

# CMPT 881 - Pseudorandomness: Solutions to Problem Set 1

Valentine Kabanets

November 29, 2004

1. **Random walks and Electrical networks** Let  $G$  be a connected, undirected graph on  $n$  vertices, and let  $s$  and  $t$  be any two distinct vertices of  $G$ . For any vertex  $v$  of  $G$ , let  $p_v$  denote the probability that a random walk on  $G$  starting at the vertex  $v$  will visit  $s$  before visiting  $t$ . (Using a more picturesque language, imagine that  $G$  represents a map of some city. A drunken tourist is trying to get to his hotel, represented by the vertex  $s$ , by performing a random walk in the city. The vertex  $t$  represents a bar. For each point in the city, we are interested in the probability that our tourist will get to his hotel before he gets to the bar (where he would stay all night)).

(a) Let  $\hat{G}$  be the electrical network corresponding to the graph  $G$  (where each edge of  $G$  becomes a unit resistance). For each vertex  $v$  of  $\hat{G}$ , let  $\phi_v$  denote the voltage difference between  $v$  and  $t$ , when a source of one volt is applied to  $\hat{G}$  between  $s$  and  $t$  so that  $\phi_s = 1$  and  $\phi_t = 0$ . Prove that, for each vertex  $v$  of  $G$ ,

$$p_v = \phi_v.$$

(You will need to prove the *uniqueness* of a solution to a certain system of linear equations.)

**Solution:** Let  $d_v$  denote the degree of a vertex  $v$ . For every vertex  $v$  of  $G$  other than  $s$  and  $t$ , we have

$$p_v = \frac{1}{d_v} \sum_{u \in N(v)} p_u,$$

and  $p_s = 1$ ,  $p_t = 0$ .

In the corresponding electrical network, we have  $\phi_s = 1$  and  $\phi_t = 0$ . For every other node  $v$ , we have by Kirchhoff's law that

$$\sum_{u \in N(v)} i_{vu} = 0,$$

where  $i_{vu}$  is the current from  $v$  to  $u$ . Since the resistances are all equal to 1, we have by Kirchhoff's that  $i_{vu} = \phi_{vu}$ , and also  $\phi_{vu} = \phi_v - \phi_u$ . Thus, for every  $v$  other than  $s$  or  $t$ , we have

$$\sum_{u \in N(v)} (\phi_v - \phi_u) = d_v \phi_v - \sum_{u \in N(v)} \phi_u = 0,$$

and so,  $\phi_v = \frac{1}{d_v} \sum_{u \in N(v)} \phi_u$ .

Identifying the variables  $\phi_v$  and  $p_v$ , we see that the two systems of linear equations are identical. Thus it remains to show that this system of linear equations has exactly one solution.

Let  $A$  be the normalized adjacency matrix of  $G$ , and let  $A'$  be the matrix obtained from  $A$  by replacing the rows  $s$  and  $t$  with the all-zero vectors. Then our linear system can be written in the matrix form as  $(I - A')p = a$ , where  $p = (p_1, \dots, p_n)$  is the vector of  $n$  unknowns, and  $a$  is the vector of constants where  $a_s = 1$  and  $a_j = 0$  for all  $j \neq s$ . We'll show that the matrix  $B = I - A'$  has full rank  $n$ . This will immediately give us the existence of a unique solution.

Consider any sequence of coefficients  $\alpha_1, \dots, \alpha_n$  such that  $\sum_{i=1}^n \alpha_i c_i = 0$ , where  $c_i$  is the  $i$ th column-vector of the matrix  $B$ . Note that it must be the case that  $\alpha_s = \alpha_t = 0$ . We'll show that all other  $\alpha_j = 0$  as well.

