Constructive Combinatorics
Tibor Szabó

So 2018

Exercise Sheet 7

Due date: July 18th

You should try to solve and write clear solutions to as many of the exercises as you can.

Exercise 1 A random variable is called *almost constant* if there exists a single value that it takes with probability 1.

(a) Show that if the N random variables $r_1, \dots r_N : \Omega \to \mathbb{R}$ are mutually independent and not almost constant, then the 2^N functions of the form $f_J = \prod_{j\in J}(r_j - \mathbb{E}[r_j])$, $J \subseteq [N]$, are linearly independent in the vector space $\mathbb{R}^\Omega$.

(b) In class we have seen how to construct $2N^{\lfloor \frac{d}{2} \rfloor}$ d-wise independent 0/1-valued random variables having the uniform distribution. Here we show that this is best possible up to a constant factor depending only on d.
Let $m(N,d)$ be the sum of the following binomial coefficients:

$$m(N,d) = \begin{cases} \sum_{j=0}^{d/2} \binom{N}{j} & \text{if } d \text{ is even} \\ \sum_{j=0}^{(d-1)/2} \binom{N}{j} + \binom{n-1}{(d-1)/2} & \text{if } d \text{ is odd.} \end{cases}$$

Show that if the (not necessarily 0/1-valued) random variables $r_1, \dots, r_N$ over the sample space Ω are d-wise independent and not almost constant, then the size $|\Omega|$ of the sample space is at least $m(N,d)$ (which is of the order $n^{\lfloor \frac{d}{2} \rfloor}$).

Exercise 2 A set $C \subseteq \{0,1\}^N$ of vectors is called a *binary code* and its elements are called *code words*. We say that a code $C \subseteq \{0,1\}^N$ *corrects up to d errors*, if for any vector $a \in \{0,1\}^N$, there is *at most one* code word which differs from a in at most d bits. Let M be a matrix whose columns are the elements of a d-wise independent N-dimensional linear sample space S of size $|S| = m$, and let

$$C = \{x \in \mathbb{F}_2^N : x^T M = 0\}$$

be the subset defined by the vectors orthogonal to all members of S. Show that C corrects up to $d/2$ errors.

Exercise 3 A family of graphs $\mathcal{G} = \{G_n : n \in S\}$, where $S \subseteq \mathbb{N}$ and $v(G_n) = n$, is called *strongly explicit* if there is an algorithm $\texttt{Alg}_{strong}$ that on inputs $u, v \in V(G_n)$ runs in time polylog(n) and decides whether $uv \in E(G_n)$.
Suppose that addition and multiplication in $\mathbb{F}_q$ can be carried out in constant time. Show that P_q is strongly explicit; that is, there is some constant C such that one can decide if two given vertices u and v are adjacent in $O(\log^C(q))$ time. How long does it take to determine the entire graph P_q?

Exercise 4

(a) Show that if H_1 and H_2 are abelian groups, then for $H = H_1 \times H_2$ we have $\widehat{H} \cong \widehat{H}_1 \times \widehat{H}_2$.

(b) Let $G = C(H, S)$ be a Cayley graph over an abelian group H with generating set $S \subseteq H$. Show that the spectrum of the adjacency matrix of G is the n-element multiset $\{\sum_{s \in S} \chi(s) : \chi \in \widehat{H}\}$. What are the eigenvectors?