Problem 7. A unique decoding

Dung Le Quoc

October 19, 2023

1 Problem

Consider a binary error-correcting code $\mathcal{C}$ of length n. Obtaining some $\boldsymbol{y} \in \mathbb{F}_2^n$, we suppose that the number of errors happend, say $d_{\boldsymbol{y}}$, is minimal possible, i.e.

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} wt(\boldsymbol{x} \oplus \boldsymbol{y})$$

Next, let $\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : wt(\boldsymbol{x} \oplus \boldsymbol{y}) = d_{\boldsymbol{y}}\}$. Finally, we decode $\boldsymbol{y}$ into any $\boldsymbol{x} \in \mathcal{D}(\boldsymbol{y})$.

We are interested in all cases of codes for which

$$|\mathcal{D}(\boldsymbol{y})| = 1, \quad \text{for all } \boldsymbol{y} \in \mathbb{F}_2^n \tag{1}$$

2 Solution

This solution can be applied for both two questions.

Remark 1

If code $\mathcal{C} \equiv \mathbb{F}_2^n$. Then $\mathcal{C}$ satisfies property about $\mathcal{D}(\boldsymbol{y})$.

Proof. For every vector $\boldsymbol{y} \in \mathbb{F}_2^n$, we take $\boldsymbol{x} \equiv \boldsymbol{y} \in \mathcal{C}$. So for each vector $\boldsymbol{y} \in \mathbb{F}_2^n$,

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$$

when $\boldsymbol{x} \equiv \boldsymbol{y}$.

As the result, only one vector $\boldsymbol{x} \in \mathcal{C}$ can give $d_{\boldsymbol{y}} = 0$. In other word

$$\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : \boldsymbol{x} \equiv \boldsymbol{y}\}$$

For each vector $\boldsymbol{y} \in \mathbb{F}_2^n$, the set $\mathcal{D}(\boldsymbol{y})$ contains only one element. So when code $\mathcal{C} \equiv \mathbb{F}_2^n$, it satisfies given property. □

Conclusion 1

For all $n \geq 1$, the code $\mathcal{C} \equiv \mathbb{F}_2^n$ satisfies property (1).

Remark 2

Considering $\mathbb{F}_2^n$, if we take above half of $\mathbb{F}_2^n$ (in decimal they are numbers from 0 to $2^{n-1} - 1$) as code $\mathcal{C}$, then this code also satisfies property (1).

Proof. Every vector of above half of $\mathbb{F}_2^n$ have form

$$\boldsymbol{x} = (0, x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_2^n, \quad x_i \in \mathbb{F}_2$$

Or I can say that

$$\mathcal{C} = \{\boldsymbol{x} = (0, x_1, x_2, \ldots, x_{n-1}), x_i \in \mathbb{F}_2\}$$

Now consider $\boldsymbol{y} \in \mathbb{F}_2^n$.

First case. Vector $\boldsymbol{y}$ has form

$$\boldsymbol{y} = (0, y_1, y_2, \ldots, y_{n-1}) \in \mathbb{F}_2^n$$

In decimal, vector $\boldsymbol{y}$ is equivalent with number from 0 to $2^{n-1} - 1$.

Then in $\mathcal{C}$ exists only one vector $\boldsymbol{x}$ such that $\boldsymbol{x} \equiv \boldsymbol{y}$. In other word $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$.

So for every vector $\boldsymbol{y} = (0, y_1, y_2, \ldots, y_{n-1})$, we have

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$$

As the result,

$$\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : \boldsymbol{x} \equiv \boldsymbol{y}\}$$

and this set contains only one element $\boldsymbol{x} \equiv \boldsymbol{y}$.

Second case. Vector $\boldsymbol{y}$ has the form

$$\boldsymbol{y} = (1, y_1, y_2, \ldots, y_{n-1}) \in \mathbb{F}_2^n$$

In decimal, vector $\boldsymbol{y}$ is equivalent with number from from 2^{n-1} to $2^n - 1$.

