^k$ into the first $k-1$ coordinates would be injective, which is a contradiction.

If we naively translate everything to bits, we do not obtain a code with great distance. The right way is to recursively encode each field element using a smaller code. Let's leave it at that.

1.2 ϵ-biased Sets

Goal: A small set $S \subset \mathbb{F}_2^n$ such that for every non-empty set $T \subseteq [n]$, if x is a uniformly random element from S, $\sum_{i \in T} x_i$ is ϵ-close to uniform.

We show a construction due to Alon, Goldreich, Hastad and Peralta. Let $\mathbb{F}$ be a field of size $2^t \geq n/\epsilon$. Every element of the set is indexed by $a, b \in \mathbb{F}$. First consider the vector

$$x = (a, ab, ab^2, \ldots, ab^{n-1}) \in \mathbb{F}^n$$

Then for any non-empty set $T \subset [n]$, $\sum_{i \in T} x_i = \sum_{i \in T} ab^{i-1} = a \sum_{i \in T} b^{i-1} = a \cdot p_T(b)$, where here p_T is the polynomial defined by T. This polynomial has degree at most $n-1$, so the probability that $p_T(b) = 0$ is at most $\frac{n-1}{n/\epsilon} < \epsilon$. Whenever it is not 0, $x \cdot p_T(b)$ is uniformly distributed. Thus we get a field element that is uniformly distributed except for ϵ fraction of the time.

This did not yet give us a distribution on $\mathbb{F}_2^n$, but we can easily fix that. Note that every element of $\mathbb{F}$ can be viewed as a degree $(t-1)$ polynomial in $\mathbb{F}[X]/p(X)$, for some irreducible polynomial p

of degree t. Further, adding two field elements is exactly like adding two polynomials (namely, the addition is coordinate-wise). Let us write y^0 to denote the constant bit of the field element y. We use just the constant terms of the above sequence:

$$x = (a^0, (ab)^0, \ldots, (ab^{n-1})^0) \in \mathbb{F}_2^n$$

Then for any non-empty set $T \subset [n]$, $\sum_{i \in T} x_i = \sum_{i \in T} (ab^{i-1})^0 = \left(\sum_{i \in T} ab^{i-1}\right)^0 = (a \cdot p_T(b))^0$, where here p_T is polynomial defined by T. Again, whenever $p_T(b) \neq 0$, $(a \cdot p_T(b))^0$ is uniformly distributed.

1.3 Sets with Small pairwise Intersection

Recall that if we have a r-uniform family of sets $\mathcal{F}$ with pairwise intersection at most k, then:

Lemma 2 (Corradi). *If $r^2 > kn$, $|\mathcal{F}| \leq \frac{rn-kn}{r^2-kn}$.*

In other words, if $r^2 > kn$, there can be at most poly(n) sets. Now we show how to get exponentially many sets of smaller size.

Take a finite field $\mathbb{F}$ of size $\sqrt{n}$. Our universe will be $\mathbb{F} \times \mathbb{F}$. Consider all degree k polynomials in $\mathbb{F}[X]$. There are $(k+1)^{\sqrt{n}}$ such polynomials, and for each such polynomial $p(X)$ we obtain a set $S_p = \{(\alpha, p(\alpha) : \alpha \in \mathbb{F})\}$ of size $r = \sqrt{n}$. By Fact 1, any two sets can intersect in at most k points.

2 Randomness from Hardness

In this section, we shall describe a pivotal construction of Nisan and Wigderson, that led to theorems that can be paraphrased as: "A function that cannot be computed by small circuits can be used to generate small support distributions that look random to small circuits".

A more concrete consequence of these results is the following theorem (which is a special case of a theorem by Impagliazzo and Wigderson that builds on the work of Nisan and Wigderson):

Theorem 3. *Either there are circuits of size $2^{n/10000}$ that can compute SAT, or every randomized polynomial time algorithm can be simulated by a deterministic polynomial time algorithm.*

In the above theorem, SAT can actually be replaced by any exp computable function. We shall need the concept of a *pseudorandom generator*. Let u_ℓ denote a uniformly random element of $\{0,1\}^\ell$.

