Algebraic Methods in Computer Science	December 31, 2014
Lecture: 10	
Lecturer: *Amir Shpilka*	Scribe: *Renen Perlman*

Combinatorial Nullstellensatz

We will see applications of the following theorem that was proved in the previous lecture.

Theorem 1 (Theorem 2 from last lecture)**.** *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial over some field $\mathbb{F}$ such that $\deg(f) = \sum_{i=1}^{n} t_i$. Assume that the coefficient of the monomial $\prod_{i=1}^{n} x_i^{t_i} \neq 0$. Let $S_1, \ldots, S_n \subset \mathbb{F}$ a collection of n subsets such that $|S_i| > t_i$ for every $i \in [n]$. Then, there exists $s \in S_1 \times \ldots \times S_n$ such that $f(s) \neq 0$.*

We will use the theorem to prove the existence of certain objects. The proof scheme will roughly be: given the setting we will define a polynomial such that the required object is a nonzero of the polynomial. Thus, to show that the object exists we have to prove that the polynomial does not vanish identically over the entire domain. This will follow from a careful examination of the structure of the polynomial that we defined and an application of Theorem 1.

Cauchy-Davenport Theorem

Let $\mathbb{F}_p$ be a field over some prime number p. Let $A, B \subset \mathbb{F}_p$ be two subsets. Define the summation of those sets to be $A + B := \{a + b \mid a \in A, b \in B\}$. We wish to bound the size of $A + B$.

Clearly, an obvious upper bound is $|A + B| \leq |A| \cdot |B|$. However, this can be far from the truth as for $A = \{0, \ldots, k\}$ and $B = \{0, \ldots, m\}$ we have $A + B = \{0, \ldots, k + m\}$ and thus $|A + B| = |A| + |B| - 1$. We will show that in fact, this is the worst possible example. I.e., we shall prove the lower bound $|A + B| \geq min\{p, |A| + |B| - 1\}$. We note that taking A and B to be any two arithmetic progressions we get an example where the lower bound is tight. It is also important to note that it is crucial that p is a prime and not prime power. Otherwise we can take $A = B$ to be some subspace, and get $A + B = A$.

Theorem 2 (Cauchy-Davenport)**.** *Let A, B be subsets as defined above, then $|A+B| \geq \min\{p, |A| + |B| - 1\}$*

Proof. We consider two cases.

1. $|A| + |B| > p$: We claim that in this case, $A + B = \mathbb{F}_p$. Indeed, for every $c \in \mathbb{F}_p$ we have that
$$A \cap (c - B) \neq \emptyset,$$
where $c - B = \{c - b \mid b \in B\}$. Since $|B| = |c - B|$ the intersection is not empty. Hence, there exists $a \in A$ and $b \in B$ such that $a = c - b$. This implies that $a + b = c$ and thus $c \in A + B$. It follows that in this case $A + B = \mathbb{F}_p$ and the bound holds.

2. $|A| + |B| \leq p$: Denote $C = A + B$. Assume towards a contradiction that $|C| \leq |A| + |B| - 2$. Without loss of generality we can assume that $C = |A| + |B| - 2$, otherwise we just add some elements from $\mathbb{F}_p$ to C. Let $f(x, y)$ be the polynomial
$$f(x, y) = \prod_{c \in C} (x + y - c).$$

Note that $f|_{A\times B} \equiv 0$ and that $\deg(f) = |C| = |A| + |B| - 2$. We would like to use Theorem 1 with A and B playing the role of S_1 and S_2, respectively. Looking at the monomial $x^{|A|-1}y^{|B|-1}$ we get that its coefficient in f is $\binom{|C|}{|A|-1} = \binom{|A|+|B|-2}{|A|-1} \not\equiv_p 0$ (because $|A| + |B| \leq p$ all the terms are non zero). Applying Theorem 1 we get that there exists $(a, b) \in A \times B$ such that $f(a, b) \neq 0$, in contradiction.