Indeed, let  $1 \leq M \leq n$  be such that  $\alpha_M$  is the maximal of the  $\alpha_j$ s. Suppose that  $M \neq s, t$ . Consider the  $M$ th row of  $B$ . It follows that  $\alpha_M$  equals the average of  $\alpha_u$  for  $u \in N(M)$ . Since the maximum can equal the average if and only if all  $\alpha_u = \alpha_M$ , we get that  $\alpha_u = \alpha_M$  for all neighbours of  $M$ . Using the fact that  $G$  is connected, the same argument applied to the neighbours of  $M$  shows that  $\alpha_j = \alpha_M$  for all  $j$ , and hence all  $\alpha_j = \alpha_s = 0$  in this case.

Similarly, let  $1 \leq m \leq n$  be such that  $\alpha_m$  is the minimal of  $\alpha_j$ . If  $m \neq s, t$ , we conclude as above that  $\alpha_j = \alpha_m$  for all  $j$ , and hence  $\alpha_j = \alpha_s = 0$  in this case.

If  $M = s$  or  $M = t$ , then we know that  $\alpha_j \leq 0$  for all  $j$ . If  $m = s$  or  $m = t$ , then we know that  $\alpha_j \geq 0$  for all  $j$ . Thus, if  $M = s$  or  $M = t$  and if  $m = s$  or  $m = t$ , then we get  $0 \leq \alpha_j \leq 0$  for all  $j$ , and so  $\alpha_j = 0$  in this case as well. Thus we have proved that the only linear combination of columns of  $B$  that is equal to zero is the trivial all-zero combination, and so  $B$  has full rank.

- (b) Let  $G$  be a graph on  $n$  vertices  $1, 2, \dots, n$  lying on a line, i.e., with edges  $(i, i + 1)$ , for  $1 \leq i \leq n - 1$ . Using the connection between random walks and electrical networks established in the previous question, compute  $p_i$  for each  $1 \leq i \leq n$  (i.e., give a formula for  $p_i$ ).

**Solution:**  $p_i = \frac{n-i}{n-1}$  (assuming that  $s = 1$  and  $t = n$ ).

- (c) Generalize the conclusion of question (i) above to the case of *weighted* graphs, where each edge  $e$  of  $G$  has some weight  $w_e$ . A random walk on weighted graphs is defined as follows: If you are at a vertex  $v$  that is connected to  $d$  neighbours with edges  $e_1, \dots, e_d$  having weights  $w_1, \dots, w_d$ , respectively, then the probability of moving to the  $i$ th neighbour is  $w_i/W_v$ , where  $W_v = \sum_{j=1}^d w_j$  is the total weight of the edges leaving  $v$ .

**Solution:** The solution is analogous to that of item (a) above, when we consider the electrical network with resistances  $r_{uv} = 1/w_{uv}$ . Instead of the normalized adjacency matrix  $A$  of  $G$ , we need to consider the matrix of corresponding transition probabilities in the weighted graph: the row  $v$  will have  $w_u/W_v$  in position  $u$  for  $u \in N(v)$  and 0 everywhere else. The rest of the argument is the same as in item (a).

2. **Existence of expanders** A  $d$ -regular bipartite graph on  $n + n$  vertices is a bipartite graph on the vertex set  $L \cup R$ , where  $|L| = |R| = n$  and  $L \cap R = \emptyset$ , such that each vertex in  $L$  has  $d$  neighbours in  $R$  (and no neighbours in  $L$ ), and each vertex in  $R$  has  $d$  neighbours in  $L$  (and no neighbours in  $R$ ). Using the probabilistic method, prove that for every  $d \geq 3$ , there is a family of  $d$ -regular bipartite graphs on  $n + n$  vertices that are  $(\alpha n, A)$ -expanders, for some constant  $\alpha > 0$  and constant  $A > 1$ , and all sufficiently large  $n$ . Try to make  $A$  as close to the degree  $d$  of the graph as possible (say,  $A = d - 1.01$ ), at the expense of making  $\alpha$  a very small constant. Note that your expander graph must “expand” every small subset  $S$  of vertices by a factor  $A$ , where  $S$  may contain vertices from both  $L$  and  $R$ .

