

## Problem Set 3

## 1 Homework Policy

You are allowed to discuss the problems in groups of two or three, but you must write up the solutions on your own. If you do work with anyone, you should acknowledge your collaborators. Similarly, if you use references such as books, lecture notes, or web pages, you should cite these as well.

## 2 Corrections

1. In problem 3, I defined  $N_k(u)$ .
2. In problem 3, I changed  $d^u$  to  $d^k$ .

### Problem 1: Analysis of random walks

In Lecture 9, we proved that a random walk on an expander that starts at a random vertex is very unlikely to hit a small set often. In this problem, you will consider the chance that the walk is always in some small set. Let  $S$  be a subset of vertices of size at most  $|V|/100$ .

Consider the walk that starts at a random vertex and then takes  $t$  steps. Prove that the probability that it is in  $S$  at all times is at most

$$\left(\frac{1}{5}\right)^{t+1}.$$

### Problem 2: Codes with less randomness

In Lecture 11, we prove that a random linear code of rate  $r$  and length  $n$  is probably asymptotically good. However, we needed  $rn^2$  random bits to generate the code. We would rather do it with  $O(n)$  random bits, and we can.

We will just consider the case of  $r = 1/2$ , so set  $m = n/2$ . We will build a code by exploiting the finite field of  $2^m$  elements. If you don't know what that is, don't worry. Let  $F_{2^m}$  denote the finite field of  $2^m$  elements. There is a simple way of representing each element of  $F_{2^m}$  as a string of  $m$  zeros and ones. For  $f \in F_{2^m}$ , let  $\pi(f) \in \{0, 1\}^m$  denote this representation.

A finite field has two operations: addition and multiplication. They satisfy the following axioms.

1. There exists an identity under addition, called 0, such that  $0 + f = f + 0 = f$  for all  $f \in F_{2^m}$ .
2. There exists an identity under multiplication, called 1, such that  $1f = f1 = f$  for all  $f \in F_{2^m}$ .
3. For every  $f$  there is an element  $-f$  such that  $f + (-f) = 0$ .
4. For every  $f \neq 0$ , there is an element  $f^{-1}$  such that  $ff^{-1} = 1$ .
5. Addition and multiplication are commutative, so  $f + g = g + f$  and  $fg = gf$ .
6. For all  $f, g$  and  $h$ ,

$$f(g + h) = fg + fh.$$

You can deduce for yourself that  $0f = 0$  for all  $f$ .

In our case, addition is very easy to understand: for  $f, g \in F_{2^m}$

$$\pi(f + g) = \pi(f) + \pi(g), \quad \text{and} \quad f + g = \pi^{-1}(\pi(f) + \pi(g)).$$

So, you can really treat the addition as component-wise addition modulo 2 in  $\{0, 1\}^m$ .

You only need to know one thing about multiplication in a finite field: if we fix  $f \in F_{2^m}$  and let  $g$  vary over all elements in  $F_{2^m}$ , then the product  $fg$  will vary over all elements in  $F_{2^m}$ .

For two elements  $f, g \in F_{2^m}$ , define the code  $C_{f,g}$  by

$$C_{f,g}(h) = (\pi(fh), \pi gh).$$

That is, we encode a field element  $h \in F_{2^m}$  by multiplying by  $f$ , multiplying by  $g$ , and concatenating the representations of the results. By the properties of addition proved above, this code is necessarily linear.

Prove that there exists a  $\delta > 0$  so that if  $n$  is sufficiently large and if we choose  $f$  and  $g$  uniformly at random, then the minimum distance of  $C_{f,g}$  is probably at least  $\delta n$ .

### Problem 3: Generalized Ring Graphs

- a. Let  $n$  be an integer and let  $S \subset \mathbf{Z}/n$  be subset of  $|S| = d$  integers modulo  $n$  such that  $g \in S \iff -g \in S$ . Form the Cayley graph on  $V = \mathbf{Z}/n$  with generator set  $S$ . Let  $u \in V$  be any vertex of the graph. Prove that

$$|N^k(u)| \leq d^k,$$

where  $N^k(u)$  is the set of vertices at distance exactly  $k$  from  $u$ .

- b. Prove that for every  $d$  and for every  $\epsilon > 0$ , there exists an  $n_0$  such that for all  $n \geq n_0$ , every  $d$ -regular Cayley graph  $G$  of  $\mathbf{Z}/n$  has

$$\lambda_2(G) \leq \epsilon.$$

That is, we cannot obtain constant-degree expanders from Generalized Ring graphs.

## Problem 4: Awesome Codes

We will treat codes as subsets of  $\{0, 1\}^n$ . We say that a code is *awesome* if its minimum distance is strictly greater than  $n/2$ . That is, if all pairs of codewords differ in more than  $n/2$  bits. We will prove that awesome codes cannot have many codewords. Let  $|C|$  denote the number of codewords in the code  $C$ . We will prove that  $|C| \leq n + 1$ . We will prove this *whether or not  $C$  is a linear code*.

Our proof will use a special matrix  $M$  with both positive and negative entries. The rows and columns of  $M$  are indexed by vectors in  $\{0, 1\}^n$ . The entries of  $M$  are given by

$$M(\mathbf{x}, \mathbf{y}) = n + 1 - 2\text{dist}(\mathbf{x}, \mathbf{y}).$$

So, the diagonals of  $M$  are  $n + 1$ . If you like, you can think of  $M$  as the adjacency matrix of a graph that has positive edge weights, negative edge weights, and self-loops. This is essentially a weighted cayley graph on  $\{0, 1\}^n$ .

- a. Let  $C$  be an awesome code, and let  $\chi_C$  be its characteristic vector. Prove that

$$\chi_C^T M \chi_C \leq (n + 1) |C|.$$

- b. Prove that  $\mathbf{1}$  is an eigenvector of  $M$  of eigenvalue of  $2^n$ , and that all of its other eigenvalues are non-negative. (Hint: there are  $n$  more eigenvalues of  $2^n$ , and all the others are zero).
- c. Prove that

$$\chi_C^T M \chi_C \geq |C|^2.$$

Combining parts *a* and *c*, we may conclude that  $|C| \leq n + 1$ .