ECC 2020 Final exam — Solutions

Problem 1

(A). Consider a binary (n, M) code whose codewords are chosen independently (with replacement) from $\{0,1\}^n$.

Let $U_1 = \{a_1, a_2\}$, $U_2 = \{b_1, b_2\}$ be two pairs of codewords.

The probability that they are not separated is

$$\left(1-\frac{1}{8}\right)^n = (7/8)^n$$

The expected number of "bad" pairs U_1, U_2 is

$$E \leq \binom{M}{2}\binom{M-2}{2}(7/8)^n \leq \frac{M^4}{4}(7/8)^n$$

Take a code of size M in which the number of such pairs does not exceed the average.

Let $M = \left(2(7/8)^{-n}\right)^{1/3}$, then

$$E \leq \frac{1}{4}\left(2\left(\frac{7}{8}\right)^{-n}\right)^{4/3}\left(\frac{7}{8}\right)^n = 4^{-1/3}\left(\frac{7}{8}\right)^{n/3} = \frac{M}{2}$$

Discarding from every 4-tuple one vector, we obtain a $(2,2)$ separating code of size $\geq \frac{M}{2} = \exp_2\left(\frac{n}{3}\log_2\frac{8}{7}(1-o(1))\right) = \exp_2\left(n\left(1-\frac{1}{3}\log_2 7\right)\right)$ //

(B)

(1) The probability that a given coordinate in a t-tuple is t-hash equals

$$a_t := \prod_{i=1}^{t-1}\left(1-\frac{i}{q}\right)$$

(2) The probability that a given t-tuple has $\leq d-1$ hash coord's equals

$$P_b = \sum_{j=0}^{\delta n-1}\binom{n}{j}a_t^j(1-a_t)^{n-j} \leq e^{-2n(\delta-a_t)^2}$$

and the expected number of bad t-tuples is $p_b\binom{M}{t}$

Take $M = \left(t!\, n^{-2} e^{2n(\delta - a_t)^2}\right)^{\frac{1}{t-1}}$, then applying Markov's ineq.

$$P\left(\#\text{ bad } t\text{-tuples in } C \leq \frac{M}{n}\right) \geq 1 - \frac{1}{n}.$$

Thus, there exists a code C with at most as many bad t-tuples. Discarding one vector from each bad tuple, we obtain a code with t-hash distance $\geq d = \delta n$ of cardinality $\geq \frac{M}{n}$.

(3) This translates into rate

$$R_t(\delta) \geq 2\,\frac{1}{(t-1)\ln q}\,(\delta - a_t)^2 \quad //$$

Reference: A. B. and G. Kabatiansky, Robust parent-identifying codes and combinatorial arrays, IEEE Trans. IT, 2012.

Problem 2.

Suppose that G has $c \geq 1$ connected components and no isolated vertices.

(a) A mod 2 sum of ≥ 2 cycles is a subgraph of G in which all the vertices have even degree. Such subgraphs are often called circuits (or even cycles), and their characteristic vectors form an $\mathbb{F}_2$ linear space called the cycle space of G.

To construct a basis of the cycle space

Let T_i be a spanning tree of component $G_i(V_i, E_i)$

Add to T_i an edge in $E_i \setminus \text{edges}(T_i)$; this gives rise to a cycle.

The characteristic vectors of such cycles are linearly independent.

The total number of such cycles across the c components

$$= \sum_{i=1}^{c} \left(|E_i| - (|V_i| - 1)\right) = |E| - |V| + c$$

Thus, $\dim(\text{cycle code } C) \geq |E| - |V| + c.$ (1)

In Part (b) we show that the cutset code $C^\perp$ is of dimension $|V| - c$, so (1) holds with equality

Parameters of the cycle code of G

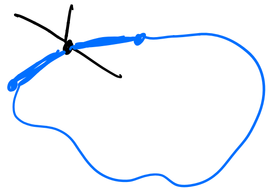
Length $= |E|$; dimension $= |E| - |V| + c$; distance $=$ length of the shortest cycle, also called the girth of G

(b) A cutset (cocycle) in G is a set of edges such that, removing them, we increase the number of connected components.

