Harmonic Analysis of Boolean Functions, and applications in CS

Lecture 7

April 14, 2008

Lecturer: Guy Kindler | Scribe by: Zvika Brakerski | Updated: May 3, 2008

In this lecture we complete Kalai's proof of Arrow's Theorem (Section 1) and then go on to introduce the subject of testing codes and specifically the *Long Code* (Section 2).

1 Arrow's Theorem — Continued

1.1 In Previous Lecture

Recall the discussion of voting schemes from the previous class. We consider a set of candidates C, and a set of n permutations $\{R_i\}_{i\in[n]}$ over C such that R_i is the preference of the i^{th} voter. A voting scheme F takes $R_1,\ldots,R_n$ and returns a relation $R = F(R_1,\ldots,R_n)$ on C. We listed some (possibly desirable) properties of a voting scheme:

1. Rationality.
2. Independence of Irrelevant Choices.
3. Neutrality.
4. Transitivity.

Kalai's formulation of Arrow's theorem is the following two theorems.

Theorem 1 *There exists a constant $c < 1$ s.t. if F has 2, 3, 4 then*

$$\Pr\left[F \text{ is rational}\right] < c < 1 \ .$$

Theorem 2 *There exists a constant k s.t. if F has 2, 3 and $\varepsilon = \Pr[F \text{ is irrational}]$ then F is $k\varepsilon$-close to a dictatorship.*

Recall that we showed that it is sufficient to prove the theorems for the case of only 3 candidates. Since in both theorems F has property 2, we are able to represent a voting scheme F by 3 functions $f, g, h : \{\pm1\}^n \to \{\pm1\}$, where each function represents the preferences of the voters with respect to two of the three candidates.

Thus F is a function of $3n$ variables

$$F(x_1,\ldots,x_n,\underbrace{x_{n+1},\ldots,x_{2n}}_{y_1,\ldots,y_n},\underbrace{x_{2n+1},\ldots,x_{3n}}_{z_1,\ldots,z_n}) = (f(x),g(y),h(z)) \ .$$

Recall that F is rational iff $\mathrm{NAE}(f(x),g(y),h(z)) = 1$. $\mathrm{NAE} : \{\pm1\}^3 \to \{0,1\}$ is the *not-all-equal* function that can be expressed as a polynomial $\mathrm{NAE}(\alpha,\beta,\gamma) = \frac{3}{4} - \frac{1}{4}\alpha\beta - \frac{1}{4}\beta\gamma - \frac{1}{4}\alpha\gamma$. We also defined the set of all rational votes $\Psi = \{(x,y,z) : \forall_i\ \mathrm{NAE}(x_i,y_i,z_i) = 1\}$.

We further defined an indicator variable $A = \mathbb{1}_\Psi$ so that $A(x,y,z) = \prod_{i=1}^n \mathrm{NAE}(x_i, y_i, z_i)$. Using these definitions, we showed that the probability of rationality is

$$\begin{aligned}
\Pr_{R_1,\ldots,R_n}[F \text{ is rational}] &= \frac{1}{\Pr[\Psi]} \cdot \langle A(x,y,z), \mathrm{NAE}(f(x), g(y), h(z))\rangle = \ldots \\
&= \frac{3}{4} - \frac{1}{4}\left(\frac{4}{3}\right)^n \cdot \langle A(x,y,z), f(x)g(y) + g(y)h(z) + f(x)h(z))\rangle \quad (1)
\end{aligned}$$

We use Plancharel's identity to compute the inner product in (1). To this end we computed the Fourier representation of $f(x)g(y)$. Or in other words, represented it as a polynomial in variables x, y, z.

$$f(x)g(y) = \sum_{S,T\subseteq[n]} \hat{f}(S)\hat{g}(T)\chi_S(x)\chi_T(y) \ , \tag{2}$$

we note that $\chi_S(x)\chi_T(y)$ is a monomial in x, y, z and thus is a character function.

By symmetry this also yields the Fourier representation of $g(y)h(z)$, $f(x)h(z)$.

1.2 Completing the Proof

To complete the computation of the inner product in (1), we consider the Fourier transform of A.

$$A(x,y,z) = \prod_{i=1}^n \mathrm{NAE}(x_i, y_i, z_i) = \prod_{i=1}^n \left(\frac{3}{4} - \frac{1}{4}x_i y_i - \frac{1}{4}y_i z_i - \frac{1}{4}x_i z_i\right) \ . \tag{3}$$

We note that it is sufficient to compute the inner product of A and $f(x)g(y)$ and obtain the rest of the terms by symmetry. Since the Fourier representation of $f(x)g(y)$ (see (2)) only contains characters $\chi_S(x)\chi_T(y)$, it is sufficient to compute the coefficients of such characters in the Fourier representation of A.

