Solutions 12

Exercise 12.1.

1. Suppose that $n = 1$, so that $P(x_1)$ is a univariate polynomial of degree d over $\mathbb{F}_q$. Then we know that P has at most d roots in $\mathbb{F}_q$, therefore for x_1 chosen uniformly at random in $\mathbb{F}_q$, we get
$$\Pr[P(x_1) = 0] \leq d/q.$$

2. Now suppose that for a given $n \geq 2$, for any nonzero $(n-1)$-variate polynomial $P(x_1, \cdots, x_{n-1})$ of degree d, $\Pr[P(x_1, \cdots, x_{n-1}) = 0] \leq d/q$ when $x_1, \cdots, x_{n-1}$ are chosen uniformly in $\mathbb{F}_q$. We want to prove that for a nonzero n-variate polynomial $P(x_1, \cdots, x_n)$ of degree d, $\Pr[P(x_1, \cdots, x_n) = 0] \leq d/q$ when $x_1, \cdots, x_n$ are chosen uniformly in $\mathbb{F}_q$.
Write
$$\begin{aligned} P(x_1, \ldots, x_n) &= \sum_{i=0}^{d} x_1^i P_i(x_2, \ldots, x_n) \\ &= \sum_{i=0}^{j} x_1^i P_i(x_2, \ldots, x_n), \end{aligned}$$
where j is the largest index such that $P_j(x_2, \ldots, x_n)$ is not the zero polynomial. Note that $\deg P_j + j \leq d$. We have that
$$\begin{aligned} \Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0] &= \Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0 \wedge P_j(x_2, \ldots, x_n) = 0] \\ &\quad + \Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0 \wedge P_j(x_2, \ldots, x_n) \neq 0]. \end{aligned}$$
But
$$\Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0 \wedge P_j(x_2, \ldots, x_n) = 0] \leq \Pr_{x_2,\ldots,x_n}[P_j(x_2, \ldots, x_n) = 0] \leq \frac{\deg P_j}{q},$$
where we have used the induction hypothesis. Also,
$$\begin{aligned} &\Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0 \quad \wedge \quad P_j(x_2, \ldots, x_n) \neq 0] \leq \\ &\qquad \Pr_{x_1}[P(x_1, \cdots, x_n) = 0 | x_2, \ldots, x_n \text{ are s.t. } P_j(x_2, \ldots, x_n) \neq 0]. \end{aligned}$$
But when we condition on the event that $P_j(x_2, \ldots, x_n) \neq 0$, we have that $P(x_1, \cdots, x_n) = \sum_{i=0}^{j} x_1^i P_i(x_2, \ldots, x_n)$ is a **nonzero** degree-j univariate polynonomial in x_1. We can now apply the result from part 1 and deduce that the probability that such a polynomial evaluates to 0 is upper-bounded by j/q.
We thus have that
$$\Pr[P(x_1, \cdots, x_n) = 0] \leq \frac{\deg P_j + j}{q} \leq d/q,$$
which completes the induction step.

3. By definition,
$$\Pr[P(x_1, \cdots, x_n) = 0] = \frac{\sharp \text{ roots } (a_1, \ldots, a_n) \text{ of } P}{q^n}.$$
Putting this together with the result of part 2, we conclude that the number of roots $(a_1, \ldots, a_n)$ of P over $\mathbb{F}_q$ is less than or equal to dq^{n-1}.

Note that we could consider the alternative problem of bounding the number of roots $(a_1, \ldots, a_n)$ of P where all a_i belong to a subset $S \subseteq \mathbb{F}_q$. Then we could follow a similar method to upper bound the number of such roots by $d|S|^{n-1}$.

Exercise 12.2.

1. Write $f(x,y)$ as $\sum_i f_i(y)x^i$. For any $\beta \in I$, $f(x,\beta) = \sum_i f_i(\beta)x^i$ is a univariate polynomial in x of degree $< k$, and it has at least k roots (x instantiated with all elements of I). Hence it is identically zero, and $f_i(\beta) = 0 \, \forall i$. Now for each such index i, we thus have that $f_i(\beta) = 0$ for all elements β of I, i.e., $f_i(y)$ has at least k roots. But it is a univariate polynomial in y of degree $< y$, so that $f_i(y)$ must be identically zero. We thus have that $f(x,y) = \sum_i f_i(y)x^i$ is identically 0.

