CS 599B: Math for TCS, Spring 2022

Exercise Set 3

Due: 10:00PM, Monday February 28, 2022 on Gradescope.

Instructions. You're encouraged to discuss these problems with other students as you solve them, but the written solutions you hand in must be in your own words. Don't worry about polishing the presentation of your solutions; these are primarily intended to keep you thinking about and engaged with the material.

Problem 1 (Sample space lower bounds)**.** In this exercise, you'll prove a sample space size lower bound for k-wise independent distributions on n bits. For simplicity, assume k is even. (Though similar calculations can handle odd k as well.) Think of generating k-wise independent random variables by sampling r uniformly from some sample space Ω and outputting $x_1(r), \dots, x_n(r)$ for some functions $x_1, \dots, x_n : \Omega \to \{-1, 1\}$.

(a) A collection of functions $f_1, \dots, f_m : \Omega \to \{-1, 1\}$ is linearly independent if for reals α_i, we have that $\sum_{i=1}^{m} \alpha_i f_i \equiv 0$ implies $\alpha_1 = \cdots = \alpha_m = 0$. Explain why if $f_1, \dots, f_m$ are linearly independent, $|\Omega| \geq m$.

(b) Let $m = \sum_{j=0}^{k/2} \binom{n}{j}$. Show that there exist m distinct subsets $S_1, \dots, S_m \subseteq [n]$ such that $|S_i \cup S_j| \leq k$ for all $i \neq j$.

(c) Show that if $x_1(r), \dots, x_n(r)$ are k-wise independent, then the parity functions $\chi_{S_1}(x_1(r), \dots, x_n(r)), \dots, \chi_{S_m}(x_1(r), \dots, x_n(r))$ corresponding to the sets you constructed in part (b) are linearly independent.

(d) Conclude a sample space size and seed length lower bound for sampling k-wise independent distributions. How close are these to the parameters of the construction we saw in class?