□

Remark 3. *Looking at the case $A = A$ of Cauchy-Davenport theorem we see that the question concerns the additive structure of A. Intuitively, $|A + A|$ should be small when A resembles a set that is (almost) close under addition. In the integers such sets are arithmetic progressions, and in vector spaces those sets are subspaces.* Additive Combinatorics *is a relatively modern subfield of mathematics that examines, among other questions, the relation between $|A + A|/|A|$ and the resemblance of A to an arithmetic progression or a subspace. Thus, it can be viewed as the study of "approximate linear algebra".*

For example, it is known that if $A \subset \mathbb{N}$ and $|A + A| = c|A|$ then there exists a subset $A' \subseteq A$ such that $|A'| > |A|/c'$ and A' is a subset of an arithmetic progression of size at most $c' \cdot |A|$, for some constant c' that depends on c. If V is a vector space and $A \subseteq V$ satisfies $|A + A| \leq c|A|$ then there exists $A' \subseteq A$ such that $|A'| > |A|/c'$ and A' is a subset of subspace U of size at most $c'|A|$. For more on additive combinatorics see the book [TV06].

Chevalley - Warning Theorem

Another application is the classical Chevalley-Warning theorem. We will prove a weaker version of the theorem.

Theorem 4 (Chevalley - Warning)**.** *Let $\mathbb{F}_p$ be a finite field, and $f_1, \ldots, f_m \in \mathbb{F}_p[x_1, \ldots, x_n]$ a set of polynomials over $\mathbb{F}_p$. Assume that $\sum_{i=1}^m \deg(f_i) < n$ and that there exists a common root to all f_i. I.e. there exists some $\alpha \in \mathbb{F}_p^n$ such that $f_i(\alpha) = 0$, for every $i = 1, \ldots, m$. Then, there exists another common root in $\mathbb{F}_p^n$.*

The stronger theorem is:

Theorem 5 (Chevalley - Warning (stronger version))**.** *Let $f_1, \ldots, f_m \in \mathbb{F}_p[x_1, \ldots, x_n]$ be as defined above. If there exists a common root, then the number of common roots is equivalent to zero modulo p.*

Proof. Assume towards a contradiction that α is the only common root. Define a polynomial

$$g(x) = \underbrace{\prod_{i=1}^{m} \left(1 - f_i(x)^{p-1}\right)}_{g_1(x)} - \underbrace{\prod_{i=1}^{n} \frac{\prod_{\beta\neq\alpha_i}(x_i - \beta)}{\prod_{\beta\neq\alpha_i}(\alpha_i - \beta)}}_{g_2(x)}$$

Note that g vanishes on $\mathbb{F}_p^n$. Indeed, as α is the unique common root by our assumption, $g_1(\gamma) = g_2(\gamma) = \delta_{\alpha,\gamma}$. Also note that $\deg(g_1) = (p-1)\sum_{i=1}^n \deg(f_i)$ and $\deg(g_2) = n(p-1)$. Since $\sum_{i=1}^m \deg(f_i) < n$ it follows that $\deg(g_1) < \deg(g_2)$, hence, $deg(g) = n(p-1)$. The coefficient of the monomial $x_1^{p-1} \cdot \ldots \cdot x_n^{p-1}$ is not zero (in fact it is $(-1)^n$, because the product of all the nonzero elements in $\mathbb{F}_p$ is -1). By Theorem 1, for $S_1 = \ldots = S_n = \mathbb{F}_p$, there exists $\gamma \in \mathbb{F}_p^n$ such that $g(\gamma) \neq 0$ in contradiction. □

Union of affine hyperplanes

Consider the following problem: we would like to represent $\{0,1\}^n\backslash\{0\}$ as a union of affine hyperplanes. Denote by H_α and H'_α the possible hyperplanes: $H_\alpha = \{x| <\alpha, x>_2= 0\}$, $H'_\alpha = \{x| <\alpha, x >_2= 1\}$. Note that we cannot take any H_α for our cover, because $0 \in H_\alpha$.

Consider the trivial example: $\bigcup_{i=1}^n \left(H'_i = \{x|x_i = 1\}\right)$. Note that we needed n hyperplanes. We will show that this is in fact the lower bound. In other words, any cover must be of size at least n.

