

Noise in Computation — Exercise 3 (submit July 26)

July 17, 2007

Recall Sudan's list-decoding algorithm for Reed-Solomon codes:

Given: Finite field F_q of size q , degree parameter k , agreement parameter a and received word $\langle (x_i, y_i) \rangle_{i=1}^n$ where $\forall i \neq i'$ we have $x_i \neq x_{i'} \neq 0$.

1. Find bivariate polynomial $Q(x, y) \in F_q[x, y]$ satisfying (i) $Q \not\equiv 0$, (ii) $\deg_x(Q) \cdot \deg_y(Q) > n$, (iii) $\forall i \in \{1, \dots, n\}$, $Q(x_i, y_i) = 0$.
2. Factor $Q(x, y)$ into irreducible factors, i.e., write $Q(x, y)$ as $Q(x, y) = \prod_{j=1}^r Q_j(x, y)$ where each $Q_j(x, y)$ is irreducible.
3. For every $j \in \{1, \dots, r\}$ do: If $Q_j(x, y) \equiv y - p_j(x)$ for some $p_j(x)$, $\deg(p_j) < k$ and

$$|\{i \in \{1, \dots, n\} : p_j(x_i) = y_i\}| \geq a,$$

Then output " $p_j(x)$ has agreement at least a with received word."

Questions

1. Assuming parts 1,2 can be performed in polynomial time in q (this was argued in class), prove that part 3 requires at most polynomial time in q .
2. Suppose $\deg_x(Q) = d_x, \deg_y(Q) = d_y, \deg_x(p) < k$ for $Q(x, y)$ as in part 1 of Sudan's algorithm and $p(x)$ a univariate polynomial. What is the minimal a (as a function of d_x, d_y and k) such that

$$\text{If } |\{i \in \{1, \dots, n\} : p(x_i) = y_i\}| \geq a, \text{ Then } Q(x, p(x)) \equiv 0?$$

3. What setting of d_x, d_y satisfying $d_x \cdot d_y > n$ will minimize a in the previous question? Compare this a to (i) the Johnson bound and (ii) the minimal agreement required for unique decoding.
4. Prove that Sudan's algorithm will recover all degree k polynomials that agree with the received word on more than a points, where a is as in the previous question. Hints: (i) Use arguments similar to those presented in the analysis of the Welch-Berlekamp algorithm. (ii) Use the following claim.

Claim: For $Q(x, y) \in F_q[x, y]$ and $p(x) \in F_q[x]$ we have $Q(x, p(x)) \equiv 0$ if and only if $(y - p(x))$ divides $Q(x, y)$.