ProblemSet 5 – Solutions of equations and cyclic codes – solutions

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.

SOLUTION:

Recall that $\mathbb{F}_q^\times$ is a cyclic group of order $q - 1$. This cyclic group contains an element $i \in \mathbb{F}_q^\times$ of order 4 if and only if $4 \mid q - 1$.

If this is the case, then $i^2 = -1$ since -1 is the unique element of $\mathbb{F}_q^\times$ of order 2.

Now, we have $X^2 + Y^2 = (X + iY)(X - iY)$.

Thus

$$X^2 + Y^2 + Z^2 - aW^2 = (X + iY)(X - iY) + Z^2 - aW^2 = X'Y' + Z^2 - aW^2 = F_a(X', Y', Z, W).$$

Thus using the linear change of variables $X' = X + iY$ and $Y' = X - iY$, we find a bijection between the sets $V(F_a)$ and $V(X'^2 + Y'^2 - ZW) = V(X^2 + Y^2 - ZW)$.

In particular, we thus have

$$|V(F_a)| = |V(X^2 + Y^2 - ZW)|.$$

---

   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 $xy \neq 0$.

SOLUTION:

Arguing as in (a), we see that after a linear change of variables, we may replace $F_1 = XY + Z^2 - W^2$ by $XY + ZW$; in particular, there is a bijection between $V(XY + Z^2 - W^2)$ and $V(XY + ZW)$.

We now compute $|V|$ where $V = V(XY + ZW)$.

A point $(x : y : z : w) \in \mathbb{P}^3$ is in V if and only if $xy = -zw$.

- We first count the points with $xy = 0 = zw$.

  One possibility is that exactly one of $\{x, y, z, w\}$ is non-zero. There are 4 such points, namely:

  $$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1).$$

  If more than one of $\{x, y, z, w\}$ is non-zero, then at exactly one of $\{x, y\}$ is zero, and since we work in projective space we may consider points where exactly one of $\{x, y\}$ is equal to 1.

  There are exactly $q - 1$ points of the form $(1 : 0 : a : 0)$ for $a \in \mathbb{F}_q$; more generally, it is easy to see that there are $4(q - 1)$ points with $xy = 0 = zw$ for which exactly one of $\{x, y\}$ is zero.

  In particular, we now see that there are $4(q - 1) + 4 = 4q$ points $(x : y : z : w)$ in V with $xy = 0$.

- Now we count the points in V with $xy \neq 0$. After observing that $(x : y : z : w)$ by $(1 : x/y : z/x : w/x)$, we see that we need to count the number of points $(1 : y : z : w)$ with $zw = -y$ and $y \neq 0$.

  There are $q - 1$ possibilities for $y \in \mathbb{F}_q^\times$, and for each such y, there are $q - 1$ pairs $(z, w) \in \mathbb{F}_q^2$ for which $zw = -y$.

  Thus there are $(q - 1)^2$ points $(x : y : z : w) \in V$ with $xy \neq 0$.

We now see that the total number of points in V is given by

$$|V| = 4q + (q - 1)^2 = q^2 + 2q + 1 = (q + 1)^2.$$

Remark In fact, one can show that $V \simeq \mathbb{P}^1 \times \mathbb{P}^1$, which explains that $|V| = |\mathbb{P}^1|^2 = (q + 1)^2$.

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.

SOLUTION:

Consider the group homomorphism $\phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $\phi(x) = x^2$.

The kernel of ϕ is the set of elements of $\mathbb{F}_q^\times$ whose order divides 2; since $\mathbb{F}_q^\times$ is *cyclic* and since p is odd, $\ker \phi$ has order 2 (in fact, $\ker \phi = \{\pm 1\}$).

By the first isomorphism theorem, we see that the *image* of ϕ has order

$$|\operatorname{image}(\phi)| = |\mathbb{F}_q^\times| / |\ker \phi| = (q - 1)/2$$

.

Thus there are $(q - 1)/2$ non-zero squares in $\mathbb{F}_q$; since 0 is also a square, we see that

$$|S| = (q - 1)/2 + 1 = (q + 1)/2.$$

In particular, there are $q - |S| = q - (q + 1)/2 = (q - 1)/2$ non-squares in $\mathbb{F}_q$.