Theorem 6. *For every representation of $\{0,1\}^n\backslash\{0\}$ as a union of m affine hyperplanes, $m \geq n$.*

Proof. Let $H'_{\alpha_1}, \ldots, H'_{\alpha_m}$ be a set of affine hyperplanes such that $\{0,1\}^n\backslash\{0\} = \bigcup_{i=1}^m H'_{\alpha_i}$. Assume towards a contradiction that $m < n$.
We use the same pattern to achieve a polynomial that vanishes over our domain.

$$g(x) = \underbrace{\prod_{i=1}^{m} \left(1- <\alpha_i, x> \right)}_{g_1(x)} - \underbrace{\prod_{i=1}^{n} (1 - x_i)}_{g_2(x)}$$

Note that for every $x \in \{0,1\}^n\backslash\{0\}$, $g_1(x) = 0$, because x must be in some plane from the cover. On the other hand $g_1(0) = 0$. Hence, $g_1(x) = \delta_{0,x}$. Similarly $g_2(x) = \delta_{0,x}$ too. We also get that $\deg(g_1) = m$ and $\deg(g_2) = n$. From the assumption $m < n$, so $\deg(g) = n$. The coefficient of the monomial $x_1 \ldots x_n$ is $(-1)^{n+1} \neq 0$. By Theorem 1, choosing $S_1 \ldots S_n$ to be $\{0,1\}^n$, there exists $\gamma \in \{0,1\}^n$ s.t. $g(\gamma) \neq 0$, a contradiction. □

The permanent Lemma and its applications

We begin with a definition

Definition. *Let A be a square n by n matrix. The permanent polynomial is defined as*

$$Perm(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Where S_n is the set of all permutations over $[n]$.

This definition is very similar to the one of the determinant. The former differs from the latter in that it doesn't take into account the signature of the permutations. Although this difference seems minor, the determinant can be computed in polynomial time, while the computation the permanent of a $(0,1)$-matrix is #P-complete. Yet, it is easy to compute the all 1's matrix, denoted by J, simply $Perm(J) = n!$.

Lemma 7 (The Permanent Lemma)**.** *Let A by a n by n matrix over a field $\mathbb{F}$. If $Perm(A) \neq 0$, then for every vector $b \in \mathbb{F}^n$ and every n subsets of size 2 $S_1, \ldots, S_n \subset \mathbb{F}$ there exists a vector $v \in S_1 \times S_2 \times \ldots \times S_n$ such that $(Av)_i \neq b_i$ for every $i = 1, \ldots, n$.*

Proof. Define the polynomial

$$g(x) = \prod_{i=1}^{n} \Big(\underbrace{\sum_{j=1}^{n} a_{i,j} x_j}_{=(Ax)_i} - b_i \Big)$$

f is of degree n. Note that the coefficient of the monomial $x_1 \dots x_n$ is $Perm(A) \neq 0$. That is because f could be written as

$$\begin{aligned} g(x) = &(a_{1,1}x_1 + \dots + a_{1,n}x_n - b_1) + \\ &+ (a_{2,1}x_1 + \dots + a_{2,n}x_n - b_2) + \\ &\vdots \\ &+ (a_{n,1}x_1 + \dots + a_{n,n}x_n - b_n) \end{aligned}$$

Therefore, the coefficient of the monomial is the summation of the coefficient of x_i, over all possibilities of choosing a specific x_i from every row. Which is the summation of $a_{i,\sigma(i)}$ over all the permutations σ. By Theorem 1, we get that there exists $\gamma \in S_1 \times \dots \times S_n$ such that $g(\gamma) \neq 0$ which implies $(A\gamma)_i \neq b_i$ for every $i = 1, \dots, n$. □

Now we'll see some applications of this lemma.

Theorem 8. *Let p be some prime number. For every sequence of $2p-1$ elements $(a_i)_{i=1}^{2p-1} \in \mathbb{F}_p$ there exists a sub sequence of length p $(a_{n_i})_{i=1}^{p}$ such that $\sum_{i=1}^{p} a_{n_i} = 0 \ (mod\ p)$*

Proof. We sort the sequence such that $0 \leq a_1 \leq a_2 \leq \dots \leq a_{2p-1} < p$. Consider the two following cases

1. If there is an index i such that $a_i = a_{i+p}$ then we have a sub sequence of p identical elements, and we are done.

