TW 314 (Applied Discrete Mathematics)

Tutorial 7: 16 March 2017

(Oplossings)

1. (a) $n = 8,\ M = 4,\ d = 5$. C kan twee foute korrigeer.
   (b) Nee. Hamming se grens word nie bevredig nie.
   (c) i. 11000011
      ii. 11011100
      iii. Kan nie hierdie vektor dekodeer nie; meer as twee foute is gemaak. (Die Hamming-afstande na die vier kodewoorde is onderskeidelik 6, 3, 3 en 4.)
      iv. 00111011
      v. 11011100

2. (a) $\{000000, 111111\}$
   (b) $(F_2)^3$
   (c) Voeg pariteitskontrole by elke kodewoord van $(F_2)^3$.
   (d) So 'n kode is nie moontlik nie. Veronderstel tot die teendeel dat C 'n $(5, 3, 4)$–kode is en gestel sonder verlies aan algemeenheid dat 00000 een van die kodewoorde is. Dan moet die ander twee kodewoorde elk vier of vyf ene bevat. Maar dit impliseer dat hulle in hoogstens twee posisies kan verskil, in teenspraak met $d(C) = 4$.
   (e) $\{00000, 11100, 00111, 11011\}$
   (f) Nie moontlik nie, aangesien Hamming se grens nie deur hierdie parameters bevredig word nie.

3. (a) Gestel C is 'n ternêre $(3, M, 2)$–kode. Dan moet die M geordende pare wat verkry word deur die derde koordinaat van elke kodewoord weg te laat almal verskillend wees, want sou twee sulke pare identies wees, dan sou die twee ooreenstemmende kodewoorde slegs in die derde posisie verskil, in teenspraak met $d(C) = 2$. Dus is $M \leq 9$.
   (b) 'n Ternêre $(3, 9, 2)$–kode is

$$\left\{ \begin{array}{ccc} 000 & 101 & 202 \\ 011 & 112 & 210 \\ 022 & 120 & 221 \end{array} \right\}$$

4. Gestel C is a $(n, 27, 2)$-kode. Dan moet die 27 vektore wat verkry word deur die eerste koordinaat van elke kodewoord weg te laat almal verskillend wees, want sou twee sulke vektore identies wees, dan sou die twee ooreenstemmende kodewoorde slegs in die eerste posisie verskil, in teenspraak met $d(C)$. Dus $3^{n-1} = 27$ en daarom $n = 4$.

5. Suppose $d(C) = 4$. If a received vector $\mathbf{y}$ has distance ≤ 1 from some codeword, we decode to that codeword. If $\mathbf{y}$ has distance at least 2 from every codeword, we seek re-transmission. This scheme guarantees the simultaneous correction of single errors and detection of double errors. Note that C could also be used either as a single-error-correcting code or as a triple-error-detecting code, but not both simultaneously (why not?).

6. $(\mathbb{Z}_6, +, \cdot)$ is nie 'n liggaam, aangesien $(\mathbb{Z}_6 - \{0\}, \cdot)$ nie 'n groep is nie.

TW 314 (Applied Discrete Mathematics)

Tutorial 7: 16 March 2017

(Solutions)

1. (a) $n = 8,\ M = 4,\ d = 5$. C can correct two errors.
   (b) No. Hamming's bound is not satisfied.
   (c) i. 11000011
       ii. 11011100
       iii. Cannot decode this vector; more than two errors have been made. (The Hamming distances to the four codewords are 6, 3, 3 and 4 respectively.)
       iv. 00111011
       v. 11011100

2. (a) $\{000000, 111111\}$
   (b) $(F_2)^3$
   (c) Add parity check to every codeword of $(F_2)^3$.
   (d) Such a code is not possible. Suppose to the contrary that C is a $(5, 3, 4)$ code and suppose, without loss of generality, that 00000 is one of the codeword. Then the other two codewords must each have four or five ones. But this implies that they can differ in at most two positions, contradicting $d(C) = 4$.
   (e) $\{00000, 11100, 00111, 11011\}$
   (f) Not possible, since Hamming's bound is not satisfied by these parameters.

3. (a) Suppose C is a ternary $(3, M, 2)$ code. Then the M ordered pairs obtained by deleting the third coordinate of each codeword must all be distinct, since if two such pairs were identical, then the two corresponding codewords would have differed only in the third position, contradicting $d(C) = 2$. Thus $M \leq 9$.
   (b) A ternary $(3, 9, 2)$ code is

$$\left\{ \begin{array}{ccc} 000 & 101 & 202 \\ 011 & 112 & 210 \\ 022 & 120 & 221 \end{array} \right\}$$

4. Suppose C is a ternary $(n, 27, 2)$-code. Then the 27 vectors obtained by deleting the first coordinate of each codeword must all be distinct, for if two such vectors were identical, then the two corresponding codewords would have differed only in the first position, contradicting $d(C)$. Thus $3^{n-1} = 27$ and so $n = 4$.

5. Suppose $d(C) = 4$. If a received vector $\mathbf{y}$ has distance ≤ 1 from some codeword, we decode to that codeword. If $\mathbf{y}$ has distance at least 2 from every codeword, we seek re-transmission. This scheme guarantees the simultaneous correction of single errors and detection of double errors. Note that C could also be used either as a single-error-correcting code or as a triple-error-detecting code, but not both simultaneously (why not?).

6. $(\mathbb{Z}_6, +, \cdot)$ is not a field, since $(\mathbb{Z}_6 - \{0\}, \cdot)$ is not a group.