Problems

22/02/11

1. (basic) Let F_q be a finite field. Prove that $\prod_{\alpha \in \mathrm{F}^*}(x-\alpha) = x^{q-1} - 1$.
2. (basic) Let F_q be a finite field of odd characteristic. An element $x \in \mathrm{F}_q^*$ is a *quadratic residue* if there exists $y \in \mathrm{F}_q$ such that $x = y^2$. What is the number of quadratic residues in F_q? Prove that the set of quadratic residues is a multiplicative group.
3. (simple) Let F be a finite field. What is the expected number of roots of a random univariate polynomial of degree k over F ?
4. (basic) We represent F_{16} as $\mathrm{F}_2[X](\text{mod } X^4 + X + 1)$. X is a generating element for F_{16}^*. Below you can find a table relating the vector space representation to powers of X. Find how many elements generate F_{16}^*. How many elements generate F_q^* for an arbitrary prime power q?

$Power$	$Element$	$Vectorspacerepresentation$
0	0	$(0,0,0,0)$
$X^0 = X^{15} = 1$	1	$(0,0,0,1)$
X	X	$(0,0,1,0)$
X^2	X^2	$(0,1,0,0)$
X^3	X^3	$(1,0,0,0)$
X^4	$1+X$	$(0,0,1,1)$
X^5	$X+X^2$	$(0,1,1,0)$
X^6	X^2+X^3	$(1,1,0,0)$
X^7	$1+X+X^3$	$(1,0,1,1)$
X^8	$1+X^2$	$(0,1,0,1)$
X^9	$X+X^3$	$(1,0,0,1)$
X^{10}	$1+X+X^2$	$(0,1,1,1)$
X^{11}	$X+X^2+X^3$	$(1,1,1,0)$
X^{12}	$1+X+X^2+X^3$	$(1,1,1,1)$
X^{13}	$1+X^2+X^3$	$(1,1,0,1)$
X^{14}	$1+X^3$	$(1,0,0,1)$

5. (basic) Give an efficient algorithm (polynomial in the input length) that given a degree m polynomial $E(X)$ that is irreducible over F_p, and a non-zero element $x \in \mathrm{F}_q = F_p[X](\bmod E)$, finds x^{-1}.

07/03/11

6. Prove Proposition 4, Lemma 5 and Propositions 6 and 7 of [Dvir, Kopparty, Saraf, Sudan].
7. Prove the generalized Schwartz-Zippel lemma (Lemma 8 in the above paper).
8. (basic) Let X, Y be distributions over Λ. Prove that $|X - Y|_1 = \frac{1}{2} Max_{S \subseteq \Lambda}[X(S) - Y(S)]$.

9. (basic) Let X, Y be distributions over Λ_1. Let f be any probabilistic function mapping Λ_1 to Λ_2. Prove that $|f(X) - f(Y)|_1 \le |X - Y|_1$.

10. (moderate) Prove that any k-source X can be expressed as a convex combination of flat sources over 2^k elements.

11. Let A be a distribution over Λ. Prove that if A is not ϵ-close to a k-source then there exists a subset $S \subseteq \Lambda$ of cardinality at most 2^k such that $\Pr_{a \in A}[a \in S] \ge \epsilon$.

14/03/11 - Mandatory

In class we defined and constructed mergers. In this question I ask you to complete the proof. Feel free to consult the paper, but please write the solution yourself (photocoping the paper does not count).

12.
    - Define a (k, ϵ) merger $E : (\{0,1\}^m)^n \times \{0,1\}^t \to \{0,1\}^m$.
    - Describe the construction of the merger $E : (\{0,1\}^m)^n \times \{0,1\}^t \to \{0,1\}^m$ we gave in class.
    - Prove that E is a $((1-\delta)k, \epsilon)$ merger when $t \ge \frac{1}{\delta} log(\frac{8n}{\epsilon})$.