---

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

I should have stipulated that the assumption $q \equiv 1 \pmod 4$ is still in effect

---

SOLUTION:

For $a \in S$, we know that F_1 is obtained by a linear change-of-variables from F_a. Indeed, writing $a = t^2$ we see that

$$F_a = XY + Z^2 - aW^2 = XY + (Z - tW)(Z + tW) = XY + Z'W'$$

where $Z' = Z - tW$ and $W' = Z + tW$.

In other words, we can obtain $XY + ZW$ from F_a through a linear change of variables.

Since $q \equiv 1 \pmod 4$, we've already seen (above) that $XY + Z^2 + W^2 = F_1$ can be obtained by a linear change of variables from $XY + ZW$.

Thus, F_1 can be obtained by a linear change of variables from F_a.

Now, this linear change-of-variables defines a bijection between $V(F_a)$ and $V(F_1)$. In particular, we have

$$|V(F_a)| = |V(F_1)| = (q+1)^2.$$

---

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 $|\ker N| = q + 1$.

SOLUTION:

On the one hand, the image of the norm homomorphism $\ell^\times \to k^\times$ is given by

$$\{c^2 - ad^2 \mid (0,0) \neq (c,d) \in k^2\}.$$

On the other hand, $\ell^\times$ is cyclic of order $q^2 - 1$ and $k^\times$ is cyclic of order $q - 1$. The norm mapping is given by $x \mapsto x^{1+q}$. Thus the norm mapping is *onto* and $\ker N$ is cyclic of order $q + 1$.

In particular, it follows that the norm mapping $N : \ell^\times \to k^\times$ is *onto*, and for each $\alpha \in K^\times$ there are exactly $q + 1$ elements $y = c + d\sqrt{a} \in \ell$ for which $\alpha = N(y) = c^2 - ad^2$.

---

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.

SOLUTION:

We count the number of points $(x : y : z : w) \in \mathbb{P}^3$ for which $xy - az^2 + w^2$.

Note that if $xy = 0$ there are *exactly two solutions*. Indeed, since a is not a square, we have

$$-az^2 + w^2 = N(w + z\sqrt{a}) = 0 \quad \text{if and only if} \quad w + z\sqrt{a} = 0 \quad \text{in } \ell$$

so the only solutions in this case are

$$(1:0:0:0), (0:1:0:0).$$

Now suppose that $xy \neq 0$. After division by x, we must count all points $(1 : y : z : w)$ for which $-y = N(w + z\sqrt{a})$. There are $q - 1$ possibilities for y and – according to the preceding part e. – for each y there are exactly $q + 1$ possibilities for (z, w). Thus there are $(q - 1)(q + 1)$ solutions with $xy \neq 0$.

Finally, we see that the total number of solutions is given by

$$2 + (q - 1)(q + 1) = 2 + q^2 - 1 = q^2 + 1.$$

---

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

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

SOLUTION:

Note that

$$4^5 = 4 \cdot 16^2 \equiv 4 \cdot 5^2 \equiv 4 \cdot 3 \equiv 1 \pmod{11}.$$

Since $\mathbb{F}_{4^5}^\times$ is a cyclic group whose order $4^5 - 1$ is divisible by 11, it follows that $\mathbb{F}_{4^5}^\times$ has an element a of order 11. This element $a \in \mathbb{F}_{4^5}$ is then a root of $T^{11} - 1$.

---

   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.

SOLUTION:

If $\mathbb{F}_{4^5}^\times = \langle \beta \rangle$ then β has order $4^5 - 1$, so that $a = \beta^{(4^5-1)/11}$ is an element of order 11.

---

   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?

SOLUTION:

We know that the Galois group of the extension $\mathbb{F}_4 \subset \mathbb{F}_{4^5}$ is cyclic of order 5, and is generated by the Frobenius automorphism $\sigma : x \mapsto x^4$.

Since $\mathbb{F}_4 \subset \mathbb{F}_{4^5}$ is a *Galois* extension (all extensions of finite fields are galois!) we know for $y \in \mathbb{F}_{4^5}$ that $y \in \mathbb{F}_4$ if and only if $\sigma(y) = y$ i.e. if and only if $y = y^4$.