The edges incident to a given vertex form a cut, and characteristic vectors of such cuts are linearly independent (we can disregard isolated vertices).

There are $|V_i| - 1$ linearly independent cuts (the "last" vertex has all of its edges already covered by the other vertices).

Note that every such cutset intersects with a cycle by an even number of edges:



Every cutset in G is a linear combination of single-vertex cutsets.

Thus, characteristic vectors of the cutsets are orthogonal the cycle space.

Counting the number of linearly independent cuts, we obtain

$$\sum_{i=1}^{c} |V_i| - 1 = |V| - c$$

The parameters of the cocycle code are:

length $= |E|$; dimension $= |V| - c$; distance $=$ # edges in the smallest cut.

Problem 3.

(a) Differentiate the relation

$$\sum_{i=0}^{n} A_i y^i = \frac{1}{2^{n-k}} \sum_{i=0}^{n} A_i^{\perp} (1+y)^{n-i} (1-y)^i$$

on y and put $y=1$. We obtain

$$(1) \quad \boxed{\sum_{i=1}^{n} i \frac{A_i}{2^k} = \frac{n}{2} - \frac{A_1^{\perp}}{2} = \frac{n}{2} \text{ if } d^{\perp} \geqslant 2.}$$

Differentiating once again, we obtain

$$\sum_{i=0}^{n} i(i-1) A_i y^{i-2} = \frac{1}{2^{n-k}} \sum_{i=0}^{n} A_i^{\perp} \Big[(n-i)(n-i-1)(1+y)^{n-i-2}(1-y)^i - (n-i)i(1+y)^{n-i-1}(1-y)^{i-1}$$
$$- i(n-i)(1+y)^{n-i-1}(1-y)^{i-1} + i(i-1)(1+y)^{n-i}(1-y)^{i-2} \Big]$$

Putting $y=1$, we obtain

$$\sum i(i-1) \frac{A_i}{2^k} = \frac{n(n-1)}{4} - \frac{n-1}{2} A_1^{\perp} + \frac{1}{2} A_2^{\perp}$$

Thus $$\sum i^2 \frac{A_i}{2^k} = \frac{n(n-1)}{4} - \frac{n-1}{2} A_1^{\perp} + \frac{1}{2} A_2^{\perp} + \underbrace{\frac{n}{2} - \frac{A_1^{\perp}}{2}}_{(1)} = \boxed{\frac{n^2+n}{4} - \frac{n}{2} A_1^{\perp} + \frac{A_2^{\perp}}{2}}$$

[MacWilliams - Sloane] p. 130 ff.

(b) Let G be a generator matrix and $I \subseteq \{1, \dots, n\}$, $|I| =: t \leqslant d^{\perp} - 1$ be a subset of coordinates. By the Singleton Bound, $d^{\perp} - 1 \leqslant k$. Consider the $k \times t$ matrix $G(I)$ and the linear map

$$\varphi_I : \mathbb{F}_q^k \to \mathbb{F}_q^t$$

defined by it. Consider the quotient space $\mathbb{F}_q^k / (\ker \varphi_I)$, where $\dim(\ker \varphi_I) = k - t$. The vectors within each coset have the same coordinate projection on I, so the cosets partition $\mathbb{F}_q^k$ into q^t subsets of size q^{k-t}, as required.

Problem 4.