14/03/11

13. Let $G = (V, E)$ be an undirected graph over n vertices with transition matrix A. Prove (or recall) that $(I + A)^t[i, j] > 0$ iff there is a path of length at most t from i to j in G.
    - Give an $O(\log^2 n)$ space algorithm for computing A^n.
    - Conclude that $STCON \in Space(\log^2 n)$ and $NL \subseteq Space(\log^2 n)$

14. Prove that $BPL \subseteq Space(\log^2 n)$

15. Now we slightly strengthen the mixing lemma we gave in class. If you don't solve it yourself, you can find a proof, e.g., in http://www.cs.yale.edu/homes/spielman/eigs/lect9.pdf.

    Let $G = (V, E)$ be a D regular, undirected graph over N vertices, and $A, B \subseteq V$. For $X \subseteq V$ let $\rho(X) = |X|/|V|$ and $\overline{X} = V \setminus X$, i.e., the set complement of X. Prove that:

    $$|E(A, B) - \rho(A)\rho(B)DN| \le \overline{\lambda} N \sqrt{\rho(A)\rho(\overline{A})\rho(B)\rho(\overline{B})}.$$

16. Prove Tanner inequality: under the above conditions, for every $X \subseteq V$,

    $$|\Gamma(X)| \ge \frac{D^2|X|}{\overline{\lambda}^2 + \frac{|X|}{N}(D^2 - \overline{\lambda}^2)}.$$

17. Prove that the first eigenvalue of D-regular undirected graphs is 1.

18. Let G be a regular, undirected graph. Prove that the number of connected components of G equals the dimension of its 1-eigenspace.

19. Prove that if λ is an eigenvalue of an undirected *bipartite* graph, then do does $-\lambda$. Prove that a D-regular, undirected connected graph G is bipartite iff $\lambda_n = -1$. What is the associated eigenvector v_n ?

20. Let H be a group and S a set of generators. The Caylely graph $C(H, S)$ is defined as follows: The vertices are labeled with elements of H, and (a, b) is an edge iff $a = bs^{-1}$ for some $s \in S$.

    - What is $C(Z_n, \{1, -1\})$?
    - What is $C(Z_2^n, \{e_1, , e_n\})$, where e_i has 1 in the i'th coordinate and 0 otherwise.

    We will later on (Question 31) compute the spectrum of these graphs.

21. (basic) Let G be an undirected graph, A its adjacency matrix. Prove that: $\lambda_2(A) = \max_{v \perp 1} \frac{<v,Av>}{<v,v>}$.

22. Prove that for any undirected graph G, $h(G) \geq (d - \lambda_2)/2$.
    Remark: Using the mixing lemma, you can deduce the same but with $\overline{\lambda} = \min\{-\lambda_n, \lambda_2\}$ replacing λ_2.

23. Prove that in any D-regular, undirected graph with N vertices, if $D \leq N/2$ then $\overline{\lambda} = \min\{-\lambda_n, \lambda_2\} \geq \sqrt{D/2}$.
    Hint: Calculate $Tr(A^2)$ in two different ways.

21/03/11

24. (basic) Prove that the operator norm is a norm, and that if A is symmetric then $\|A\| = \lambda_1(A)$.

25. (basic) Let A be a matrix. Define $\|A\| = sup_{v \neq 0} \frac{\|Av\|_1}{\|v\|_1}$. Prove:

    - $\|A\| = max_i \|A_i\|_1$, where A_i is the i'th row of A.
    - $\|A + B\| \leq \|A\| + \|B\|$
    - $\|cA\| = |c|\|A\|$, $\|A\| = 0$ iff $A = 0$
    - $\|AB\| \leq \|A\|\|B\|$
    - If A is a transition probability matrix then $\|A\| = 1$.

26. Calculate the seed length of Nisan's generator fooling branching programs of length n, width n and alphabet n. I.e., find the constant c hiding in the $O(\log^2 n)$ notation. The purpose of this of this exercise is to force you to completely follow the proof.