2. The code C is the image of the map
$$\begin{array}{rcl} \phi : \mathbb{F}_q[x,y]_{<k,<k} & \to & \mathbb{F}_q^{q^2} \\ f & \mapsto & \big(f(a,b) : (a,b) \in \mathbb{F}_q^2\big) \end{array}$$
We would like to show that ϕ is injective. Take an element f of kerϕ. f is such that it evaluates to 0 on all $(a,b) \in \mathbb{F}_q^2$. Apply part 1 with $I = \mathbb{F}_q$ to get that f is the zero polynomial. Thus ϕ is injective and dim$C =$ dim(Im$\phi) = k^2$.

3. Finding such a nonzero polynomial $Q(x,y,z) = \displaystyle\sum_{i=0}^{\ell-1}\sum_{j=0}^{\ell-1}\sum_{k=0}^{t-1} q_{ijk}x^iy^jz^k$ amounts to finding its $\ell^2 t$ coefficients. The conditions $Q(\alpha,\beta,y_{\alpha,\beta}) = 0$ for all $\alpha,\beta \in \mathbb{F}_q$ correspond to q^2 linear equations that the $\{q_{ijk}\}$ must satisfy. As long as $\ell^2 t > q^2$, this linear system has a nontrivial solution.

Exercise 12.3.

1. We want to find the number of points $(x,y,z) \in \mathbb{F}_{q^2}^3$ such that
$$\begin{array}{rcl} z^{q+1} & = & y^q + y \\ y^{q+1} & = & x^q + x. \end{array}$$
Recall that the map $x \mapsto x^q + x$ is the *trace* of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and is a surjective homomorphism, and that the map $x \mapsto x^{q+1}$ is the *norm*, which means that it maps $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. Now z can take q^2 possible values, for each of which z^{q+1} is in $\mathbb{F}_q$. The trace map being a surjective homomorphism, we know that it maps to each value in $\mathbb{F}_q$ q times, so that there are q corresponding values of y such that $y^q + y = z^{q+1}$. But for each such value of y, there are again q values of x such that $x^q + x$ maps to $y^{q+1} \in \mathbb{F}_q$. In total, there are q^4 common zeros of f and g.

2. Consider $f(x,y) = x^q + x - y^{q+1}$. The space of polynomials of degree $< m$ in $\mathbb{F}_{q^2}[x,y]/(f)$ can be represented by

$$\Gamma_{<m} = \mathbb{F}_q[x]_{<m} \oplus y\mathbb{F}_q[x]_{<m-1} \oplus \cdots \oplus y^q\mathbb{F}_q[x]_{<m-q}$$

and is of dimension

$$\mathrm{dim}\Gamma_{<m} = (m-1)(q+1) - \frac{q(q-1)}{2} + 1 = 5m - 10$$

for $q := 4$. Now consider $g(x,y,z) = y^q + y - z^{q+1}$. The space of polynomials of degree $< n$, in $\mathbb{F}_{q^2}[x,y,z]/(f,g)$ can be represented by

$$\Gamma_{<n} \oplus z\Gamma_{<n-1} \oplus \cdots \oplus z^q\Gamma_{<n-q},$$

for $n > q$. This space has dimension

$$\sum_{m=n-q}^{n} (5m - 10) = 25n - 100.$$

3. We consider the curve given by $f(x,y,z) = 0, g(x,y,z) = 0$ and define the corresponding AG code $C = \mathrm{Im}\phi$, where

$$\begin{array}{rcl} \phi : \Gamma_{<n} \oplus z\Gamma_{<n-1} \oplus \cdots \oplus z^q\Gamma_{<n-q} & \rightarrow & \mathbb{F}_q^{q^4} \\ h & \mapsto & (h(a,b,c) : f(a,b,c) = g(a,b,c) = 0)\,. \end{array}$$

By Bézout's theorem, we know that the number of common zeros of any h and the curve is upper bounded by $\deg(h)\deg(f)\deg(g) < n(q+1)^2 = 25n$ (note that h belongs to such a space that it cannot be expressed as $h = h_1 f + h_2 g$ for some polynomials h_1 and h_2, so that Bézout's theorem can be applied).
We would like to make sure that ϕ is injective. For that, it is enough to impose the condition $n(q+1)^2 < q^4$, i.e., $n \leq 10$, which ensures that for any h in the domain, $\phi(h)$ is not all zeros. We then get the following parameters for the code:

$$\begin{array}{rcl} \mathrm{dim}C & = & 25n - 100 \\ \mathrm{dist}C & \geq & q^4 - n(q+1)^2 = 256 - 25n. \end{array}$$