(a) Clearly, $(\alpha^i)^{q+1} = 1$ for $i = 0, 1, \dots, q$, so

$$x^{q+1} - 1 = \prod_{i=0}^{q} (x - \alpha^i)$$

(b) Let γ be a generating element of $\mathbb{F}_{q^2}$ over $\mathbb{F}$. Note that

$$\alpha = \gamma^{q-1}.$$

Assume that q is odd, then $i = \frac{q+1}{2}$ is an integer. Then $\alpha^{(q+1)/2} = \gamma^{(q^2-1)/2} = \sqrt{1} \neq 1$, i.e., $\alpha^{\frac{q+1}{2}} = -1$. The minimal polynomial $m_i(x) = x+1$. Similarly, for $i = 0$, $m_i(x) = x - 1$.

Other than that, let $1 \leqslant i \leqslant q^2 - 2$; then

$$(\alpha^i)^q = (\alpha^q)^i = (\gamma^{q^2-q})^i = (\gamma^{1-q})^i = \alpha^{-i}$$

(In fact, the operation of raising to power q is very similar to complex conjugation in the sense that both are involutions)

The cyclotomic coset of α^i is formed of 2 elements, $\{\alpha^i, \alpha^{iq} = \alpha^{-i}\}$, and thus $m_i(x) = (x - \alpha^i)(x - \alpha^{-i})$

Observe that the solutions for parts (c) and (d) are not exactly analogous; see (*) and (**) below

(c) For odd q, consider a cyclic code C, of length $n = q+1$ with generator polynomial

$$g(x) = \prod_{i=0}^{\frac{q-k}{2}} m_i(x), \quad k \text{ odd} \qquad (*)$$

The dimension

$$\dim C_1 = n - \deg g(x) = n - \deg m_0 - 2\left(\frac{q-k}{2}\right)$$

$$= n - 1 - q + k = k$$

The zeros of the code C_1 are: α^j, where

$$j \in \left\{ -\frac{q-k}{2}, -\frac{q-k}{2}+1, \dots, -1, 0, 1, \dots, \frac{q-k}{2} \right\}$$

This set is formed of $q-k+1$ consecutive integers, so the BCH Bound (Vandermonde parity-check matrix) tells us that $d(C_1) \geq q-k+2$. Then

$$\dim(C_1) + q - k + 2 = n+1$$

which shows, at the same time, that $d(C_1) = q-k+2$ and that the code C_1 is MDS.

(d) q even. Now look at the set of exponents of α:

$$\left\{0, 1, 2, 3, \dots, \frac{q}{2}-1, \frac{q}{2}, \frac{q}{2}+1 = -\frac{q}{2}, \frac{q}{2}+2 = -\left(\frac{q}{2}-1\right), \dots, q-1 = -2, q = -1\right\}$$

To construct a cyclic code C_2 of length $n = q+1$ and dimension **$n-k$.**

(1) For $k = 2t+1$ odd, take $g(x) = m_0(x)\, m_1(x) \dots m_t(x)$

By the BCH Bound this gives

$$d(C_2) \geq (1 + 2t) + 1 = k+1 = n - \dim(C_2) + 1$$

i.e., the code is MDS and the inequality on the previous line is an equality.

In this way we can obtain all <u>even</u> values of $\dim(C_2)$ among $1, 2, \dots, q+1$

(2) For $k = 2t$, $t \geq 1$ take $g(x) = m_{\frac{q}{2}}(x)\, m_{\frac{q}{2}-1}(x) \dots m_{\frac{q}{2}-t}(x)$

$$g(x) = \prod_{i=0}^{t} m_{\frac{q}{2}-i}(x) \qquad (**)$$

This gives $\dim(C_2) = n-2t = q+1-2t$ odd

We also have $2t$ consecutive zeros

$$\frac{q}{2}-t,\ \frac{q}{2}-t+1, \dots, \frac{q}{2}, \frac{q}{2}+1, \dots, \frac{q}{2}+(t-1), \frac{q}{2}+t$$

and $d(C_2) = 2t+1$ by the BCH bound, again proving the MDS property of C_2. This covers the case of odd dimensions in the set $\{1, 2, \dots, q+1\}$. //

Reference: Roth, Problem 8.15.