2. Otherwise, define $(S_i = \{a_i, a_{i+p}\})_{i=1}^{p-1}$ a set of $p-1$ sets. Note that for every i, $|S_i| = 2$, else we get back to the former case. Denote by A the all 1's matrix of size $p-1$ by $p-1$. Define $b \in \mathbb{F}_p^n$ to be the vector containing all the element of $\mathbb{F}_p$ besides $-a_{2p-1}$, in some order. Since $Perm(A) = (p-1)! \neq_p 0$, then we can use The Permanent Lemma 7. Meaning there exists $v \in S_1 \times S_2 \times \dots \times S_n$ such that $(Av)_i \neq b_i$ for every $i = 1, \dots, n$. Denote by $\alpha = \sum_{i=1}^{p-1} v_i$. We get that
$$\forall i \in [p-1] \qquad (Av)_i = \alpha \neq b_i \Rightarrow \alpha = -a_{2p-1}$$
Since α doesn't equal any of b_i, which are $\mathbb{F}_p \backslash \{-a_{2p-1}\}$, then $\sum_{i=1}^{p-1} v_i = \alpha = -a_{2p-1}$. So
$$\sum_{i=1}^{p-1} v_i + a_{2p-1} = 0$$
Since $v \in S_1 \times S_2 \times \dots \times S_n$, then it can be seen as a sub sequence of $p-1$ elements. Adding a_{2p-1} to it, we get a sub sequence of length p with sum 0.

□

We see now that we could have farther demanded that the sub sequence will contain a specific element.
Now we move to another application. Again begin with a definition

Definition (Additive Basis)**.** *A subset (with repetitions) $C \subset \mathbb{F}_p^n$ is called an <u>additive basis</u> if every $v \in \mathbb{F}_p^n$ can be represented as a summation of a subset of C*

For example if $\{v_1, \ldots, v_n\}$ is a basis, then

$$C = \{\underbrace{v_1, \ldots, v_1}_{p-1 \text{ times}}, \underbrace{v_2, \ldots, v_2}_{p-1 \text{ times}}, \ldots, \underbrace{v_n, \ldots, v_n}_{p-1 \text{ times}}\}$$

is an additive basis.

Hypothesis 9. *There exists some constant $c(p)$ (depends solely on p) such that any union of $c(p)$ bases is an additive basis.*

This is still an open problem. It is known so far that any union of $p\,logn$ bases is an additive basis. We will give a sufficient condition for any set of size $(p-1)n$ to be an additive basis, as described in the following lemma.

Lemma 10. *Let $S = \{v_1, \ldots, v_{(p-1)n}\} \subset \mathbb{F}_p^n$ be a multi-set (a set with repetitions). Define A to be the $(p-1)n$ by $(p-1)n$ matrix*

$$A = \left.\begin{pmatrix} | & & | \\ n\{ v_1 & \cdots & n\{ v_n \\ | & & | \\ \hline \vdots & \ddots & \vdots \\ \hline | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}\right\} n(p-1)$$

If $Perm(A) \neq 0$ then S is an additive basis

Proof. Define the sets $S_1 = \ldots = S_{(p-1)n} = \{0, 1\}$ and let $a \in \mathbb{F}_p^n$ be some vector. Define a new vector b

$$\bar{b} = \begin{pmatrix} \bar{a} + \bar{1} \\ \hline \vdots \\ \hline \bar{a} + (p-1) \end{pmatrix}$$

Using The Permanent Lemma 7, we get a vector $u \in \{0, 1\}^n$ such that for every $i = 1, \ldots, n(p-1)$ $(Au)_i \neq b_i$. Again, like in the previous theorem, denote by α the summation $\alpha = \sum_{\substack{i=0 \\ u_i=1}}^{n} v_i$, then

$$Au = \begin{pmatrix} \alpha \\ \hline \alpha \\ \hline \vdots \\ \hline \alpha \end{pmatrix}$$

So $\alpha \neq a + q$ for every $1 \leq q \leq p-1$. Therefore $q = 0$ and

$$a = \sum_{\substack{i=0 \\ u_i=1}}^{n} v_i$$

Meaning that a is the sum of a subset of S. □

Hypothesis 11. *Let $c(p)$ be the constant from the former hypothesis. Then, $c(p) = p$*

