MAS309 Coding Theory: Sheet 8

Please send comments and corrections to `M.Jerrum@qmul.ac.uk`.
Put solutions in the orange box on the ground floor by 17:00 on 31st March.

1. Write out the parity-check matrix for $\mathrm{Ham}(4, 2)$, in which column j gives the binary representation of the number j. Use this to decode the word `100111000011111`. [4]

2. (a) Use the Gilbert-Varshamov bound to show that a ternary $[7, 2, 5]$-code exists. [2]

   (b) Using one of the standard upper bounds on $A_3(n, d)$, show that no ternary $[7, 3, 5]$-code exists. [3]

   (c) Suppose n, r, d and q satisfy the inequality in the statement of the Gilbert-Varshamov bound. The proof of the bound presented in the lectures/notes provides a method for constructing, column by column, a parity-check matrix for a $[n, n - r, d]$-code over $\mathbb{F}_q$. Use this method to construct a parity check matrix H for the $[7, 2, 5]$-code of part (a). [4]

   Hint: Try looking for a parity-check matrix in standard form. Then you'll have five of the seven columns for free!

3. (a) Suppose $r \geq 1$ and q is a prime power. What is the largest number $n_{r,q}$ for which the Gilbert-Varshamov bound guarantees the existence of a $[n, n-r, 3]$-code over $\mathbb{F}_q$, with $n = n_{r,q}$? [3]

   (b) Verify that $n_{r,q}$ is equal to the length of the Hamming code $\mathrm{Ham}(r, q)$. [1]

   (c) The proof of the Gilbert-Varshamov bound presented in the lectures/notes is constructive. Consider the parity-check matrix H for a $[n, n - r, 3]$-code constructed according to that proof, when $n = n_{r,q}$. Demonstrate that H *is* the parity check matrix for $\mathrm{Ham}(r, q)$ up to permutation of columns, and multiplication of columns by non-zero elements of $\mathbb{F}_q$. [3]

4. (a) Compute the Singleton bound for $A_7(8, 5)$. [1]

   (b) Write down a parity check matrix H for a linear $[8, k, 5]$-code over $\mathbb{F}_7$ that achieves the bound from part (a). [3]

   (c) Compute the syndrome for the word `11111111` $\in \mathbb{F}_7^8$, given your parity-check matrix H from part (b). [1]

Solutions

1.
$$\begin{pmatrix} 000000011111111 \\ 000111100001111 \\ 011001100110011 \\ 101010101010101 \end{pmatrix}.$$

To decode 100111000011111, we calculate the syndrome

$$(100111000011111)\begin{pmatrix} 0001 \\ 0010 \\ 0011 \\ 0100 \\ 0101 \\ 0110 \\ 0111 \\ 1000 \\ 1001 \\ 1010 \\ 1011 \\ 1100 \\ 1101 \\ 1110 \\ 1111 \end{pmatrix} = (1101).$$

This is the binary representation of the number 13, so we change the thirteenth symbol of 100111000011111 to get 100111000011011.

2. (a) In this instance, $n = 7$, $r = n - k = 7 - 2 = 5$, $d = 5$ and $q = 3$. The left-hand side of $(*)$ in Theorem 6.10 evaluates to

$$\begin{aligned} &\binom{7-1}{0} + (3-1)\binom{7-1}{1} + (3-1)^2\binom{7-1}{2} + (3-1)^3\binom{7-1}{3} \\ &= \binom{6}{0} + 2\binom{6}{1} + 2^2\binom{6}{2} + 2^3\binom{6}{3} \\ &= 1 + 2 \times 6 + 4 \times 15 + 8 \times 20 \\ &= 1 + 12 + 60 + 160 \\ &= 233. \end{aligned}$$

Since the right-hand side of $(*)$ is $3^5 = 243$, the Gilbert-Varshamov bound is satisfied. So a ternary $[7, 2, 5]$ code does exist.

(b) Use the Hamming (sphere-packing bound). We are interested in the existence of a code of minimum distance 5: such a code must be 2-error correcting (p.2 of the

course notes). The number V of words in sphere of radius 2 is

$$V = \binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 = 1 + 7 \times 2 + 21 \times 4 = 99.$$

So the Hamming bound (Thm 2.6) is $\lfloor q^n/V \rfloor = \lfloor 2187/99 \rfloor = 22$. Now a ternary $[7, 3, 5]$-code would have $q^k = 3^3 = 27$ codewords, which exceeds the Hamming bound. So no such code exists.

