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 $g = \gcd(a, x^n - 1)$.

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.

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

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 $\tilde{}$: $\mathbb{C}^R \longrightarrow \mathbb{C}^R$ 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 $f \in \mathbb{C}^R$.