Similarly, we know that a polynomial $g \in \mathbb{F}_{4^5}[T]$ satisfies $g \in \mathbb{F}_4[T]$ if and only if $g = \sigma(g)$ [1]

Now, define a polynomial $g \in \mathbb{F}_{4^5}[T]$ by the rule

$$g = \prod_{i=0}^{4} (T - a^{4^i}).$$

[1] For a polynomial $g \in \mathbb{F}_{4^5}[T]$, the application $\sigma(f)$ applies σ to the *coefficients* of g, and $\sigma(T) = T$. If $g = \sum_{i=0}^{N} a_i T^i$ then $\sigma(g) = \sum_{i=0}^{N} \sigma(a_i) T^i$.

Note that a is a root of g, and that

$$\sigma(g) = \prod_{i=0}^{4}(T - \sigma(a^{4^i})) = \prod_{i=0}^{4}(T - a^{4^{i+1}}) = g$$

since $a^{4^5} = a$.

It follows that $g \in \mathbb{F}_4[T]$. Since the Galois group acts transitively on the roots of g, it follows that g is *irreducible* over $\mathbb{F}_4$; g is thus the *minimal polynomial* of a over $\mathbb{F}_4$.

It is clear that g has degree 5; moreover its roots are a^i for i in the list `[1,4,4^2,4^3,4^4]`; since a has order 11, these roots are the elements a^i for i in the list `[1,4,5,9,3]` obtained by reducing the power 4^j modulo 11.

---

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?

SOLUTION:

We define $h \in \mathbb{F}_{4^5}[T]$ by the rule

$$h = \prod_{i=0}^{4}(T - a^{2\cdot 4^i}).$$

Then once again $\sigma(h) = h$ so that $h \in \mathbb{F}_4[T]$, and again h is irreducible over degree 5. Moreover, g is the minimal polynomial of a^2 over $\mathbb{F}_4$.

Since 1, a and a^2 are roots of $f = T^{11} - 1$, it follows that the minimal polynomials of these three elements divide f. These minimal polynomials are $T-1, g, h$ respectively. Since these three polynomials are relatively prime, we find that their productd $(T-1)\cdot g \cdot h$ divides f, and then for degree reasons we see that

$$f = (T-1)\cdot g \cdot h$$

(note that f, g, h are all monic!)

---

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

Typo: that should have been $\langle g \rangle$ rather than $\langle f \rangle$.

SOLUTION:

We need to compute the `minimal degree` of the code , so we use `SageMath`.

We first get the degree 5 irreducible factors of `f = T^11 - 1` over `GF(4)`:

```
k = GF(4)
R.<T> = PolynomialRing(k)

f = T^11 - 1

ff = f.factor()

g,_ = ff[1]
h,_ = ff[2]

(g,h)
=>
```

```
(T^5 + z2*T^4 + T^3 + T^2 + (z2 + 1)*T + 1,
T^5 + (z2 + 1)*T^4 + T^3 + T^2 + z2*T + 1)
```

Now we include the (previously used) code for computing minimal distance of a cyclic code:

```
V = VectorSpace(k,11)

def pad(ll,n):
    # pad the list ll with 0's to make it have length n
    x = len(ll)
    if x < n:
        return ll + (n-x)*[0]
    else:
        return ll[0:n]

def vectorize(p,n):
    # make a vector of length n out of a polynomial
    coeffs = p.coefficients(sparse=False)
    return V(pad(coeffs,n))


def mkCode(p):
    # vectorize the polynomial T^i * p and use the  vectors as a basis for the code C
    # I'm assuming deg p = 5...
    return V.subspace([ vectorize( T^i * p, 11) for i in range(6) ])

C1 = mkCode(g)
C2 = mkCode(h)

def weight(v):
    r = [x for x in v if x != 0]
    return len(r)

def min_distance(D):
    # brute-force computation of minimal distance of D
    return min([ weight(v) for v in D if v != 0])

[ min_distance(c) for c in [C1,C2]]
=>
[5, 5]
```

This shows that the minimal distance of the code $\langle g \rangle$ (and of the code $\langle h \rangle$) is 5.