Hypothesis 12. *For every set of p invertible matrices with size n by n, $A_1, \ldots, A_p$ there exists a matrix $C_{p \times pn}$*

$$Perm \left(\begin{array}{cccc} A_1 & A_2 & \cdots & A_p \\ \hline A_1 & A_2 & \cdots & A_p \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_1 & A_2 & \cdots & A_p \\ \hline \multicolumn{4}{c}{C} \end{array} \right) \neq 0$$

Clearly hypothesis 11 $\Rightarrow$ hypothesis 9. Furthermore hypothesis 12 $\Rightarrow$ hypothesis 11, since we can construct a vector

$$b = \begin{pmatrix} a+1 \\ a+2 \\ \vdots \\ a+p-1 \\ \phi \end{pmatrix}$$

(where ϕ could be any element of $\mathbb{F}_p$), and simply repeat the proof above with the matrix:

$$\left(\begin{array}{cccc} A_1 & A_2 & \cdots & A_p \\ \hline A_1 & A_2 & \cdots & A_p \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_1 & A_2 & \cdots & A_p \\ \hline \multicolumn{4}{c}{C} \end{array} \right)$$

Fourier Transform on the Boolean Cube

We are looking for a basis to the functions space $\{0,1\}^n \to \mathbb{R}$ (could be to $\mathbb{C}$ as well, the difference will be in the inner product). For example the set of functions are a basis to the sub space $\{0,1\}^n \to \{0,1\}$:

$$\forall \alpha \in \{0,1\}^n. \qquad \delta_\alpha(\bar{x}) = \begin{cases} 1 & \bar{x} = \alpha \\ 0 & \text{otherwise} \end{cases}$$

Clearly they are linearly independent. Also, there are $2^d = \dim(\{0,1\}^n \to \{0,1\})$ such function. Therefore its is a basis. Hench, each function $f : \{0,1\}^n \to \mathbb{R}$ can be represented as $f(\bar{x}) = \sum_\alpha f(\alpha)\delta_\alpha(\bar{x})$. Another very important example is the set of all characters.

Definition (Character)**.**

$$\chi_\alpha : \{0,1\}^n \to \mathbb{R} \qquad \chi_\alpha(x) = (-1)^{<\alpha,x>} = (-1)^{(\sum_{i=1}^n \alpha_i x_i)_{mod 2}}$$

Properties:

$$\forall \alpha, \beta \in \{0,1\}^n \qquad \chi_\alpha(\beta) = \chi_\beta(\alpha) \tag{1}$$

$$\forall \alpha, \beta \in \{0,1\}^n \qquad \chi_\alpha \cdot \chi_\beta = \chi_{\alpha \oplus \beta} \quad \oplus \text{ is bitwise XOR} \tag{2}$$

We can define inner product over our function space

$$<f,g>= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)g(x)$$

(Over $\mathbb{C}$ we take $\overline{g(x)}$ instead)
So we get the following property:

$$<f,g>= \mathbb{E}[f \cdot g] \tag{3}$$

The mean is taken over the uniform distribution U_n.

Claim 13. *For every $\alpha, \beta \in \{0,1\}^n$, using the inner product defined above,*

$$<\chi_\alpha, \chi_\beta>= \begin{cases} 0 & \alpha \neq \beta \\ 1 & \alpha = \beta \end{cases}$$

Proof. Using property 2 and property 3.

$$<\chi_\alpha, \chi_\beta>= \mathbb{E}[\chi_\alpha \cdot \chi_\beta] = \mathbb{E}[\chi_{\alpha \oplus \beta}]$$

If $\alpha = \beta$, then $\alpha \oplus \beta = \bar{0}$, so $\mathbb{E}[\chi_\alpha \cdot \chi_\beta] = \mathbb{E}[\chi_{\bar{0}}] = 1$.
Otherwise, then for exactly half of the elements of $\{0,1\}^n$ $< \alpha \oplus \beta, x >= 0$, and the others $<\alpha \oplus \beta, x>= 1$. Therefore $\chi_{\alpha\oplus\beta} = 1$ for half of the elements, and $\chi_{\alpha\oplus\beta} = -1$ for the other elements. So $\mathbb{E}[\chi_{\alpha\oplus\beta}] = 0$ □

Corollary 14. $\{\chi_\alpha\}_{\alpha \in \{0,1\}^n}$ *is an orthonormal basis of* $\{0,1\}^n \to \{-1,1\}$.