**Solution:** We pick our random bipartite graph as follows. We independently pick  $d$  permutations  $\sigma_1, \dots, \sigma_d$  on  $[n]$ , and define for each  $i \in L$  the  $d$  edges to  $R$  as  $(i, \sigma_1(i)), \dots, (i, \sigma_d(i))$ . Clearly, the resulting graph will be  $d$ -regular bipartite (both the left degree and the right degree will be equal to  $d$ ). We'll show that with nonzero probability, a  $d$ -regular graph chosen this way will be  $(\alpha n, d - 1.01)$ -expander.

We'll show that the probability that such a graph is a *left* expander is at least  $3/4$ . The same proof will show that the probability that we get a *right* expander is also at least  $3/4$ . Hence, we conclude that we get an expander with probability at least  $1/2$ .

To prove that a random  $G$  is a left  $(\alpha n, d - 1.01)$ -expander, fix any  $k \leq \alpha n$  and denote by  $p_k$  the probability that there is a set  $S \subseteq L$  of size  $k$  such that  $|N(S)| < (d - 1.01)k$ . By the union bound,  $p_k \leq \binom{n}{k} \Pr[\text{fixed set } S \text{ of size } k \text{ is s.t. } |N(S)| < (d - 1.01)k]$ ; the latter probability is equal to the probability of having at least  $1.01k$  repeats among the  $kd$  neighbours of  $S$  when those neighbours are chosen in our  $d$  random and independent permutations.

Consider the  $d$  permutations restricted to the set  $S$ . The first permutation creates no repeats, yielding  $k$  distinct neighbours of  $S$  in  $R$ . The second permutation gives a repeat at the  $i$ th vertex of  $S$  with probability  $k/(n - (i - 1)) \leq k/(n - i)$  (since some of the  $k$  vertices in  $R$  chosen by the first permutation can be picked by the second permutation as the value of the  $i$ th vertex in  $S$  with probability  $k/(n - (i - 1))$ ). Similarly, the  $d$ th permutation creates a repeat at the  $i$ th vertex of  $S$  with probability  $(d - 1)k/(n - (i - 1)) \leq (d - 1)k/(n - i)$ . So the maximal probability of a repeat is at most  $(d - 1)k/(n - k) \leq dk/n$  for  $\alpha < 1/d$ .

Thus, the probability of having more than  $1.01k$  repeats is at most  $\binom{kd}{1.01k} (kd/n)^{1.01k}$ , and so,

$$p_k \leq \binom{n}{k} \binom{kd}{1.01k} (kd/n)^{1.01k}.$$

Upperbounding the binomial coefficient  $\binom{m}{i} \leq (me/i)^i$  and using the fact that  $k \leq \alpha n$ , we get that

$$p_k \leq \frac{e^{2.01k} d^{2.02k} \alpha^{0.01k}}{1.01^{1.01k}},$$

which is less than  $(1/5)^k$  for sufficiently small constant  $\alpha$ .

Finally, by the union bound, the probability that there is a “bad” set  $S$  of some size at most  $\alpha n$  is at most  $p_1 + \dots + p_{\alpha n} \leq \sum_{i=1}^{\alpha n} (1/5)^i \leq \frac{1/5}{1 - 1/5} = 1/4$ , as required.

**3. Eigenvalues of special graphs** For each of the following graphs  $G$  with the normalized adjacency matrices  $A$ , prove the correctness of the formula for the eigenvalues of  $A$ .

- (a)  $G = K_n$ , a complete graph on  $n$  vertices. The eigenvalues are  $\lambda_1 = 1, \lambda_2 = \dots = \lambda_n = -\frac{1}{n-1}$ .

