Solutions 11

Exercise 11.1.

1. We can apply Eisenstein criterion with $p(x) = x$. We check that $p(x)|x$, $p(x)|x^3$ but $p^2(x) \nmid x$ and $p \nmid 1$.

2. The polynomial $\alpha^3 + \alpha + 1$ does not possess any root over $\mathbb{F}_2$. Since it has degree 3, it is irreducible as any decomposition would contain a degree 1 factor. Thus α allows us to define a degree 3 extension, i.e the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$. Besides let ω be such that $\omega^2 + \omega + 1 = 0$. We have as usual $\mathbb{F}_4 = \mathbb{F}_2[\omega]$. Caveat : F_4 is never a subfield of $\mathbb{F}_8$. In general $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^{k'}}$ if and only if k divides k'. Now we explore case by case the number of points by fixing the value of x. Note that it is not necessary to try to solve all equation involved. You can use the Frobenius to reduce the number of computation. You can also observe that if (a, b) is a point on the curve, then $(b^{-1}, a/b)$ and $(b/a, a^{-1})$ are also points on the curve (if defined).

x	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_8$
0	0	0	0
1	$\emptyset$	$\emptyset$	$\alpha, \alpha^2, \alpha^4$
ω		ω^2	
α			$1, \alpha, \alpha^6$
α^{-1}			$\alpha^3, \alpha^4, \alpha^6$

So we get $|\mathcal{K}_4(\mathbb{F}_2)| = 1$, $\mathcal{K}_4(\mathbb{F}_4) = 1 + 2 \cdot 1 = 3$ and $|\mathcal{K}_4(\mathbb{F}_8)| = 1 + 3 + 3 \cdot 3 + 3 \cdot 3 = 22$.

3. To apply the theorems seen during the lecture, we need to change a bit the defining polynomial f in order to have a polynomial of the form $x^4 + f_1(x, y)$ where the partial degree of f_1 is ≤ 3. This can be achieved by replacing y by $x + y$, since $f(x, x + y) = x^4 + (y + 1)x^3 + x^2y + (y^2 + 1)x + y^3$. This only changes the expression of the point of curve but not the parametres that we obtain. We consider the codes $C(\mathcal{K}_4(\mathbb{F}_8), m)$ for $4 \leq m \leq 6$ that yield $[22, 4m - 6, \geq 26 - 4m]_8$-codes as wanted. The table on the Internet shows that best known $[22, 10]_8$-code has minimum distance 10, best known $[22, 14]_8$-code distance 7 and best known $[22, 14]_8$-code distance 2.

Exercise 11.2.

1. We notice that $x^9 + 1$ has 1 as simple root and that $x + 1$ is an irreducible polynomial that does not divide 1. So by Eisenstein criterion, f is irreducible.

2. One can simply check that 3 divides 6 or recall that $\mathbb{F}_8$ is the set of roots of $x^8 - x$ in any extension of $\mathbb{F}_2$. Now, $\mathbb{F}_{64}^\times$ is a group of order 63 so it contains all 7-th roots of 1. We note that $x \mapsto x^9$ is a multiplicative group homomorphism on $\mathbb{F}_8^\times$. Its kernel is the set of 9th roots of unity. Since $\mathbb{F}_8^\times$ has order 7, $\mathbb{F}_8$ does not contain any such root except 1, so the map is an isomorphism of $\mathbb{F}_8^\times$. It is clear that it is remains a bijection on $\mathbb{F}_8$. On the other hand, on $\mathbb{F}_{64}^\times$, $x \mapsto x^9$ has a kernel of cardinality 9, namely $\{\alpha^{7i}, 0 \leq i \leq 8\}$ where α is a primitive element of $\mathbb{F}_{64}$. Besides, its image is in the set of the 7th root of unity,

ie $\mathbb{F}_8^\times \subseteq \mathbb{F}_{64}^\times$. Now, for cardinality reason, the morphism must be an epimorphism. So we have a $9-1$ map onto $\mathbb{F}_8^\times$.

3. On $\mathbb{F}_2$, there are two points $(0,1)$ and $(1,0)$. On $\mathbb{F}_8$, for any choice of x there is exactly a choice of y, because of the bijection property. So $|\mathcal{F}_9(\mathbb{F}_8)| = 8$. Now on $\mathbb{F}_{64}$, either x is one of the nine 9th roots of unity and y is 0 or x is one of the 55 non-9th root of unity, and y can take 9 values. In total we have $|\mathcal{F}_9(\mathbb{F}_{64})| = 9 + 55 \cdot 9 = 504$ values. Weil bounds shows that any way $-383 \leq |\mathcal{F}_9(\mathbb{F}_{64})| \leq 513$. Now actually Weil bound applies projective curves, this curve is maximal if you consider the projective curve associated with it : consider the homogenised equation $z^9 f(x/z, y/z) = x^9 + y^9 + z^9$ and count the number of non zero solutions up to homothety. You will find the 504 affine points that we have already (with $z = 1$) and 9 additionnal points (with $z = 0$). So there are 513 projective points on the curve which matches with Weil bound.

Exercise 11.3.

1. We want to find the number of points $(x, y, z) \in \mathbb{F}_{q^2}^3$ such that

$$\begin{aligned} z^{q+1} &= y^q + y \\ y^{q+1} &= x^q + x. \end{aligned}$$

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

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

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 $C = \text{Im}\phi$, where

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

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:

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

Exercise 11.4.

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

$$\Pr_{x_1,\ldots,x_n}[P(x_1, \cdots, x_n) = 0 \wedge P_j(x_2, \ldots, x_n) = 0] \leq \Pr_{x_2,\ldots,x_n}[P_j(x_2, \ldots, x_n) = 0] \leq \frac{\text{deg}P_j}{q},$$

where we have used the induction hypothesis. Also,

$$\Pr_{x_1,\ldots,x_n}[P(x_1,\cdots,x_n)=0 \quad \wedge \quad P_j(x_2,\ldots,x_n)\neq 0] \leq$$
$$\Pr_{x_1}[P(x_1,\cdots,x_n)=0|x_2,\ldots,x_n \text{ are s.t. } P_j(x_2,\ldots,x_n)\neq 0].$$

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 11.5.

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 ℓ^2t 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 $\ell^2t>q^2$, this linear system has a nontrivial solution.