We get that for every $f : \{0,1\}^n \to \mathbb{R}$ there exist coefficients $\{\hat{f}(\alpha)\}$ such that $f(x) = \sum \hat{f}(\alpha)\chi_\alpha(x)$. Which leads us to the following definition:

Definition (Fourier Coefficients)**.** *For every $f : \{0,1\}^n \to \{-1,1\}$ there exists a unique set of coefficients $\{\hat{f}(\alpha)\}_{\alpha\in\{0,1\}^n}$ such that*

$$f(x) = \sum \hat{f}(\alpha)\chi_\alpha(x)$$

Those coefficients are called the Fourier coefficients of f.

Note that, since $\{\chi_\alpha\}$ is an orthonormal basis then

$$\hat{f}(\alpha) = <f, \chi_\alpha> = \mathbb{E}_x[f(x)\chi_\alpha(x)]$$

Another property is

$$\hat{f}(\alpha) = \mathbb{E}[f(x)\chi_\alpha(x)] = Pr(f = \chi_\alpha) - Pr(f \neq \chi_\alpha)$$

So we can think of $\hat{f}(\alpha)$ as a measurement of how much f resembles to the linear function $<\alpha, x>$. We will now see some basic and important properties of the Fourier coefficients:

Claim 15.

$$\mathbb{E}[fg] = <f, g> = \sum \hat{f}(\alpha)\hat{g}(\alpha)$$

Proof. The proof is immediate using the fact that the basis is orthonormal.

$$<f, g> = <\sum_\alpha \hat{f}(\alpha)\chi_\alpha, \sum_\beta \hat{g}(\beta)\chi_\beta> = \sum_\alpha \hat{f}(\alpha) \sum_\beta \hat{g}(\beta) <\chi_\alpha, \chi_\beta>= \sum \hat{f}(\alpha)\hat{g}(\alpha)$$

□

Corollary 16 (Parseval Inequality)**.**

$$\forall f : \{0,1\}^n \to \{\pm 1\}. \qquad \sum \hat{f}^2(\alpha) = 1$$

Proof. Since the image of f is $\{\pm 1\}$, then $f^2 \equiv 1$. Therefore, using Claim 15

$$\sum \hat{f}^2(\alpha) = <f, f> = \mathbb{E}[f^2] = \mathbb{E}[1] = 1$$

□

Claim 17. *Let $S \subset \{0,1\}^n$ be some subset. Let f be its indicating function. I.e. $f(x) = \begin{cases} 1 & x \in S \\ 0 & otherwise \end{cases}$. Assume that for all $\alpha \in \{0,1\}^n$ the Fourier coefficient is bounded by $\frac{\epsilon}{2^n}$ for some $\epsilon > 0$, then S is ϵ-biased.*

Reminder 18. *A set S is ϵ-biased if there exists some $\epsilon < 0$ for all $\alpha \neq 0$*

$$\left|\frac{1}{|S|}\sum_{x\in S}(-1)^{<\alpha,x>}\right| \leq \epsilon$$

Proof.

$$\hat{f}(\alpha) = \frac{1}{2^n}\sum_{x\in\{0,1\}^n} f(x)\chi_\alpha(x) = \frac{1}{2^n}\sum_{x\in S}(-1)^{<\alpha,x>}$$

So

$$\forall \alpha \neq 0. \qquad |\hat{f}(\alpha)| \leq \epsilon\frac{|S|}{2^n} \Leftrightarrow S \text{ is } \epsilon\text{-biased}$$

□

Applications of Fourier Transform

Property Testing

Given a property of boolean functions, we would like to check whether a function f has it. We can think of this property as a sub set $P \subset \{f : \{0,1\}^n \to \{\pm 1\}\}$. Hence f has the property if and only if $f \in P$.