**Solution:** Let  $J$  be the all-one  $n \times n$  matrix, and let  $I$  be the identity  $n \times n$  matrix. Then the normalized adjacency matrix of  $K_n$  is  $\frac{1}{n-1}(J - I)$ . The matrix  $I$  has all  $n$  eigenvalues equal to 1, and any non-zero vector is an eigenvector of  $I$ . The matrix  $J$  has the all-one vector as an eigenvector corresponding to the eigenvalue  $n$ . Since  $J$  is symmetric, all the other  $n - 1$  eigenvectors of  $J$  must be orthogonal to the all-one vector. But, any vector  $v \perp (1, \dots, 1)$  is such that  $Jv = 0$ , and so all the other  $n - 1$  eigenvalues of  $J$  are 0s. Thus, the eigenvalues of  $\frac{1}{n-1}(J - I)$  are  $(n - 1)/(n - 1) = 1$  (corresponding to the eigenvector  $(1, \dots, 1)$ ), and  $(0 - 1)/(n - 1) = -1/(n - 1)$  (corresponding to all the other eigenvectors orthogonal to  $(1, \dots, 1)$ ).

- (b)  $G = Q_n$ , an  $n$ -dimensional cube, i.e., a graph on vertices  $V = \{v \mid v \in \{0, 1\}^n\}$ , where  $u, v \in V$  are connected by an edge iff  $u$  and  $v$  differ in exactly one coordinate (the Hamming distance between  $u$  and  $v$  is exactly one). The eigenvalues are  $\lambda_k = 1 - \frac{2k}{n}$ , for  $k = 0, 1, \dots, n$ , with multiplicities  $\binom{n}{k}$ . [Hint: Consider the set of vectors  $B = \{\chi_v \mid v \in \{0, 1\}^n\}$ , where the  $u$ th coordinate of  $\chi_v$  is  $\chi_v(u) = (-1)^{(v,u)}$ ; here  $(u, v) = \sum_{i=1}^n u_i v_i \pmod 2$  is the inner product of  $u$  and  $v$  modulo 2. Prove that  $B$  is an orthogonal basis of the  $2^n$ -dimensional real space  $\mathbb{R}^{2^n}$ . Then consider what happens when the adjacency matrix of  $Q_n$  is multiplied by a vector  $\chi_v$ , for each  $v \in \{0, 1\}^n$ .]

**Solution:** For any  $u, v \in \{0, 1\}^n$  such that  $u \neq v$ , we have  $\sum_{w \in \{0, 1\}^n} \chi_u(w) \chi_v(w) = \sum_{w \in \{0, 1\}^n} (-1)^{(u \oplus v, w)}$ , where  $u \oplus v$  is the bitwise XOR of  $u$  and  $v$ . Since  $u \neq v$ , we have  $u \oplus v \neq 0$ . Note that for any nonzero  $n$ -bit binary string  $x$ , exactly half of all  $n$ -bit strings  $y$  are such that  $(x, y) = 0$  while the other half are such that  $(x, y) = 1$ . This means that  $\sum_{w \in \{0, 1\}^n} (-1)^{(u \oplus v, w)} = 0$ , and so  $\chi_v \perp \chi_u$  for all  $u \neq v$ .

Next we show that each  $\chi_u$  is an eigenvector of the normalized adjacency matrix  $A$  of  $Q_n$ . For each  $1 \leq i \leq n$ , denote by  $e_i$  the  $n$ -bit vector which has 1 in position  $i$ , and zero everywhere else. Then the  $v$ th component of  $A\chi_u$  is equal to  $(1/n) \sum_{i=1}^n \chi_u(v \oplus e_i) = (1/n) \sum_{i=1}^n (-1)^{(u, v \oplus e_i)} = (-1)^{(u, v)} (1/n) \sum_{i=1}^n (-1)^{(u, e_i)}$ . The latter is  $\chi_u(v) (1/n) (\# \text{ 0s in } u - \# \text{ 1s in } u) = \chi_u(v) (1 - \frac{2}{n} * \# \text{ 1s in } u)$ . So, the vector  $\chi_u$  is an eigenvector of  $A$  with the corresponding eigenvalue  $1 - 2k/n$ , where  $k$  is the number of 1s in the vector  $u$ .

- (c) **[Bonus]**  $G = C_n$ , a cycle on  $n$  vertices (i.e.,  $1 \rightarrow 2 \rightarrow 3 \rightarrow \dots \rightarrow n \rightarrow 1$ ). The eigenvalues are  $\lambda_k = \cos \frac{2\pi k}{n}$ , for  $k = 0, 1, \dots, n-1$ .