Opening the parentheses in the product term of (3) results in a multilinear function. For all $i = 1, \ldots, n$, we select one of the four monomials in the representation of $\mathrm{NAE}(x_i, y_i, z_i)$. We notice that taking a monomial that contains z_i in any of the NAE terms, results in a character function that contains z_i. Specifically it is not a character of the form $\chi_S(x)\chi_T(y)$ that interests us. Thus the characters $\chi_S(x)\chi_T(y)$ result from selecting, in each NAE term, either the constant $\frac{3}{4}$ or the monomial $-\frac{1}{4}x_i y_i$. Hence it is impossible to select x_i without also selecting y_i (and vice verse). Therefore characters $\chi_S(x)\chi_T(y)$ where $S \neq T$ do not appear at all in the resulting expression. When $S = T$, however, the character $\chi_S(x)\chi_T(y)$ is obtained by selecting the monomial $-\frac{1}{4}x_i y_i$ for $i \in S$ and the constant $\frac{3}{4}$ for all other values of i.

Hence the coefficient of character $\chi_S(x)\chi_T(y)$ in the resulting expression is

1. If $S \neq T$ then the coefficient is 0.
2. If $S = T$ then the coefficient is $\left(\frac{3}{4}\right)^{n-|S|} \cdot \left(-\frac{1}{4}\right)^{|S|}$.

Therefore

$$\left(\frac{4}{3}\right)^n \cdot \langle A, fg\rangle = \left(\frac{4}{3}\right)^n \cdot \sum_{S\subseteq[n]} \left(\frac{3}{4}\right)^{n-|S|} \cdot \left(-\frac{1}{4}\right)^{|S|} \hat{f}(S)\hat{g}(S) = \underbrace{\sum_S \left(-\frac{1}{3}\right)^{|S|} \hat{f}(S)\hat{g}(S)}_{\text{denote } \ll f,g \gg} \ .$$

We get

$$\Pr_{R_1,\ldots,R_n}[F \text{ is rational}] = \frac{3}{4} - \frac{1}{4}(\ll f,g \gg + \ll g,h \gg + \ll f,h \gg) \ .$$

Recall that in our theorems, F is neutral — that is the relation it produces is invariant to permutations on the set of candidates C. Consider the preference between candidates a and b, which is determined by $f(x)$. Applying the permutation $(a,b,c) \to (c,a,b)$, results in the preference between a and b being $g(x)$. Neutrality, therefore, implies that $f = g$. Similarly neutrality over the permutation $(a,b,c) \to (a,c,b)$ implies that $f = h$. Therefore $f = g = h$. Furthermore, neutrality over the permutation $(a,b,c) \to (b,a,c)$ implies that $f(x) = -f(-x)$.

Hence the term for the probability of rationality is

$$\begin{aligned}
\frac{3}{4} - \frac{3}{4} \ll f,f \gg &= \frac{3}{4} - \frac{3}{4}\sum_S \left(-\frac{1}{3}\right)^{|S|} \hat{f}(S)^2 = \frac{3}{4} - \frac{3}{4}\sum_i \left(-\frac{1}{3}\right)^i \left\|f^{=i}\right\|_2^2 \\
&= \frac{3}{4} - \frac{3}{4}\left(\left\|f^{=0}\right\|_2^2 - \frac{1}{3}\left\|f^{=1}\right\|_2^2 + \frac{1}{9}\left\|f^{=2}\right\|_2^2 + \ldots\right) \\
&= \frac{3}{4} + \frac{1}{4}\left(\left\|f^{=1}\right\|_2^2 - \frac{1}{3}\left\|f^{=2}\right\|_2^2 + \frac{1}{9}\left\|f^{=3}\right\|_2^2 - \ldots\right) \qquad (4)
\end{aligned}$$

where the last equality is due to the fact that $f(-x) = -f(x)$ and thus $\left\|f^{=0}\right\|_2^2 = 0$.

Corollaries of formula: we have

$$\begin{aligned}
\left\|f^{=1}\right\|_2^2 - \frac{1}{3}\left\|f^{=2}\right\|_2^2 + \frac{1}{9}\left\|f^{=3}\right\|_2^2 - \ldots &\leq \left\|f^{=1}\right\|_2^2 + \frac{1}{9}\left(\left\|f^{=3}\right\|_2^2 + \left\|f^{=5}\right\|_2^2 + \ldots\right) \\
&\leq \left\|f^{=1}\right\|_2^2 + \frac{1}{9}\left(1 - \left\|f^{=1}\right\|_2^2\right) \\
&= \frac{8}{9}\left\|f^{=1}\right\|_2^2 + \frac{1}{9}. \qquad (5)
\end{aligned}$$

Therefore if Pr[rationality] $= 1$, this term must also be 1 and thus $\left\|f^{=1}\right\|_2^2 = 1$ which means, as we saw long ago, that f is a dictatorship.

