CS395T Pseudorandomness and Combinatorial Constructions
Lecture 6, February 1, 2001
Lecturer: Prof. David Zuckerman, Scribe: K. J. Balakrishnan

1 Constructing Finite Fields

We used finite fields in constucting k-wise independent probability spaces. The integers modulo a prime p form a field. Constructing a field of size 2^r requires some work. We construct this using polynomials. Note that all fields of the same size are isomorphic.

1.1 Constructing a field of size 2^r, $\mathbb{F}_{2^r}$

Proposition 1 *Let f be an irreducible polynomial of degree r over $\mathbb{F}_2$. Then the set of polynomials over $\mathbb{F}_2$ modulo f gives the field:*
$\mathbb{F}_2[X]/(f) \cong \mathbb{F}_{2^r}$

Example: $f(X) = X^2 + X + 1$ is irreducible over $\mathbb{F}_2$ since 0 and 1 are not roots and f has degree 2. Hence $\mathbb{F}_4 \cong \{0, 1, X, X+1\}$
Note: If f is reducible, then there are two non-zero factors whose product is zero. So $\mathbb{F}_2[X]/f$ is not a field.

Proposition 2 *Roughly a $\frac{1}{r}$ fraction of degree r polynomials are irreducible.*

Hence we can pick one at random in polynomial time and test for irreducibility. Usually it is better to use the following.

Proposition 3 *(Exercise 3.96 of Lidl-Niederreiter) $X^{2n} + X^n + 1$ is irreducible over $\mathbb{F}_2$ iff $n = 3^k$ for integer $k \geq 0$.*

2 Almost k-wise independence

In this section, assume that random variables $\in \{0,1\}$. Recall that $X_1, X_2, X_3 ... X_n$ are k-wise independent if

$$\forall i_1 < i_2 < ... < i_k, \alpha \in [0,1]^k$$
$$\Pr[X_{i_1} X_{i_2} X_{i_3} ... X_{i_k} = \alpha] = 2^{-k}$$

We now define ϵ-close to k-wise independence:

Definition 1 *Random variables $X_{i_k} \in \{0,1\}$ are ϵ-close to k-wise independence in* **max norm** *if*

$$\forall i_1 < i_2 < ... < i_k, \alpha \in \{0,1\}^k$$
$$|\Pr[X_{i_1} X_{i_2} X_{i_3} ... X_{i_k} = \alpha] - 2^{-k}| \leq \epsilon$$

Definition 2 *They are ϵ-close to k-wise independence in L_1* **norm** *if*

$$\forall i_1 < i_2 < ... < i_k, \alpha \in \{0,1\}^k$$
$$\sum_{\alpha \in \{0,1\}^k} |\Pr[X_{i_1} X_{i_2} X_{i_3} ... X_{i_k} = \alpha] - 2^{-k}| \leq \epsilon$$

Therefore, ϵ-close to k-wise independence in L_1 norm $\Rightarrow$ ϵ-close to k-wise independence in max norm and ϵ-close to k-wise independence in max norm $\Rightarrow$ $2^k\epsilon$-close to k-wise independence in L_1 norm.

Let us look at parameters for which we can construct polynomial size sample spaces. For k-wise independence, $k = O(1)$. But for ϵ-close to k-wise independence in L_1 norm, $k = O(\log n)$, $\epsilon = \frac{1}{poly(n)}$. And for ϵ-close to k-wise independence in max norm, k can be anything while $\epsilon = \frac{1}{poly(n)}$.

2.1 Application: Testing Circuits

Assuming each component depends upon $\leq k = O(\log n)$ inputs, we want to construct a set of vectors $\in \{0,1\}^n$ such that for any k indices, all 2^k possible values are represented.

We have $\binom{n}{k} = n^{\Theta(k)}$ conditions. We can construct such a set of vectors by choosing the whole sample space of almost k-wise independent sets whose max norm is less than 2^{-k}, since then every possibility will have a non-zero probability. For $k = O(\log n)$, we can construct a polynomial size sample space.