Definition 4. *$G : \{0,1\}^\ell \to \{0,1\}^n$ is an ϵ-pseudorandom generator for circuits of size s, if for any circuit C of size s, $\Pr[C(G(u_\ell)) = 1] - \Pr[C(u_n) = 1] \leq \epsilon$.*

Observe that if we have such a pseudorandom generator,

$$|\Pr[C(G(u_\ell)) = 1] - \Pr[C(u_n) = 1]| \leq \epsilon$$

for circuits of size $s-1$, since one can always flip the output bit of the circuit with a single not gate. If $\ell = n$, then the identity function is a pseudorandom generator. Pseudorandom generators are interesting when $n \gg \ell$, since in this case, the generator must be using some facts about circuits, since its output is actually very far from uniformly distributed (in particular it is supported on only 2^ℓ elements).

2.1 Obtaining One Pseudorandom Bit

Let $f : \{0,1\}^t \to \{0,1\}$ be a function that is so hard, that for every circuit C of size s,

$$\Pr_x[f(y) = C(y)] \leq \epsilon.$$

We can use f to come up with a non-trivial pseudorandom generator as in the following claim.

Claim 5. *$G(x) = (x, f(x))$ is $\epsilon/4$-pseudorandom for circuits of size $s-1$.*

Proof Suppose C is a circuit such that $\Pr[C(x, f(x)) = 1] - \Pr[C(x,u) = 1] > \epsilon$. This means that $\mathbb{E}_x\left[\Pr_u[C(x,f(x)) = 1] - \Pr_u[C(x,u) = 1]\right] > \epsilon/4$. Say that C is *correct* on x if $C(x, f(x)) = 1$ and $C(x, 1-f(x)) = 0$, and that C is *wrong* on x if $C(x, f(x)) = 0$ and $C(x, 1-f(x)) = 1$. Then,

$$\Pr_u[C(x,f(x)) = 1] - \Pr_u[C(x,u) = 1] = \begin{cases} 1/2 & \text{if } C \text{ is correct on } x \\ -1/2 & \text{if } C \text{ is wrong on } x \\ 0 & \text{else.} \end{cases}$$

Thus,

$$\left(\Pr_x[C \text{ is correct on } x] - \Pr_x[C \text{ is wrong on } x]\right) > 2\epsilon/4 = \epsilon/2.$$

Now construct a circuit for computing f as follows. Consider the circuit C' that takes in x and a random bit u and computes:

$$C'(x,u) = \begin{cases} u & C(x,u) = 1 \\ 1-u & C(x,u) = 0 \end{cases}$$

If C is correct on x, then $C'(x,u) = f(x)$. If C is wrong on x, then $C'(x,u) \neq f(x)$. Otherwise, $C'(x,u) = f(x)$ with probability $1/2$. In total, we get that $\Pr_{x,u}[C'(x,u) = f(x)] > 1/2 + \epsilon$. By averaging there must be some fixing of u that gives a deterministic circuit of the same size with the same advantage in computing f. This contradicts the hardness of f. ■

2.2 Obtaining Many Bits

However, this only gave us one extra bit. In order to obtain many (exponential in ℓ) number of bits, we use our construction of sets with small intersection.