Then in $\mathcal{C}$ exists only one vector $\boldsymbol{x} = (0, y_1, y_2, \ldots, y_{n-1})$. In other word $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 1$.

So for every vector $\boldsymbol{y} = (1, y_1, y_2, \ldots, y_{n-1})$, we have

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 1$$

As the result, if $\boldsymbol{y} = (1, y_1, y_2, \ldots, y_{n-1})$ then

$$\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : \boldsymbol{x} = (0, y_1, y_2, \ldots, y_{n-1})\}$$

and this set contains only one element, too.

In both cases, we see that if code $\mathcal{C}$ defined as

$$\mathcal{C} = \{\boldsymbol{x} = (0, x_1, x_2, \ldots, x_n), x_i \in \mathbb{F}_2\} \tag{2}$$

Then code $\mathcal{C}$ satisfies given property and we finish our proof. □

Example 1. *For $n = 4$, then*

$$\mathcal{C} = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111\}$$

Conclusion 2

Code of length n

$$\mathcal{C} = \{(0, x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_2^n, x_i \in \mathbb{F}_2\}$$

satisfies property in (1).

Now we write all vector in $\mathcal{C}$ as rows of matrix $\boldsymbol{C}$. Then we permutate its columns. For example, for $n = 4$ and code $\mathcal{C}$ as above, we write

$$\boldsymbol{C} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Now we change position of the first and third columns, and change position of the second and fourth columns. We can do this by multiple matrix $\boldsymbol{C}$ to matrix $\boldsymbol{A}$ such that

$$\boldsymbol{A} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

We have the result

$$\boldsymbol{C} \cdot \boldsymbol{A} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

In the result, we have exchanged position of first and third columns, and the same for second and fourth columns.

We can see that, in any way of changing position of columns, matrix $\boldsymbol{A}$ is always invertible. Matrix $\boldsymbol{A}$ has only one element (number 1) on each column and each row, so its determinant is ± 1.

Return to our problem, let $\boldsymbol{A}$ is the matrix that changing position of columns in matrix $\boldsymbol{C}$. Then let

$$\mathcal{C}' = \{\boldsymbol{x} \cdot \boldsymbol{A} : \boldsymbol{x} \in \mathcal{C}\}$$

For every vector $\boldsymbol{y} \in \mathbb{F}_2^n$, let $\boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A}$. Because $\boldsymbol{A}$ is invertible matrix, the map

$$\boldsymbol{A} : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n, \quad \boldsymbol{y} \mapsto \boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A} \tag{3}$$

is bijection from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.

Also because $\boldsymbol{A}$ is invertible matrix, then the map

$$\boldsymbol{A} : \mathcal{C} \mapsto \mathcal{C}', \quad \boldsymbol{x} \to \boldsymbol{x'} = \boldsymbol{x} \cdot \boldsymbol{A} \tag{4}$$

is also bijection from $\mathcal{C}$ to $\mathcal{C}'$.

Now we will prove that code $\mathcal{C}'$ also satisfies property (1).

Proof. **First case.** If $\boldsymbol{y}$ has the form $(0, y_1, y_2, \ldots, y_{n-1})$, in code $\mathcal{C}$ has element $\boldsymbol{x} = (0, y_1, y_2, \ldots, y_{n-1})$, and $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$ is minimal weight among vectors $\boldsymbol{y}$ of that form.

From here, if $\boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A} \in \mathbb{F}_2^n$, then from $\boldsymbol{x'} = \boldsymbol{x} \cdot \boldsymbol{A} \in \mathcal{C}'$ we will have

$$wt(\boldsymbol{x'} \oplus \boldsymbol{y'}) = wt((\boldsymbol{x} \cdot \boldsymbol{A}) \oplus (\boldsymbol{y} \cdot \boldsymbol{A})) = wt((\boldsymbol{x} \oplus \boldsymbol{y}) \cdot \boldsymbol{A}) = wt(\boldsymbol{0} \cdot \boldsymbol{A}) = 0$$

Here I wrote $\boldsymbol{0}$ as zero-vector $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$. This means that $d_{\boldsymbol{y'}} = 0$.