(c) Following the hint, look for a parity-check matrix of the form:

$$H = \begin{pmatrix} h_{11} & h_{12} & 1\,0\,0\,0\,0 \\ h_{21} & h_{22} & 0\,1\,0\,0\,0 \\ h_{31} & h_{32} & 0\,0\,1\,0\,0 \\ h_{41} & h_{42} & 0\,0\,0\,1\,0 \\ h_{51} & h_{52} & 0\,0\,0\,0\,1 \end{pmatrix}$$

We need to choose the column vectors $h_{\cdot 1} = (h_{11}, h_{21}, h_{31}, h_{41}, h_{51})^T$ and $h_{\cdot 2} = (h_{12}, h_{22}, h_{32}, h_{42}, h_{52})^T$ so that any four columns chosen from H are linearly independent. What to we require of $h_{\cdot 1}$ and $h_{\cdot 2}$? Firstly, they must both contain at least four non-zero entries (otherwise they would be linearly dependent on three of the existing columns). And every non-trivial linear combination of $h_{\cdot 1}$ and $h_{\cdot 2}$ must contain at least three non-zero entries (otherwise there would be a linear dependency with two of the existing columns). Those are the only constraints. A possible choice for the two undetermined columns is:

$$H = \begin{pmatrix} 0110000 \\ 1101000 \\ 2100100 \\ 1100010 \\ 2100001 \end{pmatrix}.$$

3. (a) The Gilbert-Varshamov bound asserts that a $[n, n-r, d]$-code exists if

$$\binom{n-1}{0}(q-1)^0 + \cdots + \binom{n-1}{d-2}(q-1)^{d-2} < q^r,$$

i.e., since $d = 3$,

$$\binom{n-1}{0}(q-1)^0 + \binom{n-1}{1}(q-1) < q^r.$$

Simplifying, $1+(n-1)(q-1) < q^r$ or $n-1 < (q^r-1)/(q-1)$. The last inequality is equivalent to $n \leq (q^r-1)/(q-1)$, since both sides are integers. Thus the largest value of n for which a $[n, n-r, d]$-code is guaranteed to exist is $n_{r,q} = (q^r-1)/(q-1)$.

(b) From the notes, $(q^r-1)/(q-1)$ is also the length of the Hamming code $\mathrm{Ham}(r, q)$.

(c) The construction in the proof of the G-V bound forms a matrix H by adding columns $h_1^T, \ldots, h_n^T$ in sequence, subject only to the constraint that no linearly dependent set of at most $d - 1 = 2$ columns is ever created. Equivalently, it allows column h_i to be added if (a) $h_i \neq 0$ and (b) $h_i \neq \lambda h_j$ for all $\lambda \in \mathbb{F}_q \setminus \{0\}$ and $1 \leq j < i$. Recall the equivalence relation $\equiv$ from the notes. We may write (b) as: $h_i \not\equiv h_j$ for all $1 \leq j < i$. Thus the G-V construction will select one representative (arbitrarily) from each equivalence class under $\equiv$ except for the singleton class containing the zero vector. But this is exactly the rule for constructing the parity-check matrix of $\mathrm{Ham}(r, q)$. (The order in which equivalence classes are considered is arbitrary, as is the representative chosen from each equivalence class. But we may bring H to a canonical form by column permutations and column scalings.)

4. (a) $A_7(8, 5) \leq A_7(7, 4) \leq \cdots \leq A_7(4, 1) = 7^4$.

(b) We use the MDS code from the notes. If we are to achieve the bound from (a) we need $k = 4$, and hence $r = n - k = 8 - 4 = 4$. The required parity check matrix is

$$\begin{pmatrix} 1&1&1&1&1&1&1&0 \\ 0&1&2&3&4&5&6&0 \\ 0&1&4&2&2&4&1&0 \\ 0&1&1&6&1&6&6&1 \end{pmatrix}.$$

(The first seven columns are obtained by taking powers $1, \lambda^1, \lambda^2, \lambda^3$ of all field elements $\lambda \in \mathbb{F}_7$.)

(c) The syndrome is $S(\texttt{11111111}) = \texttt{0001}$ (independent of the ordering of the columns of H).