---

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.

SOLUTION:

It is clear from the construction that $C \subset \mathbb{F}_q^n$. Moreover, $\dim C = k$ since that mapping
$$\phi : \mathbb{F}_q[T]_{<k} \to C \quad \text{via} \quad \phi(f) = (f(a_1), \cdots, f(a_n))$$

is injective and dim $\mathbb{F}_q[T]_{<k} = k$.

Finally, the minimal distance d of the (linear) code C is the minimal weight of a non-zero vector in C. If $x = \phi(f) \in C$, we have $n + \text{weight}(x) = \#\{ \text{ roots of } f \}$. Since f has degree $< k$, f has no more than $k-1$ roots; this shows that $\text{weight}(x) \geq n - k + 1$. This shows that $d \geq n - k + 1$.

To see that $d = n - k + 1$, note that $k \leq n \leq |\mathbb{F}_q|$ so that we may find k distinct elements $\alpha_1, \cdots, \alpha_{k-1}$ of $\mathcal{P}$. Now let f be a monic polynomial of degree $k-1$ with these $k-1$ roots; thus

$$f(T) = \prod_{i=1}^{n} (T - \alpha_i).$$

Then $\text{weight}(f) = n - k + 1$, so indeed $d = n - k + 1$.

We have now shown 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*.

SOLUTION:

We show that *for a suitable ordering of $\mathcal{P}$, the code C is* cyclic.

We fix a *generator* α for the (cyclic) multiplicative group $\mathbb{F}_q^\times$. Thus

$$\mathcal{P} = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}.$$

Now, for $f \in \mathbb{F}_q[T]_{<k}$, the corresponding code-word is

$$(f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{q-2})) \in C.$$

To see that C is cyclic, we must argue that

$$(\heartsuit) \quad (f(\alpha^{q-2}), f(1), f(\alpha), \cdots, f(\alpha^{q-3})) \in C.$$

Well, let $g(T) = f(\alpha^{-1}T) \in \mathbb{F}_q[T]$. Then $\deg g = \deg f < k$ so that $g \in \mathbb{F}_q[T]_{<k}$. Thus $x = \phi(g) \in C$. We now note that

$$\begin{aligned} x = (g(1), g(\alpha), g(\alpha^2), \cdots, g(\alpha^{q-2})) &= (f(\alpha^{-1}), f(\alpha^{-1}\alpha), f(\alpha^{-1}\alpha^2), \cdots, f(\alpha^{-1}\alpha^{q-2})) \\ &= (f(\alpha^{-1}), f(1), f(\alpha), \cdots, f(\alpha^{q-3})) \end{aligned}$$

so indeed $(\heartsuit)$ holds. This proves that $\mathcal{P}$ is cyclic.

---

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

SOLUTION:

Again, we show *for a suitable ordering of $\mathcal{P}$ that C is* cyclic*.

Note that $\mathcal{P} = \mathbb{F}_p$ may be written

$$\mathcal{P} = \{0, 1, 2, \cdots, p-1\}.$$

For an arbitrary $f \in \mathbb{F}_q[T]_{<k}$, the corresponding codeword $\phi(f)$ is given by

$$(f(0), f(1), f(2), \cdots, f(p-1)).$$

To see that C is cyclic, we must argue that

$$(\diamondsuit) \quad (f(p-1), f(0), f(1), \cdots, f(p-2)) \in C.$$

We set $g(T) = f(T-1) \in \mathbb{F}_[T]$, and we note that $\deg g = \deg f$ so that $g \in \mathbb{F}_q[T]_{<k}$. Thus $x = \phi(g) \in C$. Now we calculcate

$$\begin{aligned} x = (g(0), g(1), g(2), \cdots, g(p-1)) &= (f(0-1), f(1-1), f(2-1), \cdots, f(p-1-1)) \\ &= (f(p-1), f(0), f(1), \cdots, f(p-2)) \end{aligned}$$

so indeed $(\diamondsuit)$ holds. This proves that $\mathcal{P}$ is cyclic.

Bibliography