Suppose we have m sets $S_1, \ldots, S_m \subseteq [\ell]$, each of size t, with pairwise intersections k. For $x \in \{0,1\}^\ell$, let x_{S_i} denote x projected on the coordinates of S_i. The construction is to output

$$\mathsf{NW}(x) = (f(x_{S_1}), f(x_{S_2}), \ldots, f(x_{S_n})).$$

Theorem 6. *$\mathsf{NW}(x)$ is $\epsilon n/4$ pseudorandom for circuits of size $s - 2^k n$.*

In order to prove this, let C be a circuit that contradicts the theorem. We will consider the behavior of C on $n+1$ different distributions. Define the distribution

$$A_i = (f(x_{S_1}), f(x_{S_2}), \ldots, f(x_{S_i}), u_{n-i}),$$

for a random x. In other words, A_i is distributed like the output $\mathsf{NW}(x)$ in the first i coordinates, and has uniformly random and independent bits in the remaining coordinates. Note that $A_n = \mathsf{NW}(x)$, and $A_0 = u_n$. Then we have that

$$\begin{aligned}\epsilon n/4 < (\Pr[C(A_n) = 1] - \Pr[C(A_0) = 1]) = &\Pr[C(A_n) = 1] - \Pr[C(A_{n-1}) = 1] \\ &+ \Pr[C(A_{n-1}) = 1] - \Pr[C(A_{n-2}) = 1] \\ &\vdots \\ &+ \Pr[C(A_1) = 1] - \Pr[C(A_0) = 1]\end{aligned}$$

By averaging, we get

Claim 7. *There exists i such that* $\Pr[C(A_i) = 1] - \Pr[C(A_{i-1}) = 1] > \epsilon/4$.

Let $x_{S_i^c}$ denote x projected on the complement of the set S_i. By averaging, there must be some fixing of the bits in $x_{S_i^c}$ and the uniform bits in the last $n - i + 1$ coordinates such that $\Pr[C(A_i) = 1] - \Pr[C(A_{i-1}) = 1]$. Henceforth fix these bits so that this difference is maximized. The net effect is that we obtain a circuit T of size at most the size of C such that

$$\Pr[T(f(x_{S_1}), \ldots, f(x_{S_i})) = 1] - \Pr[T(f(x_{S_1}), \ldots, f(x_{S_{i-1}}), u) = 1] > \epsilon/4.$$

As in the proof of Claim 5, say that T is *correct* on x_{S_i} if

$$T(f(x_{S_1}), \ldots, f(x_{S_i})) = 1 \text{ and } T(f(x_{S_1}), \ldots, 1 - f(x_{S_i})) = 0,$$

and say that T is *wrong* if

$$T(f(x_{S_1}), \ldots, f(x_{S_i})) = 0 \text{ and } T(f(x_{S_1}), \ldots, 1 - f(x_{S_i})) = 1.$$

Just like in Claim 5, we get that

$$\Pr_{x_{S_i}}[T \text{ is correct on } x_{S_i}] - \Pr_{x_{S_i}}[T \text{ is wrong on } x_{S_i}] > \epsilon/2.$$

As in Claim 5, we define

$$T'(x_{S_i}, u) = \begin{cases} u & T(f(x_{S_1}), \ldots, f(x_{S_{i-1}}), u) = 1 \\ 1 - u & T(f(x_{S_1}), \ldots, f(x_{S_{i-1}}), u) = 0 \end{cases}$$

Then $\Pr[T'(x_{S_i}, u) = f(x_{S_i})] \geq 1/2 + \epsilon$, so there is some fixing of u that gives a function computing f. However, this is not yet a contradiction, since we have not yet shown that T' is computable by a small circuit. The key insight is that since $|S_i \cup S_j| \leq k$, each of the functions $f(x_{S_j})$ actually only depend on k bits of S_i. Any function on k bits can be computed by a circuit of size 2^k. Thus we obtain a circuit that computes T' of size at most $s - n2^k + n2^k = s$. This is a contradiction.

The explicit construction of sets with small pairwise intersection using polynomials allows us to set $t = 100 \log n$, $k = \log n$. Then we obtain a generator that has an input size of $t^2 = 10^4 \log^2 n$ that generates $n < t^k$ bits that cannot be distinguished from uniform by any circuit of size $n^{100} - n^2$. By being more careful in the above analysis, one can obtain n bits that fool circuits of size n using only $\log n$ truly random bits as input.