ProblemSet 5 – Solutions of equations and cyclic codes

George McNinch

due 2024-03-29

1. Let q be a power of a prime $p > 3$ and let $k = \mathbb{F}_q$.

   For a homogeneous polynomial $F \in k[X, Y, Z, W]$, let us write

   $$V(F) = \{P = (x : y : z : w) \in \mathbb{P}^3_k \mid F(x, y, z, w) = 0\}$$

   for the set of solutions of the equation $F = 0$ in $\mathbb{P}^3_k$.

   For $a \in k^\times$, consider the polynomial

   $$F_a = XY + Z^2 - aW^2 \in k[X, Y, Z, W].$$

   a. If $4 \mid q - 1$ show that
   $$|V(F_a)| = |V(X^2 + Y^2 + Z^2 - aW^2)|$$

      Hint: First show that $X^2 + Y^2 + Z^2 - aW^2$ is obtained from F_a by a linear change of variables.

   b. If $a = 1$, show that $|V(F_1)| = q^2 + 2q + 1$.

      Hint: Making a linear change of variables, first show that $|V(F_1)| = |V(G)|$ where $G = XY + ZW$.

      To count the points $(x : y : z : w)$ in $V(G)$, first count the points with $xy = 0$ (and hence also $zw = 0$), and then the points with $xy \neq 0$.

   Let $S = \{a^2 \mid a \in k\}$.

   c. Show that $|S| = \dfrac{q+1}{2}$. Conclude that there are $q - \dfrac{q+1}{2} = \dfrac{q-1}{2}$ *non-squares* in k.

   d. If $a \in S$, show that $|V(F_a)| = |V(F_1)| = q^2 + 2q + 1$.

   e. If $a \in k$, $a \notin S$, show for any $\alpha \in k^\times$ that there are exactly $q + 1$ pairs $(c, d) \in k \times k$ with $c^2 - ad^2 = \alpha$.

      Hint: We may identify $\ell = \mathbb{F}_{q^2} = \mathbb{F}_q[\sqrt{a}]$. Under this identification, the norm homomorphism $N = N_{\ell/k} : \ell^\times \to k^\times$ is given by the formula

      $$N(c + d\sqrt{a}) = (c + d\sqrt{a})(c - d\sqrt{a}) = c^2 - ad^2.$$

      On the other hand, by Galois Theory, we have $N(x) = x \cdot x^q = x^{1+q}$ for any $x \in \ell$. Thus $N(\ell^\times) = k^\times$ and $|\ker N| = q + 1$.

   f. If $a \in k$, $a \notin S$ show that $|V(F_a)| = q^2 + 1$

      Hint: Notice that the equation $Z^2 - aW^2 = 0$ has *no solutions* $(z : w) \in \mathbb{P}^1_k$, and use (e) to help count.

2. Let $f = T^{11} - 1 \in \mathbb{F}_4[T]$.

   a. Show that $T^{11} - 1$ has a root in $\mathbb{F}_{4^5}$.

   b. If $\alpha \in F_{4^5}$ is a primitive element – i.e. an element of order $4^5 - 1$, find an element $a = \alpha^i \in \mathbb{F}_{4^5}$ of order 11, for a suitable i.

   c. Show that the minimal polynomial g of a over $\mathbb{F}_4$ has degree 5, and that the roots of g are powers of a. Which powers?

d. Show that $f = g \cdot h \cdot (T-1)$ for another irreducible polynomial $h \in \mathbb{F}_4[T]$ of degree 5. The roots of h are again powers of a. Which powers?

e. Show that $\langle f \rangle$ is a $[11, 6, d]_4$ code for which $d \geq 4$.

3. Consider the following variant of a Reed-Solomon code: let $\mathcal{P} \subset \mathbb{F}_q$ be a subset with $n = |\mathcal{P}|$ and write $\mathcal{P} = \{a_1, \cdots, a_n\}$.

Let $1 \leq k \leq n$ and write $\mathbb{F}_q[T]_{<k}$ for the space of polynomial of degree $< k$, and let $C \subset \mathbb{F}_q^n$ be given by

$$C = \{(p(a_1), \cdots, p(a_n)) \mid p \in \mathbb{F}_q[T]_{<k}.$$

a. If $n \geq k$, prove that C is a $[n, k, n-k+1]_q$-code.

b. If $P = \mathbb{F}_q^\times$, prove that C is a *cyclic code*.

c. If $q = p$ is *prime* and if $P = \mathbb{F}_p$, prove that C is a *cyclic code*.

Bibliography