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 I

Problem 1:

(a) Find 8 distinct points in $\mathbb{F}_2^6$ that pairwise differ in at least 3 coordinates.

(b) Show that there are no 9 distinct points in $\mathbb{F}_2^6$, that have this property. Do this by grouping such a set of points according to their first entry and then applying the pigeonhole principle.

Work: By sorting the (prospective) 9 words according to their first entry, we find at least 5 words among the 9 that share the same starting symbol (Pigeonhole Principle). Erasing this symbol, we obtain (at least) 5 binary strings of length 5 that pairwise differ in at least 3 positions. The same argument leaves us with 3 binary strings of length 4 that pairwise differ in at least 3 positions. Without loss of generality (translation invariance of the Hamming metric), we may assume that one of these words is 0000. Again without loss of generality, we find that another word is of the form $111*$, where we leave it open, whether $* = 1$ or $* = 0$. For the third word, that needs to differ from the first two in 3 positions, there will be no space to exist. This is a contradiction that shows the impossibility of the existence of the initial 9 words.

Problem 2: We generalise the situation in problem 1 in the following way: Denote by $A_q(n,d)$ the maximal number of points in $\mathbb{F}_q^n$ that pairwise differ in at least d positions. Prove that

$$A_q(n,d) \;\leq\; q\,A_q(n-1,d).$$

Work: Let C be a code of lenght n and minimum distance d on the q-element alphabet, and assume it has $M = A_q(n,d)$ elements (maximal!). Like in problem 1, we sort the words according to the first entry and apply the Pigeonhole Principle to obtain a set of at least M/q words, that share the first entry. Erasing this entry, we find that these words form a code of length $n-1$ of minimum distance d, which shows that $M/q \leq A_q(n-1,d)$. This finally leads to the claim that $A_q(n,d) = M \leq q\,A_q(n-1,d)$, as desired.

Problem 3: Prove the Singleton bound, which says: If $C \subseteq F^n$ is a q-ary block code of Hamming minimum distance d, then $|C| \leq q^{n+1-d}$.

Work: There are several ways to prove the Singleten bound. One is by exploiting what we have learnt in problem 2, namely by successively applying the claim: This leads to $A_q(n,d) \leq q\,A_q(n-1,d) \leq q^2\,A_q(n-2,d) \leq \cdot \leq q^{n-d}\,A_q(d,d)$ where we observe that $A_q(d,d) \leq q$. This implies the desired inequality $A_q(n,d) \leq q^{n+1-d}$.

Problem 4: Prove the Gilbert-Varshamov bound, which says, that

$$A_q(n,d) \geq \frac{q^n}{\sum\limits_{j=0}^{d-1} \binom{n}{j}(q-1)^j}.$$

Do this by assuming a code C that has $M = A_q(n,d)$ words, and concluding that the (Hamming) disks with radius $d-1$ centered in the codewords then must cover the ambient space.

Work: Assume C is a code with $M = A_q(n,d)$ (which means maximal) number of codewords. Drawing spheres of radius $d-1$ around each of the codewords, we will cover all of the ambient space, because otherwise, there would be a word that has distance $\geq d$ from all other codewords, and M would not have been maximal. Considering that the volume of the Hamming disk of radius $d-1$ in n-space is

$$B_q(n, d-1) = \sum_{j=0}^{d-1} \binom{n}{j} q^{j-1},$$

this yields the claim.

Problem 5:

(a) Factorize the polynomial x^9+1 over $\mathbb{F}_2$.

(b) Determine all *distinct* cyclic binary linear codes of length 9, and find their parameters.

(c) Calling two codes equivalent, if they result from each other by a co-ordinate permutation, determine all *inequivalent* cyclic binary linear codes of length 9.

Work: The factorization of x^9-1 over $\mathbb{F}_2[x]$ (into irreducible factors) is given by

$$x^9 - 1 = (x+1)(x^2+x+1)(x^6+x^3+1).$$

This shows that there are $8 = 2^3$ distinct codes under investigation. We write the following table and attempt to determine the parameters of the codes brute force.

g	dim	dist
1	9	1
$x+1$	8	2
x^2+x+1	7	2
x^6+x^3+1	3	3
x^3+1	6	2
$x^7+x^6+x^4+x^3+x+1$	2	6
$\sum\limits_{i=0}^{8} x^i$	1	9
x^9+1	0	∞

These are the *distinct* binary cyclic codes of length 9. No pair of these are equivalent (which you would suspect at least from identical parameters). Hence this list is at the same time the list of *inequivalent* cyclic codes of length 9.