Problems

Topics in Pseudorandomness and Complexity (Spring 2018)
Rutgers University
Swastik Kopparty

Do any two problems. Due April 26, 2018, in class.

1. Let G be an undirected graph. Let A be the adjacency matrix of G. Let D be the diagonal matrix whose (i, i) entry equals the degree of the ith vertex. Recall that $M = AD^{-1}$ is the random walk matrix of G.

   Show that the probability distribution p^* which picks a vertex with probability proportional to its degree is stable under M.

   If A is nonbipartite and connected, show that the distribution of the tth step of the simple random walk (starting at an arbitrary vertex) on G converges to p^* as $t \to \infty$.

   How large a t makes the above distribution to ϵ-close in statistical distance to p^*?

   Hint: Define $P = D^{-1/2}AD^{-1/2}$. Note that P is symmetric, and thus has a basis of orthonormal eigenvectors. Express M^t in terms of P^t. Show that the top eigenvalue of P is 1. When is there another eigenvalue with absolute value 1?

2. Below is a collection of facts/problems related to finite fields. Try to verify them yourself or look them up.

   (a) Let p be prime. Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ along with operations addition and multiplication mod p. Every integer can be treated as an element of $\mathbb{F}_p$ (by taking the remainder after dividing by p).

   All of $\mathbb{F}_p$ forms a group under addition. The nonzero elements of $\mathbb{F}_p$, denoted $\mathbb{F}_p^*$ form a group under multiplication. Both groups are commutative.

   (b) For each $a \in \mathbb{F}_p$, we have $a^p = a$. If $a \neq 0$, then $a^{p-1} = 1$.

   (c) Let $\mathbb{F}_p[X]$ be the set of polynomials with $\mathbb{F}_p$ coefficients. Then the division theorem holds in $\mathbb{F}_p[X]$, and thus every element of $\mathbb{F}_p[X]$ can be uniquely factorized into irreducible polynomials.

   (d) The remainder theorem holds in $\mathbb{F}_p[X]$. Thus $X^p - X = \prod_{\alpha \in \mathbb{F}_p}(X - \alpha)$.

   (e) For each integer d, the number of $a \in \mathbb{F}_p^*$ satisfying $a^d = 1$ is at most d. Combining this with the fact that $\mathbb{F}_p^*$ is commutative, this implies that $\mathbb{F}_p^*$ is cyclic (i.e., there is an element $g \in \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$.

   Not every element of $\mathbb{F}_p^*$ generates $\mathbb{F}_p^*$. Look at the cases $p = 7, 13$ and find a generator for $\mathbb{F}_p^*$ in each case.

   (f) Suppose p is an odd prime. Then exactly 1/2 the elements of $\mathbb{F}_p^*$ are perfect squares. If $a \in \mathbb{F}_p^*$, then $a^{(p-1)/2}$ equals either 1 or -1, depending on whether a is a perfect square or not.

   (g) Generalize the above to perfect dth powers. Note that if d is relatively prime to $p - 1$ then every element of $\mathbb{F}_p^*$ is a perfect dth power.

(h) Let $f(X)$ be an irreducible polynomial of degree d in $\mathbb{F}_p[X]$. We can consider the set $\mathbb{F}_p[X]/f(X)$ of polynomials modulo $f(X)$. Every polynomial is equivalent modulo $f(X)$ to a unique polynomial of degree $< d$. Thus there are p^d residue classes. Addition and multiplication of polynomials is compatible with reducing mod $f(X)$. Every nonzero element of $\mathbb{F}_p[X]/f(X)$ has a multiplicative inverse (this is where irreducibility of $f(X)$ is used). Thus $\mathbb{F}_p[X]/f(X)$ is a field of cardinality p^d.

The relationship between $\mathbb{Z}$, the prime p and the field $\mathbb{Z}/p$ is entirely analogous to the relationship between $\mathbb{F}_p[X]$, the irreducible $f(X)$ and the field $\mathbb{F}_p[X]/f(X)$.

(i) The field $\mathbb{F}_p[X]/f(X)$ is a d-dimensional vector space over the field $\mathbb{F}_p$. We denote this field $\mathbb{F}_{p^d}$. It is tricky to prove but true that any two fields of cardinality p^d are isomorphic fields. Thus there is a unique such field. If n is an integer not of the form p^d for p prime, then there does not exist a finite field of cardinality n. Thus whenever we talk of the finite field $\mathbb{F}_q$, we will insist that q be a prime power.

(j) Note that the above construction of $\mathbb{F}_{p^d}$ required the existence of an irreducible polynomial of degree d over $\mathbb{F}_p$. Such polynomials exist for every d! Try to show this.

(k) Construct the fields $\mathbb{F}_8$ and $\mathbb{F}_9$.

(l) Note that the field $\mathbb{F}_{p^d}$ is not isomorphic to the ring $\mathbb{Z}/p^d$.

(m) Many of the facts you proved about the field $\mathbb{F}_p$ also hold for $\mathbb{F}_{p^d}$. Polynomials over $\mathbb{F}_{p^d}$ can be defined, and they have nice properties. The multiplicative group $\mathbb{F}_{p^d} \setminus \{0\}$ is cyclic. Etc. To prove all these properties, you need not use the explicit construction of $\mathbb{F}_{p^d}$ described above. It suffices to just use the fact that $\mathbb{F}_{p^d}$ is a field of cardinality p^d.

(n) $X^{p^d} - X = \prod_{\alpha \in \mathbb{F}_{p^d}} (X - \alpha)$.