From here it is similar to proof above (for code $\mathcal{C}$), which means if $\boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A}$, then

$$\mathcal{D}(\boldsymbol{y'}) = \{\boldsymbol{x'} = \boldsymbol{x} \cdot \boldsymbol{A} : \boldsymbol{x} = \boldsymbol{y}\}$$

and this set has only one element.

Second case. Similarly, if $\boldsymbol{y}$ has the form $(1, y_1, y_2, \ldots, y_{n-1})$, in code $\mathcal{C}$ has element $\boldsymbol{x} = (1, y_1, y_2, \ldots, y_{n-1})$ and $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 1$ is minimal weight among vectors $\boldsymbol{y}$ of that form.

From here, if $\boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A} \in \mathbb{F}_2^n$, then with $\boldsymbol{x'} = \boldsymbol{x} \cdot \boldsymbol{A}$ we will have

$$wt(\boldsymbol{x'} \oplus \boldsymbol{y'}) = wt((\boldsymbol{x} \cdot \boldsymbol{A}) \oplus (\boldsymbol{y} \cdot \boldsymbol{A})) = wt((\boldsymbol{x} \oplus \boldsymbol{y}) \cdot \boldsymbol{A}) = wt((1, 0, 0, \ldots, 0) \cdot \boldsymbol{A}) = 1$$

This is because each column of matrix $\boldsymbol{A}$ contains only one element 1, so only column $(1, 0, 0, \ldots, 0)^T$ will give product 1, other columns will give product 0. As a result, received vector has only one element 1 and its Hamming weight is 1.

So, if $\boldsymbol{y'} = \boldsymbol{y} \cdot \boldsymbol{A}$ where $\boldsymbol{y} = (1, y_1, y_2, \ldots, y_{n-1})$ then

$$\mathcal{D}(\boldsymbol{y'}) = \{\boldsymbol{x'} = \boldsymbol{x} \cdot \boldsymbol{A} : \boldsymbol{x} = (1, y_1, y_2, \ldots, y_{n-1}) \in \mathbb{F}_2^n\}$$

and this set has only one element.

In both cases, $\mathcal{D}(\boldsymbol{y'})$ contains only one element, we finish our proof. $\square$

From the conclusion above, I have said that every code $\mathcal{C}$ containing vectors $(0, x_1, x_2, \ldots, x_{n-1})$ satisfies property (1).

This code is linear supspace of $\mathbb{F}_2^n$ with basis is set of vectors

$$\begin{aligned}\boldsymbol{v}_1 &= (0, 1, 0, 0, \ldots, 0),\\ \boldsymbol{v}_2 &= (0, 0, 1, 0, \ldots, 0),\\ \cdots &= \cdots\\ \boldsymbol{v}_{n-1} &= (0, 0, 0, 0, \ldots, 1)\end{aligned}$$

When we multiply these vectors to matrix $\boldsymbol{A}$ in order to change position of columns, we received another basis of another linear supspace in $\mathbb{F}_2^n$. As a result, code $\mathcal{C}'$ as defined above is also linear subspace spanned by new basis

$$\{\boldsymbol{v}_1 \cdot \boldsymbol{A}, \boldsymbol{v}_2 \cdot \boldsymbol{A}, \ldots, \boldsymbol{v}_{n-1} \cdot \boldsymbol{A}\}.$$

So I can conclude that:

Conclusion 3

Code $\mathcal{C}$, which is linear supspace of $\mathbb{F}_2^n$ spanned from $n-1$ vectors in n following vectors

$$\begin{aligned}\boldsymbol{v}_1 &= (1, 0, 0, \ldots, 0),\\ \boldsymbol{v}_2 &= (0, 1, 0, \ldots, 0),\\ \cdots &= \cdots\\ \boldsymbol{v}_n &= (0, 0, 0, \ldots, 1)\end{aligned}$$

satisfies property (1). This code then has 2^{n-1} elements and dimension $n-1$.

