

Exercise Sheet 12

Exercise 12.1. (Schwartz-Zippel lemma) Let $P(x_1, \dots, x_n)$ be a nonzero n -variate polynomial of total degree d over \mathbb{F}_q . We would like to bound the number of roots of P in \mathbb{F}_q^n .

1. First, suppose that $n = 1$, and $x_1 \in \mathbb{F}_q$ is chosen uniformly at random. Upper bound the probability $\Pr[P(x_1) = 0]$.
2. Now let $n > 1$. Use induction on n to show that, if x_1, \dots, x_n are chosen uniformly at random, $\Pr[P(x_1, \dots, x_n) = 0] \leq d/q$.
Hint: Write $P(x_1, \dots, x_n) = \sum_{i=0}^d x_1^i P_i(x_2, \dots, x_n)$, let j be the largest integer such that P_j is not identically zero and consider the events where $P_j(x_2, \dots, x_n) = 0$ and $P_j(x_2, \dots, x_n) \neq 0$.
3. Conclude that P can have at most dq^{n-1} roots.

Exercise 12.2. Let $\mathbb{F}_q[x, y]_{<k, <k}$ denote the space of bivariate polynomials over \mathbb{F}_q in which the degree in x and the degree in y are both less than k .

1. Show that if $f \in \mathbb{F}_q[x, y]_{<k, <k}$ vanishes on $I \times I$ for some subset I of $\{1, \dots, q\}$ of size $\geq k$, then $f = 0$.
2. Consider the code C obtained by evaluating polynomials in $\mathbb{F}_q[x, y]_{<k, <k}$ on all points $(x, y) \in \mathbb{F}_q^2$. What is the dimension of C if $k < q$?
3. Given elements $y_{\alpha, \beta}, \alpha, \beta \in \mathbb{F}_q$, show that there exists a nonzero polynomial $Q(x, y, z) \in \mathbb{F}_q[x, y, z]$ of x -degree $< \ell$, of y -degree $< \ell$, and of z -degree $< t$ such that $Q(\alpha, \beta, y_{\alpha, \beta}) = 0$ for all $\alpha, \beta \in \mathbb{F}_q$, provided that $\ell^2 t > q^2$.

Exercise 12.3. Consider the ideal in $\mathbb{F}_{q^2}[x, y, z]$ generated by the polynomials $f(x, y, z) := x^q + x - y^{q+1}$ and $g(x, y, z) := y^q + y - z^{q+1}$.

1. Find the number of common roots $(x, y, z) \in \mathbb{F}_{q^2}^3$ of both equations.
2. Let $q := 4$, and calculate the dimension of the space of polynomials of degree less than n in $\mathbb{F}_{q^2}[x, y, z]/(f, g)$.
3. Find the dimension and a lower bound on the minimum distance of the AG-code obtained from this construction. Assume an appropriate constraint on n .