Some properties are very easy to verify. For example $P = \{f | f(\bar{0} = 1)\}$ takes one query. On the other hand some properties requires to check all the 2^n possible inputs, for example to check if f is linear. Therefore we shall determine whether f is "close" to some $g \in P$ or "far" from any $g \in P$. Doing that will require much less queries. Which leads us to our next topic.

Linearity Testing

We examine the property: linearity. Our subset is then, $P = \{\chi_\alpha\}$. Every $g \in P$ must satisfy $g(x)g(y) = g(x \oplus y)$ for any $x, y \in \{0,1\}^n$. Hence we get the following algorithm.

Algorithm(BLR)
Pick $x, y \in \{0,1\}^n$ uniformly and independently.
If $g(x)g(y) = g(x \oplus y)$ return PASS. (3 queries)
Else return FAIL.

Clearly there exists $g \notin P$ that our algorithm could output PASS for. On the other hand for any $g \in P$ it will always output PASS (this property is called one-sided error).

Now we examine the correlation between the probability that the algorithm outputs PASS for some function g to the distance between g and $f \in P$.

$$Pr_{x,y}(g \mapsto PASS) = Pr_{x,y}(g(x)g(y) = g(x \oplus y)) = Pr_{x,y}(g(x)g(y)g(x \oplus y) = 1) =: p$$

Note that we get that

$$\mathbb{E}_{x,y}(g(x)g(y)g(x \oplus y)) = p - (1 - p) = 2p - 1$$

Now we compute the expectation using Fourier coefficients. As a thumb rule, when computing a summation of Fourier coefficients we change the order of summation and use the orthonmality property of the characters.

$$\mathbb{E}_{x,y}(g(x)g(y)g(x \oplus y)) = \mathbb{E}[(\sum_\alpha \hat{g}(\alpha)\chi_\alpha(x))(\sum_\beta \hat{g}(\beta)\chi_\beta(y))(\sum_\gamma \hat{g}(\gamma)\chi_\gamma(x \oplus y))] =$$

$$= \frac{1}{2^n}\frac{1}{2^n} \sum_{x,y,\alpha,\beta,\gamma} \hat{g}(\alpha)\hat{g}(\beta)\hat{g}(\gamma)\chi_\alpha(x)\chi_\beta(y)\chi_\gamma(x)\chi_\gamma(y) = \sum_\gamma \hat{g}(\gamma)\hat{g}(\gamma)\hat{g}(\gamma) = \sum_\gamma \hat{g}(\gamma)^2\hat{g}(\gamma)$$

Because $\frac{1}{2^n}\sum_x \chi_\alpha(x)\chi_\gamma(x) = <\chi_\alpha, \chi_\gamma> \neq 0$ if and only if $\alpha = \gamma$. Similarly we get that $\beta = \gamma$. Now since, $\sum \hat{g}(\gamma)^2 = 1$, then we get a weighted mean of $\hat{g}(\gamma)$ so

$$2p - 1 = \mathbb{E}_{x,y}(g(x)g(y)g(x \oplus y)) = \sum_\gamma \hat{g}(\gamma)^2\hat{g}(\gamma) \leq max_\alpha \hat{g}(\alpha)$$

We can rewrite the maximum as

$$max_\alpha \hat{g}(\alpha) = max_\alpha(Pr_x(g(x) = \chi_\alpha(x)) - Pr_x(g(x) = \chi_\alpha(x)) = max_\alpha(2Pr_x(g(x) = \chi_\alpha(x)) - 1)$$

$$\Rightarrow p \leq max_\alpha Pr_x(g(x) = \chi_\alpha(x))$$

Therefore, there exists a linear function f such that $Pr[f = g] \geq p$.

Notes

The part about combinatorial Nullstellensatz is from the paper [Alo99]. For a treatment of Fourier analysis see [O'D14].

References

[Alo99] N. Alon, *Combinatorial nullstellensatz*, Combinatorics, Probability and Computing **8** (1999), 7–29. 10-10

[O'D14] Ryan O'Donnell, *Analysis of boolean functions*, Cambridge University Press, 2014. 10-10

[TV06] T. Tao and V.H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2006. 10-2