14 Lecture 14, November 17, 2014

14.1 Proof of Thm (59) Part (2): Lower bound on the size of k-wise independent sample spaces

The specific bound we'll prove is this:

Theorem 61 *If Ω is a k-wise indep. sample space on variables $z_1, \ldots, z_n$, none of which is a.s. constant, then $|\Omega| \geq m(n,k)$ where*

$$m(n,k) = \begin{cases} \sum_{j=0}^{k/2} \binom{n}{j} & \text{(k even)} \\ \binom{n-1}{\frac{k-1}{2}} + \sum_{j=0}^{\frac{k-1}{2}} \binom{n}{j} & \text{(k odd)} \end{cases}$$

Note that for fixed k, $m(n,k) \in \Omega(n^{\lfloor k/2 \rfloor})$.

Proof: Map the values taken by each z_i to reals in such a way that $E(z_i) = 0$.

Now for any $S \subseteq [n]$ define the random variable α_S by

$$\alpha_S = \prod_{i \in S} z_i$$

k-wise independence implies:

$$E(\alpha_S \alpha_T) \quad = \quad \begin{cases} \text{positive if } S = T \text{ and } |S| \leq k \\ 0 \text{ if } S \neq T \text{ and } |S \cup T| \leq k \end{cases}$$

Let J be the following collection of subsets of $[n]$:

If k is even:

$$J = \{S : |S| \leq k/2\}.$$

If k is odd:

$$J = \{S : |S| \leq \frac{k-1}{2}\} \bigcup \{S : 1 \in S \text{ and } |S| \leq \frac{k+1}{2}\}.$$

In either case observe:

$$|S \cup T| \leq k \quad \forall S, T \in J$$

And, $|J| = m(n,k)$.

Now, thinking of the sample space Ω just as a set, we are of course done if that set is infinite; otherwise, write the random variables α_S explicitly as functions on that set. So, $\alpha_S(i) \in \mathbb{R}$ is the value of α_S on the ith point of Ω. And we let $p(i)$ be the probability associated with this point of Ω (remember Ω is finite, otherwise we're certainly done with the theorem).

For $S \in J$ let $v_S \in \mathbb{R}^\Omega$ be the vector

$$v_S(i) = \sqrt{p(i)}\alpha_S(i)$$

Consider the matrix with rows v_S for each $S \in J$: It is an $m(n,k) \times |\Omega|$ matrix:

$$\begin{pmatrix} - - - & v_\emptyset & - - - \\ - - - & v_{\{1\}} & - - - \\ - - - & v_{\{1\}} & - - - \\ - - - & v_{\{1,2\}} & - - - \\ - - - & \cdots & - - - \end{pmatrix}$$

Observe that

$$E(\alpha_S \alpha_T) = v_S v_T^\dagger$$

so the rows of this matrix are orthogonal. They are nonzero (due to each z_i being not a.s. constant). So the matrix has full row rank.

$$\implies |\Omega| \geq m(n,k)$$

□

14.2 Graph non-isomorphism. Private-coin interactive protocol. Goldwasser-Sipser AM protocol.

See Goldwasser and Sipser [30] or Arora and Barak, Computational Complexity, Ch. 8.