3. Let q be a prime power. For each $\alpha \in \mathbb{F}_q$, let $v_\alpha \in \mathbb{F}_q^k$ be the vector $(1, \alpha, \alpha^2, \ldots, \alpha^{k-1})$.

(a) Show that for any k distinct $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_q$, the vectors $v_{\alpha_1}, v_{\alpha_2}, \ldots, v_{\alpha_k}$ are linearly independent.

(b) Now suppose $q = 2^t$. Using the fact that $\mathbb{F}_q$ a vector space of dimension t over $\mathbb{F}_2$, we get a $\mathbb{F}_2$-linear isomorphism $E : \mathbb{F}_q^k \to \mathbb{F}_2^{tk}$. Show that the vectors $\tilde{v}_\alpha = E(v_\alpha) \in \mathbb{F}_2^{tk}$ are such that any k of them are linearly independent over $\mathbb{F}_2$.

Let $n = 2^t$. Show that the k-wise independent distribution over $\mathbb{F}_2^n$ that we get from these vectors has seed length $k \log n$.

(c) Again suppose $q = 2^t$, and let k be even. Let $u_\alpha \in \mathbb{F}_q^{k/2}$ be the vector $(\alpha, \alpha^3, \alpha^5 \ldots, \alpha^{k-1})$. Let $\tilde{u}_\alpha = E(u_\alpha) \in \mathbb{F}_2^{tk/2}$. Show that if $\alpha_1, \ldots, \alpha_k$ are such that $\tilde{u}_{\alpha_1}, \ldots, \tilde{u}_{\alpha_k}$ are linearly dependent over $\mathbb{F}_2$, then $\tilde{v}_{\alpha_1}, \ldots, \tilde{v}_{\alpha_k}$ are linearly dependent over $\mathbb{F}_2$. Thus conclude that every set of k vectors from the collection $\{\tilde{u}_\alpha \mid \alpha \in \mathbb{F}_q\}$ are linearly independent over $\mathbb{F}_2$.

Let $n = 2^t$. Show that the k-wise independent distribution over $\mathbb{F}_2^n$ that we get from these vectors has seed length $\frac{k}{2} \log n$.

This construction is also known as the "BCH code", after R. C. Bose, D. Ray-Chaudhuri and Hocquenghem.

(d) Let k be a constant. Suppose $s < \frac{k}{2} \log n - \Omega(1)$. Show that if we take any collection of n vectors in $\mathbb{F}_2^s$, then some k of them are linearly dependent.

Thus the above construction of vectors is essentially as large as possible.

4. In this exercise we will prove a lower bound on the seed length required for generating k-wise independent random bits.

   (a) Show that a distribution μ over $\mathbb{F}_2^n$ is k-wise independent if and only if $\hat{\mu}(S) = 0$ for all $S \subseteq [n]$ with $1 \leq |S| \leq k$.
   (b) Let k be a constant. Let $X \subseteq \mathbb{F}_2^n$ with $|X| = o(n^{\lfloor k/2 \rfloor})$. Show that for $d = \lfloor k/2 \rfloor$, there is a function $f : \mathbb{F}_2^n \to \mathbb{R}$ which satisfies:

      i. f is not identically 0.
      ii. $\hat{f}(S) = 0$ for each $|S| > d$.
      iii. $f(x) = 0$ for each $x \in X$.

      Use this to show that any k-wise independent distribution over $\mathbb{F}_2^n$ has support at least $\Omega(n^{k/2})$. Thus the BCH construction of a k-wise independent distribution has essentially optimal seed length.

5. Suppose $X, Y \in \{0,1\}^n$ are *independent* random variables with $H_\infty(X), H_\infty(Y) \geq 0.51n$.

   Let Z be the random variable $\langle X, Y \rangle \in \{0,1\}$ (where the inner product is over $\mathbb{F}_2$).

   Show that Z is $2^{-\Omega(n)}$-close to a uniformly distributed bit.

   This is an example of a "two-source extractor": it extracts nearly pure randomness from two independent weak sources of randomness.

   Hint: Let f, g be the probability distributions of X, Y respectively. Consider the Fourier transforms of f, g, and express the output distribution in terms of that.

6. Show that there do not exist (k, ϵ)-extractors $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for $k = n/2$, $\epsilon = 0.01$, $d < \log n + \log \frac{1}{\epsilon}$ and $m \geq 1$.

7. A bit-fixing source of weak randomness is a $\{0,1\}^n$-valued random variable X for which there exists a subset $S \subseteq [n]$ of coordinates for which: $X|_S$ is uniformly distributed, and $X|_{[n]\setminus S}$ is constant. Note that $|S|$ is the min-entropy of such a bit-fixing source.

   (a) Show that there exist *deterministic* extractors for bit-fixing sources. Concretely, show that for every $k \gg \log n$, $m < k - 2\log(1/\epsilon) - O(1)$, there exists a function $E : \{0,1\}^n \to \{0,1\}^m$ such that for every bit-fixing source X with $H_\infty(X) \geq k$, we have $E(X)$ is ϵ-close to U_m. Such an E is called a (k, ϵ) bit-fixing extractor.
   (b) Show that if $m = k^{0.49}$, the map $E : \{0,1\}^n \to \{0, 1, \ldots, m-1\}$ given by:

   $$E(x) = x \mod m$$

   is a $(k, o(1))$ bit-fixing extractor. Here the n-bit string x is viewed as an integer in base 2, and $x \mod m$ is the remainder when the integer x is divided by m.