A Theorist's Toolkit **CMU 15-751*, Fall 2016**

PROBLEM SET 5

Due: Noon, Monday Oct. 24, email the pdf to toolkit2016homework@gmail.com

Homework policy: Exactly the same as last time.

1. Let p be a prime. We can think of $\mathbb{F}_{p^\ell}$ as a vector space of dimension ℓ over the field $\mathbb{F}_p$ (make sure you see/know why).

   (a) Fix a particular $\alpha \in \mathbb{F}_{p^\ell}$ and consider the function $M_\alpha : \mathbb{F}_{p^\ell} \to \mathbb{F}_{p^\ell}$ defined by $M_\alpha(\beta) = \alpha\beta$. Verify that this is an $\mathbb{F}_p$-linear map and is therefore representable as an $\ell \times \ell$ matrix over $\mathbb{F}_p$.

   (b) Assuming we are representing elements of $\mathbb{F}_{p^\ell}$ as polynomials of degree less than ℓ mod some explicit irreducible $R \in \mathbb{F}_p[X]$, indicate briefly how to efficiently compute the matrix for M_α.

   (c) Show that for any $a, b \in \mathbb{F}_p$ and any $\alpha, \beta \in \mathbb{F}_{p^\ell}$ we have $aM_\alpha + bM_\beta = M_{a\alpha+b\beta}$. Deduce that we can represent all field elements as $\ell \times \ell$ integer matrices mod p, with field arithmetic corresponding to matrix arithmetic.

2. Let p be a prime. Prove that the polynomial $f(X) = X^p - X - 1$ is irreducible over $\mathbb{F}_p$. In other words, if we factor $f(X) = g(X)h(X)$ for polynomials $g, h \in \mathbb{F}_p[X]$, then either g or h is a constant polynomial.

   Suggestion: One approach is to use the fact that if f has a factor of degree a, then there exists $\beta \in \mathbb{F}_{p^a}$ with $\beta^p = \beta + 1$.

3. Let p be an odd prime. Prove that the polynomial $X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1$ is irreducible over $\mathbb{F}_2$ if and only if 2 is a primitive element in $\mathbb{F}_p$, i.e., the multiplicative order of 2 mod p equals $p - 1$.

   Hint: If $f \in \mathbb{F}_2[X]$ and α is a root of f, then α^2 is also a root of f.

4. (a) Consider a nonzero polynomial $f \in \mathbb{F}_2[X_1, X_2, \ldots, X_m]$ of degree d, where we assume that the degree of each X_i in f is at most 1 (such a polynomial is called multilinear). Prove that $f(a) \neq 0$ for at least 2^{m-d} values of $a \in \mathbb{F}_2^m$. Is this tight? If so, can you characterize the nonzero degree d multilinear polynomials which are nonzero on exactly 2^{m-d} points in $\mathbb{F}_2^m$?

   (b) Let $\mathcal{F}_{m,d}$ be the space of multilinear polynomials in $\mathbb{F}_2[X_1, \ldots, X_m]$ of degree at most d. Define $\mathcal{F}_{m,d}^\perp$ be the space of multilinear polynomials $g \in \mathbb{F}_2[X_1, \ldots, X_m]$ that are orthogonal to every $f \in \mathcal{F}_{m,d}$, i.e., $\sum_{a \in \mathbb{F}_2^m} f(a)g(a) = 0, \forall f \in \mathcal{F}_{m,d}$.

   Prove that $\mathcal{F}_{m,d}^\perp = \mathcal{F}_{m,m-d-1}$ (where use the convention $\mathcal{F}_{m,-1} = \{0\}$).

5. For this problem, assume the NP-hardness of the following "finite-field subset sum" problem:

   Instance: A set $S = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{2^m}$, an element $\beta \in \mathbb{F}_{2^m}$, and an integer $1 \leq k < n$. (Also assume $m \leq n$.)

   Question: Is there a nonempty subset $T \subseteq \{1, 2, \ldots, n\}$ with $|T| = k + 1$ such that $\sum_{i \in T} \alpha_i = \beta$?

