TC10 / **Problems 1-15**

S. Xambó

1 (A binary code $(8{,}20{,}3)$). Let C be the binary code $(8{,}20)$ formed with 00000000, 11111111 and all the cyclic permutations of 10101010, 11010000 and 11100100. Check that $d_C = 3$.

```
a=[1,1,0,1,0,0,0,0]; X=cyclic_shifts(a);
b=[1,1,1,0,0,1,0,0]; Y=cyclic_shifts(b);
c=[1,0,1,0,1,0,1,0]; Z=cyclic_shifts(c);
n=length(a); M=2+length(X)+length(Y)+length(Z);
aX={hd(a,x) with x in tail(X)}; aY={hd(a,y) with y in Y}; aZ={hd(a,z) with z in Z};
bY={hd(b,y) with y in tail(Y)}; bZ={hd(b,z) with z in Z};
cZ={hd(c,z) with z in tail(Z)};
d=min(aX|aY|aZ|bY|bZ|cZ);
{n,M,d} → {8,20,3}.
```

2 (Parity check matrix)**.** Let F be a field and $G = (I_k|R)$, $R \in M_{n-k}^{k}(F)$, and $H = (-R^T|I_{n-k})$. Then $GH^T = 0$. Show that if C is the vector subspace of F^n spanned by the rows of G, then

$$C = \{x \in F^n | xH^T = 0\}.$$

3 $A_q(3,2)$**.** Show that $A_q(3,2) = q^2$. In particular, $A_2(3,2) = 4$ and $A_3(3,2) = 9$.

4 (A more general form of **P3)**. Prove that $A_2(3k, 2k) = 4$ for all $k \geq 1$.

5. Prove that if d is odd, then $A_2(n,d) = A_2(n+1, d+1)$. Using this and **P4**, show that $A_2(5,3) = 4$.

6 (An application of the function $\text{vol}_q(n,d)$)**.** Let m and s be integers with $1 \leq s \leq m$ and let $c_1, \dots, c_m \in F^n$, where F is a finite field of cardinal q. Prove that the number of vectors in F^n that are linear combinations of at most s of the vectors $c_1, \dots, c_m$is $\leq \text{vol}_q(m,s)$.

7. Check that the parmeters $[23,12,7]$, $[90.78,5]$ and $[11,6,5]_3$ satisfy the condition for perfect codes.

Check also that if $q \geq 2$ and $r > 0$ are integers, then the parameters $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]$ satisfy the condition for perfect codes.

8. Let $C \sim (n, M, d)$ and suppose the nonnegative integers r and s satisfy $2r + s \leq d - 1$. Consider the decoder $g: T^n \to C \sqcup \{?\}$ such that $g(y) = x$ for $y \in B(x, r)$ and $g(y) =?$ if $y \notin \bigsqcup_{x \in C} B(x, r)$. Show that g corrects up to r errors and detects up to $r + s$ errors.[a]

9. The Hamming bound yields $A_2(6,3) \leq 9$. Prove that actually $A_2(6,3) \leq 8$. [*Hint:* If there were a code $(6,9,3)$, show that it would contain 3 words with the same bits in the last two positions]

10. Show that $A_2(8,5) = 4$ and that all $(8,4,5)$ codes are equivalent. [*Hint*: It may be assumed that 00000000 is a code-word; then show that there is at most one word of weight ≥ 6].

11. Show that for binary codes of odd minimum distance the Hamming bound is never worse than the Singleton bound.

Is the same statement true when the minimum distance is even? And for q-ary codes with $q > 2$?

12. Prove that $A_2(n, d) \leq 2A_2(n-1, d)$.

13. [Plotkin's construction, 1960]

Let C_1 and C_2 be binary codes of type (n, M_1, d_1) and (n, M_2, d_2), respectively. Let C be the code of length $2n$ whose vectors have the form $x|(x+y)$, where $x \in C_1$and $y \in C_2$. Show that
$C \sim (2n, M_1M_2, \min(2d_1, d_2))$.

14. Establish the inequality $A_2(16{,}3) \geq 2560$.

[*Hint.* Use the code $(8{,}20{,}3)_2$ and Plotkin's construction].

15. Prove that $A_q(n+1, d+1) \leq A_q(n, d)$.

Notes

a. The set of decodable vectors is $D = \bigsqcup_{x\in C} B(x,r)$. Since $r \leq \frac{d-1}{2}$, we have $r \leq t$ and hence $D \subseteq D_C$. This shows that g coincides with the minimum distance decoder for words in D. In particular, g is well defined. Now it is clear that g corrects up to r errors.

For the second part we have to see that an undetectable error cannot occur if the number of errors is not more than $r + s$. Let us argue by contradiction: if there were $x' \in C$ such that $x' \neq x$ and $y \in B(x', r)$, then

$$hd(x, x') \leq hd(x, y) + hd(y, x') \leq r + s + r \leq d - 1,$$

which contradicts, by the definition of d, that $x' \neq x$.