**Solution:** Consider the directed cycle  $1 \rightarrow 2 \rightarrow 3 \rightarrow \dots \rightarrow n \rightarrow 1$ . Let  $A$  be its (non-normalized) adjacency matrix. Then  $A^t$  is the adjacency matrix of the directed cycle  $1 \rightarrow n \rightarrow n-1 \rightarrow \dots \rightarrow 2 \rightarrow 1$ . The adjacency matrix of the graph  $C_n$  will be  $B = A + A^t$ , and the normalized adjacency matrix of  $C_n$  will be  $\frac{1}{2}B$ . We'll compute the eigenvalues and eigenvectors of  $A$  and  $A^t$ . We'll see that they share the same set of eigenvectors  $v_1, \dots, v_n$ . If  $\lambda_i$  is the eigenvalue of  $A$  corresponding to the eigenvector  $v_i$ , and if  $\lambda'_i$  is the eigenvalue of  $A^t$  corresponding to the same eigenvector  $v_i$ , then  $\lambda_i + \lambda'_i$  is the eigenvalue of  $A + A^t$ , and  $(\lambda_i + \lambda'_i)/2$  is the eigenvalue of  $\frac{1}{2}B$ .

It is not hard to see that the determinant of  $(A - \lambda I)$  is  $(-\lambda)^n + (-1)^{n-1}$ . So the eigenvalues of  $A$  must satisfy the equation  $\lambda^n - 1 = 0$ . It follows that the eigenvalues of  $A$  are all the  $n$ th roots of unity  $1, \omega, \omega^2, \dots, \omega^{n-1}$  where  $\omega = e^{2\pi i/n}$  is the primitive  $n$ th root of unity.

Consider an eigenvector  $v_j = (x_0, \dots, x_{n-1})$  of  $A$  corresponding to the eigenvalue  $\lambda_j = \omega^j$ , for  $0 \leq j \leq n-1$ . Note that by the definition of the matrix  $A - \lambda I$  we must have  $x_i = \lambda_j x_{i-1}$  for  $1 \leq i \leq n-1$ . Setting  $x_0 = 1$ , we get  $v_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})$ , for every  $0 \leq j \leq n-1$ .

Similarly, consider an eigenvector  $u_j = (y_0, \dots, y_{n-1})$  of  $A^t$  corresponding to the eigenvalue  $\lambda_j = \omega^j$ , for  $0 \leq j \leq n-1$ . We get that  $y_{i-1} = \lambda_j y_i$ , or equivalently,  $y_i = \lambda_j^{-1} y_{i-1}$  for  $0 \leq j \leq n-1$ . Again, setting  $y_0 = 1$ , we get  $u_j = (1, \omega^{-j}, \omega^{-2j}, \dots, \omega^{-(n-1)j})$ .

Finally, note that the eigenvector  $u_{n-j}$  corresponding to the eigenvalue  $\lambda_{n-j} = \omega^{n-j} = \omega^{-j}$  (note that  $\omega^n = 1$ ) will be the vector  $v_j$ . So, the eigenvector  $v_j$  has the eigenvalue  $\omega^j$  in  $A$ , and  $\omega^{-j}$  in  $A^t$ . Hence, the  $j$ th eigenvalue  $\mu_j$  of  $\frac{1}{2}(A + A^t)$  is  $\frac{1}{2}(\omega^j + \omega^{-j}) = \frac{1}{2}(e^{2\pi i j/n} + e^{-2\pi i j/n})$ . Using the identity  $e^{i\phi} = \cos \phi + i \sin \phi$ , we get that  $\mu_j = \frac{1}{2}(\cos(2\pi j/n) + i \sin(2\pi j/n) + \cos(-2\pi j/n) + i \sin(-2\pi j/n))$ . Since  $\cos(-\phi) = \cos \phi$  and  $\sin(-\phi) = -\sin \phi$ , we get that  $\mu_j = \cos(2\pi j/n)$ .