CODING THEORY: SOLUTIONS 1

Please note, theorem/proposition numbers used in these solutions refer to the theorems/propositions in a recent (respectively, older) version of the lecture notes. If the match is not perfect in your version, please do uses your initiative.

(1)

$$\{1,2\}^3 = \{1,2\} \times \{1,2\} \times \{1,2\} = \{111, 112, 121, 211, 122, 221, 212, 222\}$$

where we take ijk to mean (i,j,k) for all $i,j,k \in \{1,2\}$.

(2) (a) $d(C_1) = d(\{000, 111\}) = 3$,

(b) $d(C_2) = d(\{000, 111, 222\} = 3$,

(c) $d(C_3) = d(\{000, 111, 222, 012\} = 2$,

(d) $d(C_4) = d(\{000, 111, 222, 012, 011\} = 1$,

(e) $d(C_5) = d(\{000, 111, 222, 012, 011, 210\} = 1$.

Note that for each i we have $C_i \subset C_{i+1}$ so we know $d(C_{i+1}) \leq d(C_i)$.

(3) (a) $d(C_1) = d(\{0000, 0111\}) = 3$,

(b) $d(C_2) = d(\{0000, 0111, 1110\}) = 2$,

(c) $d(C_3) = d(\{0000, 0111, 1110, 0101\}) = 1$.

(4) Using Proposition 3.11 (3.10), a code C can detect up to t errors if $d(C) \geq t+1$ and correct up to t errors if $d(C) \geq 2t+1$. Therefore:

(a) C is 7 - error correcting therefore $d(C) \geq 2(7) + 1 = 15$,

(b) C is 11 - error detecting therefore $d(C) \geq 11 + 1 = 12$,

(c) C is 11 - error correcting therefore $d(C) \geq 2(11) + 1 = 23$,

(d) C is 21 - error detecting therefore $d(C) \geq 21 + 1 = 22$.

(5) As $d = 5 = 2(2)+1$ we know that any codeword x sent will be decoded correctly if $0, 1$ or 2 errors occur (Proposition 3.11 (3.10) (b)). Hence:

$$P_{corr}(x) \geq (1-p)^9 + \binom{9}{1} p(1-p)^8 + \binom{9}{2} p^2(1-p)^7 > 0.9999197$$

Hence $P_{err}(x) = 1 - P_{corr}(x) < 0.0000803$.

(6)
- $(9,2,9)$: $C = \{000000000, 111111111\}$ or any other two length 9 binary sequences which are different in all places,
- $(3,8,1)$: $C = \{000, 001, 010, 100, 011, 110, 101, 111\}$,
- $(4,8,2)$: As we have just found a $(3,8,1)$ code, we can extend it to a $(4,8,2)$ code by Theorem 3.26 (3.22).

  Thus $C = \{0000, 0011, 0101, 1001, 0110, 1100, 1010, 1111\}$,
- $(5,3,4)$: Assume such a code exists, then by Theorem 3.26 (3.22) there also exists a binary $(4,3,3)$-code which we will call C.

  Without loss of generality, assume that $0000 \in C$ (if not choose $x \in C$ and in every position where a 1 appears in x swap 1 and 0 in all codewords. The end result will be a $(4,3,3)$-code $\hat{C}$ containing 0000).

  Now C must contain 3 codewords, call other two y and z say. As the smallest possible distance between all codewords is 3 both y and z must contain at least three 1's so they have distance at least 3 from 0000. However, this that y and z can only differ in at most 2 places, therefore $d(y,z) \leq 2$ contradicting the minimum distance. Thus no such code can exist.
- $(8,41,3)$: By the ball packing bound (Thm 3.18 (3.16)) for a q-array (n,M,d)-code we have:

  $$M \sum_{r=0}^{t} \binom{n}{r} (q-1)^r \leq q^n.$$

  Plugging in our values we get:
  - $d = 2(1) + 1 \Rightarrow t = 1$,
  - $q^n = 2^8 = 256$, and hence
  - $M \sum_{r=0}^{t} \binom{n}{r} (q-1)^r = 41(\binom{8}{0}(1^0) + \binom{8}{1}(1^1)) = 41(1+8) = 369$

  but $369 \not\leq 256$ hence the BP bound fails, therefore no such code can exist.

  In fact, dividing the BP bound by $\sum_{r=0}^{t} \binom{n}{r}(q-1)^r$ we can determine that for a binary $(8,M,3)$-code to exist, we must have $M \leq 256 \div 9 \approx 28$.

(7) A q-ary (n,M,d)-code is perfect if the BP-bound (Theorem 3.18 (3.16)) satisfies equality, that is if:

$$M \sum_{r=0}^{t} \binom{n}{r} (q-1)^r = q^n$$

where we have $q = 2$.

- $(7, 16, 3)$: is perfect as $t = 1$ so,
$$16(\binom{7}{0} + \binom{7}{1}) = 16(8) = 128 = 2^7.$$
- $(5, 2, 5)$: is perfect as $t = 2$ so,
$$2(\binom{5}{0} + \binom{5}{1} + \binom{5}{2}) = 2(16) = 32 = 2^5.$$
- $(15, 2048, 3)$: is perfect as $t = 1$ so,
$$2048(\binom{15}{0} + \binom{15}{1}) = 2048(16) = 32768 = 2^{15}.$$
- $(6, 2, 5)$: is not perfect as $t = 2$ so,
$$2(\binom{6}{0} + \binom{6}{1} + \binom{6}{2}) = 2(22) = 44, \quad \text{but} \quad 2^6 = 64.$$

Thanks to Dr H Burke for preparation of these solutions, in support of the notes prepared by Prof Martin.