EO 322: Assignment 1

Due date: Feb 6, 2013

General instructions:

- Submit your solutions by typesetting in LaTeX.
- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly urged to solve the problems by yourself.
- If you discuss with someone else or refer to any material (other than the course notes) then please put a reference in your answer script stating clearly whom or what you have consulted with and how it has benifited you. We would appreciate your honesty.
- If you need any clarification, please ask the instructor.

Total: 50 points

In the following problems, $\mathbb{N}$ is the set of natural numbers, $\mathbb{Q}$ is the field of rationals and $\mathbb{F}_q$ is the finite field with q elements.

1. (**3 points**) Given a number N, check if N is a perfect power (i.e. a power of some other number) in $(\log N)^c$ time, where c is a fixed constant independent of N. Find an exact value for c.
2. (**4 points**) Let $N = p \cdot q$ for two distinct primes $p, q \in \mathbb{N}$.
   (a) (**1 point**) Show how to compute p and q from the knowledge of N and $\varphi(N)$, where φ is Euler's totient function.
   (b) (**3 points**) Suppose that you are given a 'black-box' which on input $e \in \mathbb{N}$ decides whether it is coprime to $\varphi(N)$, and if so, returns $d \in \{1, \ldots \varphi(N) - 1\}$ such that $de = 1 \mod \varphi(N)$. Give an algorithm using this 'black-box' which computes $\varphi(N)$ in time $(\log N)^{O(1)}$.
3. (**4 points**) Suppose that we want to find an x such that $x = a_i \mod n_i$ for $1 \leq i \leq k$, where $a_i, n_i \in \mathbb{N}$. We are told that n_i and n_j *need not* be coprime to each other for $i \neq j$. Show that a solution x exists if and only if $a_i = a_j \mod (\gcd(n_i, n_j))$ for all i, j with $i \neq j$. Also show that this solution x is unique modulo the $\mathrm{lcm}(n_1, \ldots, n_k)$.

4. (**5 points**) *Background:* Suppose we are given m linear equations over $\mathbb{Q}$ in n variables, where $m \leq n$. The equations need not be homogeneous. Besides, the rank of the coefficient matrix might be strictly less than m - a priori we do not know what is the rank of this linear system. We want to solve this system (meaning that we want to find n affine linear polynomials in the 'free variables' such that if we assign these n linear polynomials to the n variables, the linear system is satisfied.) Assume that in this linear system, the absolute values of the numerator and denominator of any coefficient (in $\mathbb{Q}$) is bounded by $H \in \mathbb{N}$.

   Task: Design an algorithm, using Chinese remaindering theorem, to solve this linear system in time polynomial in n, m and $\log H$.

5. (**6 points**) Let $k = \binom{n+d}{d}$ where n and d are positive integers.

   (a) (**4 points**) Show the following: There exists k points $\mathbf{u}_1, \ldots, \mathbf{u}_k$ in $\mathbb{F}_q^n$ such that for every set of k values $\mathbf{a} = \{a_1, \ldots, a_k\}$ with $a_i \in \mathbb{F}_q$, there is an n-variate polynomial $P_{\mathbf{a}}(x_1, \ldots, x_n)$ with total degree at most d, satisfying $P_{\mathbf{a}}(\mathbf{u}_i) = a_i$ for all $1 \leq i \leq k$. Given d and n, design an algorithm with running time polynomial in d^n and $\log q$, to find $\mathbf{u}_1, \ldots, \mathbf{u}_k$. (You may assume that $q > d$.)

   (b) (**2 points**) Further, with the knowledge of $\mathbf{u}_1, \ldots, \mathbf{u}_k$, design an algorithm with running time polynomial in k and $\log q$ which finds the (coefficients of the) polynomial $P_{\mathbf{a}}$, given $\mathbf{a}$.

6. (**3 points**) The algorithm shown in the class computes DFT_ω over a (commutative) ring $\mathcal{R}$ by dividing the input polynomial $f \in \mathcal{R}[x]$ of degree less than n by $x^{n/2} - 1$ and $x^{n/2} + 1$ with remainder. A different approach is to split f into its odd and even parts, that is, to write $f = f_0(x^2) + x f_1(x^2)$ with $f_0, f_1 \in \mathcal{R}[x]$ of degree less than $n/2$, and then to compute $\mathsf{DFT}_{\omega^2}(f_0)$ and $\mathsf{DFT}_{\omega^2}(f_1)$ recursively. Prove that this algorithm uses $O(n \log n)$ operations over $\mathcal{R}$.

7. (**9 points**) Let $\mathcal{R}$ be a ring (commutative with unity).