   Consider the Reed-Solomon code C_{RS} over $\mathbb{F}_{2^m}$ obtained by evaluating polynomials of degree at most $k - 1$ at points in S (i.e., we only use points in S for the encoding). Define $y \in (\mathbb{F}_{2^m})^n$ as follows: $y_i = \alpha_i^{k+1} - \beta\alpha_i^k$ for $i = 1, 2, \ldots, n$.

(a) Argue that there is a codeword of C_{RS} at Hamming distance at most $n-k$ from y.

(b) Show that there is a codeword of C_{RS} at Hamming distance at most $n-k-1$ from y if and only if there is a set T as above of size $k+1$ satisfying $\sum_{i \in T} \alpha_i = \beta$.

(c) Conclude that finding the nearest codeword in a Reed-Solomon code over exponentially large fields is NP-hard. (Believe it or not, proving NP-hardness of this basic problem for polynomial-sized fields remains an embarrassing open question. If you are interested in learning more about this, come talk to me!)

6. In class, we saw how identity testing of a certain determinant polynomial can be used to give a randomized algorithm to test if a graph has a perfect matching.[1]

In this problem, we will turn to bipartite matchings, which is in fact easier (no need to be careful about signs or odd cycles in permutations), as described in the course scribe notes from 2013. For this problem though, we will be interested in the following variant of bipartite perfect matching: each edge of the bipartite graph $H = (U, V, E)$ is colored either Red or Blue. The goal is to determine if there is a perfect matching in H that has exactly r Red edges (here r is an input parameter to the problem).

(a) Suppose edge $(u, v) \in E$ of the bipartite graph has a positive integer "weight", $w_{u,v}$, which is at most $\mathrm{poly}(n)$. Give a *deterministic* polynomial time algorithm, using determinant computation of appropriate matrices, with the following properties:

- if H has no perfect matching with exactly r Red edges, then the algorithm answers NO;
- if H has at least one perfect matching with exactly r Red edges, and the perfect matching with r Red edges of *minimum total weight* is *unique*, then the algorithm answers YES.

Hint: consider the integer matrix whose (u, v) entry is $2^{w_{u,v}}$ if edge (u, v) is colored Blue, and $X \cdot 2^{w_{u,v}}$ if edge (u, v) is colored Red, for some indeterminate variable X.

(b) Let Y be a set of cardinality m. Let $\mathcal{F}$ be a nonempty collection of subsets of Y. Let $\boldsymbol{w} : Y \to \{1, 2, \ldots, M\}$ be a random "weight" function, where each value $\boldsymbol{w}(y)$ is chosen uniformly from $\{1, 2, \ldots, M\}$, independently for each $y \in Y$. For a given set $C \in \mathcal{F}$, define its weight to be $\boldsymbol{w}(C) = \sum_{y \in C} \boldsymbol{w}(y)$. After $\boldsymbol{w}$ is chosen, look at the minimum weight $\boldsymbol{w}(C)$ among sets $C \in \mathcal{F}$; there might be a unique minimum-weight set, or there might be multiple sets tied for the minimum. Show that the probability of a unique minimum-weight set is at least $1 - m/M$.

Hint: For $y \in Y$, upper bound the probability of the event A_y that there are two minimum-weight sets in F, one containing y and the other not containing y.

(c) Give a randomized polynomial time algorithm which, given a bipartite graph H whose edges are colored Red/Blue and a positive integer r, offers the following guarantees:

- if H has no perfect matching with exactly r Red edges, then the algorithm correctly reports this;
- if H has a perfect matching with exactly r Red edges, the algorithm correctly reports this with probability at least $1/2$.

[1] One advantage of this method, which we forgot to mention in lecture, is that it can be efficiently parallelized to run in polylogarithmic time (essentially because determinant can be computed efficiently in parallel). This implies that perfect matchings in graphs can be solved in RNC (randomized NC). In fact, even for bipartite graphs, it remains open if one can ascertain the existence of a perfect matching in NC, i.e., without resorting to randomization.