Prof. Dr. Marcus Greferath
Dept. of Mathematics and Systems Analysis
School of Sciences
Aalto University

Spring 2023

MS-EV0011: Codes over nonstandard alphabets

Problem Set II

Problem 1: Let C be the smallest cyclic code of length n that contains a given codeword a, where a is a polynomial of degree at most $n-1$ over the base field. Show that the generator polynomial of C is given by $g = \gcd(a, x^n - 1)$.

Work: First of all, we observe that, by definition, g is a monic divisor of $x^n - 1$, and hence it is the generator polynomial of a cyclic code. Now that g is at the same time a divisor of a, we conclude that $\mathbb{F}[x]\, a \subseteq \mathbb{F}[x]\, g$, and hence $\mathbb{F}[x]\, a/(x^n-1) \subseteq \mathbb{F}[x]\, g/(x^n-1)$. Known properties about the gcd include that there exist $s, t \in \mathbb{F}[x]$ such that $g = s\, a + t\,(x^n - 1)$. This immediately implies $\mathbb{F}[x]\, g/(x^n-1) = \mathbb{F}[x]\, sa/(x^n-1) \subseteq \mathbb{F}[x]\, a/(x^n-1)$ which is the reverse inclusion. Hence, our claim has been proved.

Problem 2: Let C be a q-ary cyclic code of length n where $\gcd(q, n) = 1$. Assume $g \in \mathbb{F}_q[x]$ is the generator polynomial, and $h \in \mathbb{F}_q[x]$ is its check polynomial, and hence $gh = x^n - 1$. Since $\gcd(g, h) = 1$ (why?) we have $a, b \in \mathbb{F}_q[x]$ with $ag + bh = 1$. Define $i = ag = 1 - bh$.

- **(a)** Show that i is a codeword, and that $ic \equiv c \pmod{x^n - 1}$ for all $c \in C$.
- **(b)** Show that i is an idempotent element, that means $i^2 \equiv i \pmod{x^n - 1}$.
- **(c)** Show that a polyomial having the properties in **(a)** is unique modulo $x^n - 1$. It is called the generating idempotent for C.

Work: Using the formal derivative (or otherwise), one can show that the assumption $\gcd(q, n) = 1$ leads to the fact that $x^n - 1$ does not have multiple zeros (in any extension field). This makes the two co-divisors g and h co-prime.

- **(a)** For $c \in C$ we have $\lambda \in \mathbb{F}_q[x]$ such that $c \equiv \lambda\, g \pmod{x^n - 1}$. This leads to $ic \equiv (1 - bh)\lambda g = \lambda g - \lambda bgh \equiv \lambda g \equiv c \pmod{x^n - 1}$.
- **(b)** Observing that $i \in C$, the equality $i^2 = i$ directly follows from **(a)**.
- **(c)** If $j \in C$ is another candidate for the role of i, we find $ij = j$ and $ji = i$ which by commutativity yields the equality of i and j.

Problem 3:

- **(a)** Using suitable existence bounds, determine whether or not binary linear codes with the following parameters exist. If you feel that such a code exists, then provide an example.

  – $[15, 11, 3]$

- $[11, 7, 6]$
- $[10, 3, 6]$
- $[16, 5, 8]$

(b) Compare the Gilbert with the Varshamov bound: using these, determine lower bounds on $A_2(16, 6)$. Conclusion?

Recall: $A_q(n, d) = \max\{M \mid \text{there exists an } (n, M, d)_q\text{-code.}\}$

Work:

(a) The triple $[15, 11, 3]$ belongs to the binary Hamming code of order $r = 4$, so the existence of a code is granted. The Singleton bound precludes the existence of a binary code with parameters $[11, 7, 6]$ because $7 + 6 \not\leq 11 + 1$. Looking at `codetables.de`, or otherwise, it turns out that the triple $[10, 3, 6]$ does not belong to an existing code, because of a violation of the Griesmer bound (that we have not covered in class). The final triple $[16, 5, 8]$ turns out to belong to the Reed-Muller Code $\mathrm{RM}(1, 4)$, hence a code with these parameters exists.

(b) The purely combinatorial version of the GV-bound yields that $A_2(16, 6) \geq 10$, while the algebraic version guarantees a linear code with at least 16 words. We conclude that the covering-based version is not as powerful as its competitor, which might be considered counter-intuitive, because linearity is a proper restriction on the code class. This problem is resolved observing that these bounds are *lower* bounds, guaranteeing rather than precluding the existence of the respective codes.

Problem 4: Let R be a finite Frobenius ring and assume χ is a generating character for R which means $\widehat{R} = R\chi$. Show that the pair of transforms $\hat{}$ and $\tilde{}\colon \mathbb{C}^R \longrightarrow \mathbb{C}^R$ where

$$\hat{f}(x) = \sum_{r \in R} f(r)\,\chi(xr) \qquad \text{and} \qquad \tilde{f}(x) = \frac{1}{|R|} \sum_{r \in R} f(r)\,\chi(-rx)$$

indeed satisfies $\tilde{\hat{f}} = \hat{\tilde{f}} = f$ for all $f \in \mathbb{C}^R$.

Work: We first observe that

$$\sum_{x \in R} \chi(xr) \;=\; \begin{cases} |R| & : \; r = 0, \\ 0 & : \; \text{otherwise.} \end{cases}$$

This stems from the fact that ${}^r\chi$ is principal if and only if $r = 0$, and is due to the fact that χ is a generating character. We will restrict to showing $\tilde{\hat{f}} = f$ for all $f \in \mathbb{C}^R$. For this, we compute

$$\tilde{\hat{f}}(x) \;=\; \frac{1}{|R|} \sum_{y \in R} \hat{f}(y)\chi(-yx),$$

combine it with

$$\hat{f}(y) \;=\; \sum_{r \in R} f(r)\chi(yr),$$

in order to obtain

$$\tilde{\hat{f}}(x) \;=\; \sum_{r \in R} f(r) \frac{1}{|R|} \sum_{y \in R} \chi(y(r - x)) \;=\; f(x).$$

In fact, by the above observation we have

$$\frac{1}{|R|} \sum_{y \in R} \chi(y(r - x)) \;=\; \begin{cases} 1 & : \; r = x, \\ 0 & : \; \text{otherwise.} \end{cases}$$