   (a) (**2 points**) For $p \in \mathbb{N}_{\geq 2}$, determine the quotient and the remainder on division of $f_p = x^{p-1} + x^{p-2} + \ldots + x + 1$ by $x - 1$ in $\mathcal{R}[x]$. Conclude that $x - 1$ is invertible modulo f_p if p is a unit in $\mathcal{R}$ and that $x - 1$ is a zero divisor modulo f_p if p is a zero divisor in $\mathcal{R}$.

   (b) (**3 points**) Assume that 3 is a unit in $\mathcal{R}$, and let $n = 3^k$ for some $k \in \mathbb{N}$, $D = \mathcal{R}[x]/(x^{2n} + x^n + 1)$, and $\omega = x \mod (x^{2n} + x^n + 1) \in D$. Prove that $\omega^{3n} = 1$ and $\omega^n - 1$ is a unit in D. Conclude that ω is a primitive $3n$-th root of unity in D.

   (c) (**4 points**) Let $p \in \mathbb{N}$ be a prime and a unit in $\mathcal{R}$, $n = p^k$ for some $k \in \mathbb{N}$ and $\phi_{pn} = f_p(x^n) = x^{(p-1)n} + x^{(p-2)n} + \ldots + x^n + 1 \in \mathcal{R}[x]$ the pn-th cyclotomic polynomial. Let $D = \mathcal{R}[x]/(\phi_{pn})$ and $\omega = x \mod \phi_{pn} \in D$. Prove that $\omega^{pn} = 1$ and $\omega^n - 1$ is a unit in D. Conclude that ω is a primitive pn-th root of unity in D.

8. (**16 points**) *Background:* Recall that a Reed Solomon code is a $[n, n-(d-1), d]_q$ code, meaning that a message of length $n - (d-1)$ over a field $\mathbb{F}_q$ is encoded as a codeword of length $n = q$ such that the distance of the code is d. We have mentioned in the class that one drawback of RS codes is that the underlying field $\mathbb{F}_q$ needs to be as large as n. In this execise, we will see how to circumvent this restriction.

   Objective: To design a code with a 'good' distance over a small alphabet (say, $\mathbb{F}_2$ or any $\mathbb{F}_p$ for a small prime p).

Construction: Start with an RS code $C = [n, n-(d-1), d]_q$, where $n = q = p^t$ for some prime p and $t \in \mathbb{N}$. (C is the set of all codewords). Define the code $C' = C \cap \mathbb{F}_p^n$, i.e. C' is the set of all those codewords in C whose coordinates belong to $\mathbb{F}_p$.

Claim: C' is a $[n, k, d]_p$ code where $k \geq n - 1 - t\lceil \frac{(d-2)(p-1)}{p} \rceil$.

Your task is to prove the claim, in steps, by finding a good lower bound on the dimension of C' over $\mathbb{F}_p$.

(a) (**1 point**) Show that C' can be viewed as a $\mathbb{F}_p$-linear subspace of the space of all functions from $\mathbb{F}_{p^t} \to \mathbb{F}_p$. Observe that the space of all functions from $\mathbb{F}_{p^t} \to \mathbb{F}_p$ has dimension n over $\mathbb{F}_p$.

(b) (**2 points**) Prove that any function from $\mathbb{F}_{p^t} \to \mathbb{F}_p$ can be expressed as a polynomial $f(x)$ over $\mathbb{F}_{p^t}$ of degree at most $n-1$. (Hint: The evaluation of the polynomial $f(x)$ at a point $\alpha \in \mathbb{F}_{p^t}$ gives the value of the function at α.)

(c) (**4 points**) Observe that in the above construction, an element of C' is the evaluations of a (message) polynomial $\sum_{i=0}^{n-1} m_i x^i$ at all points of $\mathbb{F}_{p^t}$, where $m_{n-1} = m_{n-2} = \ldots = m_{n-(d-1)} = 0$. Now use (b) to infer that the $\dim(C')$ over $\mathbb{F}_p$ is at least $n - t(d-1)$.

(d) (**5 points**) Suppose that $m(x) = \sum_{i=0}^{n-1} m_i x^i$ is a polynomial over $\mathbb{F}_{p^t}$ mapping $\mathbb{F}_{p^t}$ to $\mathbb{F}_p$. Prove that $m_j = 0$ implies $m_\ell = 0$ for any $j, \ell \in \{1, \ldots, n-2\}$ satisfying $\ell = pj \mod (n-1)$. Also, show that $m_{n-1} \in \mathbb{F}_p$. [Hint: Use the property $m(x)^p = m(x) \mod (x^n - x, p)$. (Why is it so?)]

(e) (**4 points**) Use (d) to infer that $\dim(C')$ over $\mathbb{F}_p$ is at least $n - 1 - t\lceil \frac{(d-2)(p-1)}{p} \rceil$. Finally, observe that we can encode a message of length $k = \dim(C')$ over $\mathbb{F}_p$.