27. Can you find an ordering of the blocks of Nisan's generator that does not fool log-space machines?

12/04/11

28. Look at the paper "On Read-once vs. Multiple Access to Randomness in Logspace" by N. Nisan (can be found at http://www.cs.huji.ac.il/ noam/papers.html) and give an alternative, simpler proof of Theorem 1 there, based on what we have seen in class.

29. Let n be an integer and G be the group $(Z_n, + \bmod n)$.

- Prove that there are exactly $|G|$ characters of G.
- Define a multiplication operator on the characters, and prove that the characters of G form a group $\widehat{G}$ under this product.
- Prove that $\widehat{G}$ is isomorphic to G.

30. solve question 29 for:

- $G = Z_n \times Z_m$, for any two integers n and m,
- $G = Z_2^n$, for any integer n,
- Any Abelian group G.

31. Let $C(H, S)$ be as in question 20.

- Prove that if H is Abelian then the characters of H form an orthonormal basis for $C(H, S)$.
- Calculate the eigenvalues and the spectral gap of the two Cayley graphs given in question 20.

13/04/11 - Mandatory

32. Prove (using the probabilistic method) that there exist constants c_1 and c_2 such that for every n there exists a function $E : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ that is a (k, ϵ) strong extractor, for

- $t = \log(n-k) + 2\log(\frac{1}{\epsilon}) + c_1$, and,
- $m = k - 2log(\frac{1}{\epsilon}) - c_2$.

31/05/11

33. Two norm one vectors $v_1, v_2 \in R^d$ are almost orthogonal if $| < v1|v2 > | \leq \epsilon$. Show how to convert an (ℓ, a) design $S_1, \ldots, S_m \subseteq [t]$ into:

- A set of m nearly orthogonal vectors.
- A binary error correcting code of length t with m codewords and large distance.

34. Prove that for every $\ell, a \geq 1$, there exists an (ℓ, a) design $S_1, \ldots, S_m \subseteq [t]$ with $t = O(\ell^2/a)$ and $m = 2^{\Omega(a)}$.

35. How many orthogonal vectors can one put into R^d? How many ϵ-almost orthogonal vectors can you put into R^d? Upper bound, Lower bound (is it tight?), constructive bound?

For next weeks

36. n coins are laid covered on a table, $k < n/3$ of which are pure gold and the rest copper, and you are told to uncover and take $2n/3$ coins!!! You are allowed to use any algorithm, no matter what its complexity is, but the adversary knows your algorithm and places the gold coins based on your algorithm.

    - Show that if you are deterministic, you get no gold.
    - Show that if you use n random coins you can almost certainly get $\Omega(k)$ gold coins.
    - Show that with $O(logn)$ random coins, you can guarantee $\Omega(k)$ gold coins with probability at least $1 - O(1/k)$.
    - Show that for $\epsilon \geq 1/k$, with $O(loglogn + log(1/\epsilon))$ coins, you can guarantee $\Omega(k)$ gold coins with probability at least $1 - \epsilon$.

37. Prove that a k-wise independent distribution $X = X_1, ..., X_n$ over $\{0,1\}^n$ with support S must have $|S| \geq \Omega(n^{k/2})$.

    Guided solution:

    - Prove that X has 0-bias with regard to any linear test $\alpha \in \{0,1\}^n$ of size $0 < |\alpha| \leq k$.
    - Let A be the $s \times n$ matrix having the elements of S as rows. For any test α define $v = v(\alpha) \in \{1,-1\}^s$ by $v_i = 1$ if $(A\alpha)_i = 0$ and -1 otherwise. Prove that $\{\ v(\alpha) \mid 0 < |\alpha| \leq k/2\}$ is a set of orthogonal vectors.
    - Conclude that $|S| \leq B(k/2, n)$, where $B(r,n)$ is the number of words of weight at most r in the n dimensional Boolean cube.