If code $\mathcal{C}$ is linear supspace spanned by all these n vectors, then $\mathcal{C} \equiv \mathbb{F}_2^n$, which is also satisfies property (1) as I proved at the beginning.

Now let's consider linear supspace spanned by $n-2$ vectors from n vectors above.

If code $\mathcal{C}$ is spanned $n-2$ vectors, it also satisfies property (1).

We can easily notice that, in general, suppose that basis contain

$$\begin{aligned}\boldsymbol{v}_1 &= (0, 0, 1, 0, \ldots, 0),\\ \boldsymbol{v}_2 &= (0, 0, 0, 1, \ldots, 0),\\ \cdots &= \cdots,\\ \boldsymbol{v}_{n-2} &= (0, 0, 0, 0, \ldots, 1)\end{aligned}$$

then all vectors in code $\mathcal{C}$ have 2 first elements is zero. This code also satisfies property (1).

Remark 3

Code $\mathcal{C}$ containing above one-forth of $\mathbb{F}_2^n$ (in decimal they are numbers from 0 to $2^{n-2}-1$) satisfies property (1). In other word

$$\mathcal{C} = \{\boldsymbol{x} = (0, 0, x_1, x_2, \ldots, x_{n-2}) : x_i \in \mathbb{F}_2\}$$

Proof. **First case.** Vector $\boldsymbol{y} \in \mathbb{F}_2^n$ has the form

$$\boldsymbol{y} = (0, 0, y_1, y_2, \ldots, y_{n-2}) \in \mathbb{F}_2$$

In decimal, vector $\boldsymbol{y}$ is equivalent to number from 0 to $2^{n-2}-1$.

Then in $\mathcal{C}$ exists only one vector $\boldsymbol{x} = (0, 0, y_1, y_2, \ldots, y_{n-2})$. In other word $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$ is minimal weight. This means that for every vector $\boldsymbol{y} = (0, 0, y_1, y_2, \ldots, y_{n-2})$, we have

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 0$$

As the result, $\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : \boldsymbol{x} = (0, 0, y_1, y_2, \ldots, y_{n-2})\}$, which means $|\mathcal{D}(\boldsymbol{y})| = 1$.

Second cases. Vector $\boldsymbol{y} \in \mathbb{F}_2^n$ has the form

$$\boldsymbol{y} = (0, 1, y_1, y_2, \ldots, y_{n-2}) \in \mathbb{F}_2^n$$

In decimal, vector $\boldsymbol{y}$ is equivalent to number from 2^{n-2} to $2^{n-1}-1$.

Then in $\mathcal{C}$ exists only one vector $\boldsymbol{x} = (0, 0, y_1, y_2, \ldots, y_{n-2})$. In other word $wt(\boldsymbol{x} \oplus \boldsymbol{y}) = 1$ is minimal weight. This means that for every vector $\boldsymbol{y} = (0, 1, y_1, y_2, \ldots, y_{n-2})$, we have

$$d_{\boldsymbol{y}} = \min_{\boldsymbol{x} \in \mathcal{C}} = 0$$

As the result, $\mathcal{D}(\boldsymbol{y}) = \{\boldsymbol{x} \in \mathcal{C} : \boldsymbol{x} = (0, 0, y_1, y_2, \ldots, y_{n-2})\}$, which means $|\mathcal{D}(\boldsymbol{y})| = 1$.

Third cases. Vectors $\boldsymbol{y} = (1, 0, y_1, y_2, \ldots, y_{n-2})$ also give $|\mathcal{D}(\boldsymbol{y})| = 1$.

