CS 6815: Pseudorandomness and Combinatorial Constructions **Fall 2022**

Lecture 11: September 27, 2022

Lecturer: Eshan Chattopadhyay *Scribe: Atul Ganju*

1 Balanced Codes

Recall the definition of an ϵ-biased space:

Definition 1.1 (ϵ-biased space)**.** *An ϵ-biased space, or ϵ-biased distribution, is a flat distribution D over some subset of $\mathbb{F}_2^n$ such that for all $S \subseteq [n]$:*

$$\left| \Pr_{x \sim U_n}[\chi_S(x) = 1] - \Pr_{x \sim D}[\chi_S(x) = 1] \right| \leq \epsilon.$$

similarly, an ϵ-balanced code can be defined as:

Definition 1.2 (ϵ-balanced code)**.** *An ϵ-balanced code, is an $(n, k, d)_2$ code C such that for all nonzero code words $c \in C$:*

$$\left(\frac{1}{2} - \epsilon\right) \cdot n \leq \text{weight}(c) \leq \left(\frac{1}{2} + \epsilon\right) \cdot n.$$

Observe that if a balanced code is linear, then its distance $d \geq (\frac{1}{2} - \epsilon) \cdot n$ since the distance of a linear code is the minimum hamming weight of a code word. We will now show that ϵ-biased sets are just ϵ-biased codes in a different guise.

Theorem 1.3. *If D is an ϵ-biased distribution over $\mathbb{F}_2^k$ with support size n, then the $n \times k$ matrix G that has the elements of the support of D written as its rows is a generator matrix for an ϵ-balanced code.*

Proof. Take the matrix G as defined above. By the definition of an ϵ-biased distribution, for any $S \subseteq [k]$, we have:

$$\left| \Pr_{x \sim U_k}[\chi_S(x) = 1] - \Pr_{x \sim D}[\chi_S(x) = 1] \right| \leq \epsilon.$$

Therefore, for any $y \in \mathbb{F}_2^k$ such that $y \neq 0$, if we take $T = \{i : y_i = 1\}$ and $z = Gy$ then we can conclude:

$$\text{weight}(z) = \sum_{i=1}^{n} \Pr[z_i = 1] = \sum_{x \in \text{supp}(D)} \Pr[\chi_T(x) = 1] \in \left[\left(\frac{1}{2} - \epsilon\right) \cdot n, \left(\frac{1}{2} + \epsilon\right) \cdot n \right],$$

since the sum of n terms each bounded between $\left[\frac{1}{2} - \epsilon, \frac{1}{2} + \epsilon\right]$ is going to be bounded in the range $[(\frac{1}{2} - \epsilon) \cdot n, (\frac{1}{2} + \epsilon) \cdot n]$. □

If we take $n = \frac{k^2}{\epsilon^2}$, then we can obtain an $(\frac{k^2}{\epsilon^2}, k, \frac{k^2}{\epsilon^2}(\frac{1}{2} - \epsilon)]$ code with $rate = \frac{k}{n} = \frac{\epsilon^2}{k}$. The reverse is also true:

Theorem 1.4. *Take an ϵ-balanced (n, k, d) code with generator matrix G. The rows of the generator matrix are the support of an ϵ-biased distribution D on $\mathbb{F}_2^k$.*

Proof. Since we defined the support of our ϵ-biased distribution D to be the rows of G, we know that for any set $S \in [k]$ such that $S \neq \emptyset$, if we define the vector $v \in \mathbb{F}_2^k$ such that $v_j = 1 \iff j \in S$, we have:

$$\Pr_{x \sim D}[\chi_S(x) = 1] = \frac{1}{|\text{supp}(D)|} \sum_{x \in \text{supp}(D)} \mathbf{1}\{\chi_S(x) = 1\} = \frac{\text{weight}(Gv)}{|\text{supp}(D)|} \in \left[\left(\frac{1}{2} - \epsilon\right), \left(\frac{1}{2} + \epsilon\right)\right],$$

since the weight of any code word in an ϵ-balanced code is in the range $[(\frac{1}{2} - \epsilon) \cdot n, (\frac{1}{2} + \epsilon) \cdot n]$. □

2 Derandomization

A very central question in complexity theory is the overhead of derandomization— i.e. what is the trade-off between time and space v.s. randomness? There are two main approaches we use to try and answer these questions. The first is making reasonable assumptions about circuit lower bounds and using them to design algorithms, and in particular, to give deterministic analogs of randomized algorithms. The second, which is more interesting to the author, is constructing PRGs for interesting classes of boolean functions (such as threshold functions, small-depth circuits, formulas, and polynomials).

2.1 Hardness v.s. Randomness

A very important question in derandomization is $\mathbf{BPP} \stackrel{?}{=} \mathbf{P}$ — i.e. can we derandomize all randomized polynomial time algorithms in polynomial time? To make progress in answering this question, we define some concepts:

Definition 2.1 (correlation)**.** *Take two functions $f, g : \{0,1\}^n \to \{0,1\}$. Then the correlation between f and g is defined as:*

$$corr(f, g) = \mathop{\mathbb{E}}_{x \sim U_n}\left[(-1)^{f(x)+g(x)}\right],$$

or equivalently,

$$corr(f, g) = \Pr_{x \sim U_n}[f(x) = g(x)] - \Pr_{x \sim U_n}[f(x) \neq g(x)].$$

Definition 2.2 (hardness against a function class)**.** *A function $g : \{0,1\}^n \to \{0,1\}$ is average case ϵ-hard against a function class $\mathcal{F}$ if for all $f \in \mathcal{F}$ we have:*

$$|corr(f, g)| \leq \epsilon$$

or equivalently,

$$\Pr_{x \sim U_n}[g(x) = f(x)] \leq \frac{1}{2} + \epsilon.$$

Definition 2.3 (hardness against circuits)**.** *A function $g : \{0,1\}^n \to \{0,1\}$ is average case (S, ϵ)-hard against circuits if for all circuits C of size at most S:*

$$corr(g, C) \leq \epsilon$$

or equivalently,

$$\Pr_{x \sim U_n}[g(x) = C(x)] \leq \frac{1}{2} + \epsilon.$$

Definition 2.4 (pseudorandomness against circuits)**.** *A distribution D on $\{0,1\}^n$ is (S, ϵ)-pseudorandom against circuits if for all circuits C of size at most S:*

$$\left| \Pr_{x \sim U_n}[C(x) = 1] - \Pr_{x \sim D}[C(x) = 1] \right| \leq \epsilon.$$

In the next lecture, we will see how we can connect these concepts and eventually show why there is great evidence that in fact $\mathbf{BPP} = \mathbf{P}$.