2.2 ϵ-biased sample spaces

In order to construct almost k-wise independent random variables, we construct ϵ-biased random variables. Let $X_1, X_2 ... X_n$ be random variables. Let S be any subset of [n] i.e. $S \subseteq \{1, 2, 3 ... n\}$. We define the bias of a set S as follows :

Definition 3 $b_S = \Pr[\oplus_{i\in S} X_i = 0] - \Pr[\oplus_{i \in S} X_i = 1] = 2(\Pr[\oplus_{i\in S} X_i = 0] - 1/2)$

Definition 4 *ϵ-biased space :* $(\forall S \neq \phi)$, $|b_S| \leq \epsilon$

Proposition 4 *Suppose* $(\forall S \neq \phi)$, $b_S = 0$. *Then* $X_1, X_2 ... X_n$ *is uniform over* $\{0,1\}^n$.

Proof: For $\alpha \in \{0,1\}^n$, let $p_\alpha = \Pr[X = \alpha]$. Here X denotes $X_1X_2X_3...X_n$. We can represent the bias for each S $\subseteq$ of [n] as a matrix times p_α:

$$\begin{pmatrix} b_\phi \\ b_{\{1\}} \\ \vdots \\ b_{[n]} \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 & 1 & \dots & 1 \\ 1 & \dots & 1 & -1 & \dots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} p_{0^n} \\ \vdots \\ p_{01^{n-1}} \\ p_{10^{n-1}} \\ \vdots \\ p_{1^n} \end{pmatrix}$$

or $\vec{b} = H\vec{p}$.

To define H, let v_S be the representation of the set S in binary, i.e. for each $i \in \{1, 2, \dots, n\}$ if $i \in S$ then $(v_S)_i = 1$, else it is 0. Therefore $v_S \in \{0,1\}^n$. Now if α is the corresponding string from the column matrix, then $H_{S,\alpha} = (-1)^{v_S \cdot \alpha}$. This matrix is called the Hadamard Matrix.

2.2.1 Properties of Hadamard Matrices

1. Sum of elements in any row S (except 1^{st}) of $H = |\{\alpha : v_S \cdot \alpha = 0\}| - |\{\alpha : v_S \cdot \alpha = 1\}| = 0$. Reason: Fix S. Let $X_i = \{\alpha : \alpha \cdot v_S = i\}, i = 0, 1$. Sum of elements $= |X_0| - |X_1|$. To see $|X_0| = |X_1|$, we construct a bijection between $|X_0|$ and $|X_1|$. Fix some $s \in S$, and let e_s be the vector with 1 in the s^{th} position and 0's elsewhere. Then $v \longrightarrow v \oplus e_s$ is the bijection and is its own inverse.

2. $H_S \cdot H_T = 0$ for $S \neq T$. Since

$$\begin{aligned} H_S \cdot H_T &= \sum_\alpha (-1)^{v_S.\alpha}.(-1)^{v_T \cdot \alpha} \\ &= \sum_\alpha (-1)^{(v_S \oplus v_T)\cdot \alpha} \\ &= \sum_\alpha (-1)^{v_{S\Delta T}\cdot \alpha} \\ &= 0 \end{aligned}$$

   by Property 1, where $v_{S\Delta T}$ is the symmetric difference between the two vectors v_S and v_T.

3. $H_S \cdot H_S = 2^n$.

4. From the above properties, it follows that $HH^T = 2^n I$. Since $\vec{b} = H\vec{p}$, we have $\vec{p} = H^{-1}\vec{b}$ or $\vec{p} = 2^{-n} H^T \vec{b}$. So when $b_\phi = 1$ and $b_S = 0$ for $S \neq \phi$, we have

$$\vec{p} = \begin{pmatrix} 2^{-n} \\ 2^{-n} \\ \vdots \\ 2^{-n} \end{pmatrix}$$

   Hence p is the uniform distribution.

$\square$

Proposition 5 *Suppose X is ϵ-biased i.e. $(\forall S \neq \phi), |b_S| \leq \epsilon$. Then X is ϵ-close to k-wise independence in max norm.*

Proof: Since $p_i = 2^{-n}(b_\phi \pm b_{\{1\}} \pm b_{\{2\}} \pm \ldots)$, $p_i = 2^{-n} + (2^n - 1)$ other terms each $\leq \frac{\epsilon}{2^n}$, or $|p_\alpha - 2^{-n}| < \epsilon$. Since $X_1, X_2 \ldots X_n$ is ϵ-biased, $X_{i_1}, X_{i_2} \ldots X_{i_k}$ is also ϵ-biased, and $X_{i_1}, X_{i_2} \ldots X_{i_k}$ is ϵ-close to k-wise uniform in max norm. In other words, X is ϵ-close to k-wise independence in max norm. $\square$