QDCS : Digrammatic Calculus and Error Correction

Renaud Vilmart

TD 4

1 A Small Linear Code

Let $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ be the generating matrix of code C.

Question 1. Enumerate all codewords in C. What is the minimal distance of C?

Question 2. What are the dimension and the length of C?

Question 3. Give a parity-check matrix associated to C.

2 A Linear Code

Let C be the binary code with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Note that any column of H has weight 3.

Question 1. Prove that the code has minimum distance > 3.

Question 2. Give a codeword of weight 4 of C.

Question 3. Prove that any word of C has an even weight.

Answer:

(1) Since there is no zero column, the minimum distance is > 1. Since there is no two column which are equal, the minimum distance is > 2. Finally, any column has weight 3. Thus the sum of two distinct columns has weight either 2 (if the columns match at two positions) or 4 or 6. Thus the sum of 3 distinct columns is always nonzero and hence, the minimum distance is > 3.

(2) (1 1 0 0 0 0 0 0 0 0 0 0 1 1).

(3) It suffices to check that the sum of r distinct columns of H with r odd is never 0. For this sake we will prove that the sum of an odd number of columns is odd. Note that the weight of a word of $\mathbb{F}_2^6$ modulo 2 equals the inner product of the word with $u := (1\ 1\ 1\ 1\ 1\ 1\ 1)$. Any column of H has odd weight and hence an inner product 1 with u. By linearity, the sum of an odd number of columns of H has also inner product 1 with u and hence has odd weight.

According to the lecture notes, codewords are in correspondence with tuples of columns of a parity–check matrix which sum to zero. Therefore, the code C has only even weights.

3 Intuitions on Linear Codes

Let $C \subseteq \mathbb{F}_2^n$ be an $[n, k, d]$ code and G, H be respectively a generator and a parity check matrix of C. In what follow we list operations on G yielding a new matrix G'. For any one:

- does G' generate the same code?
- if not,
  - has the new code generated by G' the same length?
  - a larger dimension?
  - a smaller dimension?
  - might this code have a larger minimum distance?
  - a smaller minimum distance?

(1) Removing a row;

(2) swapping two rows;

(3) removing a column;

(4) swapping two columns;

(5) adding an additional row drawn at random;

(6) adding an additional row defined as the sum of all the other rows;

(7) adding an additional column defined as the sum of all the other columns.

Same questions when the operations are applied to H.
Answer:

(1) Removing a row changes the code and provides a new code C' of the same length which is a subcode of C. Hence the dimension could be reduced by one unless G was not full rank and the deleted row was a linear combination of the other ones. In terms of minimum distance, the new code is a subcode and hence might have a larger minimum distance. The minimum distance is at least the same.

(2) swapping two rows does not change the code : the code is generated by the rows of the matrix. No matter how they are sorted.

(3) removing a column changes the code and provides a new code C' of length $n-1$. The new code has the same dimension unless the i–th column has been removed and C contained the codeword of weight 1:

$$(0 \ \cdots \ 0 \ 1 \ 0 \ \cdots \ 0)$$

where the 1 is at the i–th position. In terms of minimum distance, if C has minimum weight codewords with a nonzero entry at the deleted position, then the new code C' has codewords of weight $d-1$ but not less if not, the minimum weight codewords of C' remains d. Hence the new code C' has a minimum distance d' which is either $d-1$ or d.

(4) swapping two columns changes the code and provides a new code C' of the same length n. The new code is obtained by the map consisting in swapping entries at a position i and a position j. This map is bijective and preserves the Hamming weight (it is an isometry with respect to the Hamming distance). Hence, C' has the same dimension and minimum distance.

(5) adding an additional row drawn at random provides a new code C' of the same length and that contains C. If the new row is in C and hence is a linear combination of the rows of G, then $C' = C$ else $C \subsetneq C'$ and C' has dimension $k+1$ and its minimum distance is at most d but might be less.

(6) adding an additional row defined as the sum of all the other rows does not change the code since the new row is a linear combination of the other ones and hence the space spanned by the rows remains the same.

(7) adding an additional column defined as the sum of all the other columns changes the code and provides a new code C' of length $n+1$. This new code is obtained from C by joining at the end of any codeword the sum of its entries. The dimension of C' is still k since the rank of G is unchanged. In terms of minimum distance, the minimum distance is unchanged if there are minimum weight codewords whose sum of entries is zero. If not, then the minimum distance is $d+1$.