Using the expression we have, we now prove the theorems.

Proof of Theorem 2: Let ε be the probability of irrationality of F. Then combining (4) and (5) we have

$$1 - 4\varepsilon \leq \left\|f^{=1}\right\|_2^2 - \frac{1}{3}\left\|f^{=2}\right\|_2^2 + \frac{1}{9}\left\|f^{=3}\right\|_2^2 - \ldots \leq \frac{1}{9} + \frac{8}{9}\left\|f^{=1}\right\|_2^2$$

and therefore $\left\|f^{=1}\right\|_2^2 \geq 1 - \frac{9}{2}\varepsilon$ and $\left\|f^{>1}\right\|_2^2 \leq \frac{9}{2}\varepsilon$. Applying the FKN Theorem on f, yields that it is a $\left(16 \cdot \frac{9}{2}\varepsilon, 1\right)$-junta. That is, f is $\frac{16\cdot 9}{2}\varepsilon$-close to a dictatorship in one of its variables, denote its index by i^*.

Since $F(x,y,z) = (f(x), f(y), f(z))$, each coordinate of F is close to being a dictatorship in its $i^{*\text{th}}$ variable with probability at least $1 - \frac{16\cdot 9}{2}\varepsilon$.

We apply the union bound to obtain that $F(x,y,z) = (x_{i^*}, y_{i^*}, z_{i^*})$ with probability at least $1 - \underbrace{3 \cdot \frac{16 \cdot 9}{2}}_{k} \varepsilon$ as claimed. ■

Proof of Theorem 1: Assume towards contradiction that $\varepsilon = \Pr[\text{irrationality}] \leq \frac{1}{10^4}$ then by Theorem 2, f is a $\left(16 \cdot \frac{9}{2}\varepsilon, 1\right)$-junta. Thus there exists i s.t. $\left|\hat{f}(i)\right|^2 > \frac{1}{2}$. By Property 4 (transitivity) it follows that $\forall_{i.}\ \left|\hat{f}(i)\right|^2 > \frac{1}{2}$.[1] Hence $\|f\|_2^2 > \frac{n}{2}$.

Since f is boolean, however, it must be that $\|f\|_2^2 = 1$. We get a contradiction and therefore $\Pr[\text{irrationality}] > \frac{1}{10^4}$. ■

Comments. From Theorem 1 it follows that if 2, 3, 4 hold, there is some probability of an irrational outcome. This raises the question of how close we can get to rationality using a voting scheme with such properties, and which is the voting scheme that achieves this. It can be shown that, at least for the case of 3 candidates, majority has the best probability of rationality.

2 Testing Codes

Let $f : \{\pm 1\}^n \rightarrow \{\pm 1\}$. The truth table of f is a vector of bits (a binary word). A code C is a collection of such functions.

Testing, as opposed to reading the whole codeword, is a process where we read a small (say 10) bits of an alleged codeword. We must then always accept if it is indeed a codeword, and if we accept with high enough probability then the alleged codeword must be *close* to an actual codeword.

It turns out that testing, incorporated with other techniques, implies the following. Let S be a mathematical statement, and let P be a proof for S. There exists a process that reads a small number of bits (say 10) of P, and accepts with high probability only when both S is true and P is ε-close to a proof of S.

The *Long Code* over n-coordinates is $\{f(x) = x_i\}_{i=1}^n$, namely the set of all n-variable dictatorships. We can test the Long Code (or a slight variation thereof, see below) as follows: pick $(x,y,z) \in_R \Psi$ (the set of rational votes). If $\mathrm{NAE}(f(x), f(y), f(z)) = 1$ accept, otherwise reject.

It follows from Theorem 2 that:

1. If f is a dictatorship then $\Pr[\text{accept}] = 1$.

2. If $\Pr[\text{accept}] > 1 - \varepsilon$ then f is $k\varepsilon$-close to a dictatorship, that is, to Long-Code word.[2]

[1] It holds that if f is transitive then $\forall_{i,j.}\ \hat{f}(i) = \hat{f}(j)$.

[2] With the exception that f may be close to negative Long-Code word, which is also a dictatorship. This can be fixed by adding all negative dictatorships to the code.