Same questions when the operations are applied to H:

(1) Removing a row of H changes the code and provides a new code C' of the same length which contains of C. Hence the dimension could be increased by one unless H was not full rank and the deleted row was a linear combination of the other ones. In terms of minimum distance, the new code contains C and hence might have a smaller minimum distance. The minimum distance is at most the same.

(2) swapping two rows does not change the code.

(3) removing a column changes the code and provides a new code C' of length $n-1$. If the i–th column of H is removed, the new code is obtained from C by keeping only the codewords whose i–th entry is zero and by removing this entry. It is the *shortening of* C at position i.

This new code has dimension $k-1$ unless the i–th column has been removed and any codeword in C has its i–th entry equal to 0.

In terms of minimum distance, C' is constructed from the subcode of C of words whose i–th entry is 0. Therefore, the minimum distance of C' is at least d and might be larger.

(4) swapping two columns changes the code and provides a new code C' of the same length n. The new code is obtained by the map consisting in swapping entries at a position i and a position j exactly as in the case of swapping columns of a generator matrix.

(5) adding an additional row drawn at random provides a new code C' of the same length and that is contained in C. If the new row is in C and hence is a linear combination of the rows of G, then $C' = C$ else $C \subsetneq C'$ and C' has dimension $k-1$ and its minimum distance is at least d but might be larger.

(6) adding an additional row defined as the sum of all the other rows does not change the code since the new row is a linear combination of the other ones and hence the space spanned by the rows remains the same.

(7) adding an additional column defined as the sum of all the other columns changes the code and provides a new code C' of length $n+1$. This new code is obtained from C by joining at the end of any codeword the entry 0 and adding as an additional generator the codeword $(1\ 1\ \cdots\ 1)$. The dimension of C' is still k since the rank of H is unchanged. In terms of minimum distance, the minimum distance is at most d but might be less.

4 Y Errors

Consider the Pauli operator $Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$

Question 1. Compute the eigenvalues and eigenstates of Y.

Answer: $1, -1$ and the corresponding vectors are eigenvectors

$$u = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, v = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}.$$

Question 2. Give an orthonormal basis of $\mathcal{H}$ whose elements are swapped by Y.

Answer: Y is diagonalisable in the basis

$$u = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}, v = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}.$$

This basis is orthonormal for the Hermitian product and the basis:

$$\frac{1}{\sqrt{2}}(u+v) = |0\rangle\,,\ \frac{1}{\sqrt{2}}(u-v) = -i\,|1\rangle$$

is orthonormal too and its elements are swapped by Y.

Question 3. Deduce an encoding of one qubit into three which permits to correct an error in Y on one qubit.

Answer: Up to some phase, Y flips $|0\rangle$ and $|1\rangle$. Therefore, one can perform the same encoding as for correcting one error in X, namely, encoding one qubit $|\varphi\rangle = a\,|0\rangle + b\,|1\rangle$ into:

$$|\varphi\rangle\,|00\rangle \mapsto a\,|000\rangle + b\,|111\rangle\,.$$

Next a syndrome measurement leads to a state of the form $ia\,|100\rangle - ib\,|011\rangle$ or $ia\,|010\rangle - ib\,|101\rangle$ or $ia\,|001\rangle - ib\,|110\rangle$, then applying one of the operators $Y \otimes I \otimes I$ or $I \otimes Y \otimes I$ or $I \otimes I \otimes Y$ leads to the original state.

5 Admissible Pauli Subgroup

Question 1. Show that any subgroup of $\mathcal{P}_n$ that does not contain $-I \otimes ... \otimes I$ is abelian.
Hint: First show that any element in the subgroup is involutive.

Answer: Let $\mathcal{G}$ be a subgroup of $\mathcal{P}_n$ that does not contain $-I \otimes ... \otimes I$. Let $A = i^k P_1 \otimes ... \otimes P_n \in \mathcal{G}$. Since Pauli matrices are involutive, $A^2 = i^{2k} P_1^2 \otimes ... \otimes P_n^2 = i^{2k} I \otimes ... \otimes I$. Since $-I \otimes ... \otimes I$ is not in the group, but A^2 is, $k \in \{0, 2\}$. Hence, A is involutive. Let $A, B \in \mathcal{G}$. Suppose A and B don't commute. Since they are Pauli strings, they anticommute: $AB = -BA$. Then $ABAB = -AABB = -I \otimes ... \otimes I$ which is not possible by hypothesis. Hence A and B commute. This is true for every pair of elements in $\mathcal{G}$, so it is abelian.