Fourth cases. Vectors $\boldsymbol{y} = (1, 1, y_1, y_2, \ldots, y_{n-2})$ also give $|\mathcal{D}(\boldsymbol{y})| = 1$.

So in all cases of vector $\boldsymbol{y} \in \mathbb{F}_2^2$, code $\mathcal{C}$ gives us $|\mathcal{D}(\boldsymbol{y})| = 1$. We finish our proof. □

By induction, we can see following remark.

Remark 4

Code $\mathcal{C}$ of length n containing first $\dfrac{1}{2^i}$ where $0 \leq i \leq n$ satisfies property (1). In other word

$$\mathcal{C} = \{\boldsymbol{x} = (0, 0, \ldots, 0, x_1, x_2, \ldots, x_{n-i}) : x_i \in \mathbb{F}_2\} \tag{5}$$

where $\boldsymbol{x}$ starts with i zero numbers.

Similarly to above, if we write all vectors in code $\mathcal{C}$ as rows of a matrix $\boldsymbol{C}$ and exchange its columns, it is equivalent to multiply matrix $\boldsymbol{C}$ with invertible matrix $\boldsymbol{A}$ that has only one elemnt (number 1) on each row and on each column.

Then, if code

$$\mathcal{C} = \{\boldsymbol{x} = (0, 0, \ldots, 0, x_1, x_2, \ldots, x_{n-i}) : x_i \in \mathbb{F}_2\},$$

if we multiply all its vectors to matrix $\boldsymbol{A}$ then we receive new code also satisfies property (1).

$$\mathcal{C}' = \{\boldsymbol{x}' = \boldsymbol{x} \cdot \boldsymbol{A} : \boldsymbol{x} \in \mathcal{C}\}$$

We can see that code $\mathcal{C}$ is linear supspace spanned by i vectors

$$\begin{aligned}
\boldsymbol{v}_1 &= (0, 0, \ldots, 0, 1, 0, \ldots, 0),\\
\boldsymbol{v}_2 &= (0, 0, \ldots, 0, 0, 1, \ldots, 0),\\
\cdots &= \cdots,\\
\boldsymbol{v}_i &= (0, 0, \ldots, 0, 0, 0, \ldots, 1)
\end{aligned}$$

Therefore, every code $\mathcal{C}'$, which is receive by multiply all its vectors to matrix $\boldsymbol{A}$, is also a linear supspace spanned by

$$\begin{aligned}
\boldsymbol{v}'_1 &= \boldsymbol{v}_1 \cdot \boldsymbol{A},\\
\boldsymbol{v}'_2 &= \boldsymbol{v}_2 \cdot \boldsymbol{A},\\
\cdots &= \cdots,\\
\boldsymbol{v}'_i &= \boldsymbol{v}_i \cdot \boldsymbol{A}
\end{aligned}$$

So the answer for the problem (in both Q1 and Q2) is

Conclusion 4

Code $\mathcal{C}$, which is linear supspace of $\mathbb{F}_2^n$ spanned by $0, 1, \ldots, n$ vectors in n following vectors

$$\begin{aligned}
\boldsymbol{v}_1 &= (1, 0, 0, \ldots, 0),\\
\boldsymbol{v}_2 &= (0, 1, 0, \ldots, 0),\\
\cdots &= \cdots,\\
\boldsymbol{v}_n &= (0, 0, 0, \ldots, 1)
\end{aligned}$$

satisfies property (1), or $|\mathcal{D}(\boldsymbol{y})| = 1$ for all $\boldsymbol{y} \in \mathbb{F}_2^n$.

Example 2. *For $n = 3$, all codes that satisfy given property are*

$$
\begin{aligned}
&\mathcal{C}_1 = \{000\},\\
&\mathcal{C}_2 = \{000, 001\},\\
&\mathcal{C}_3 = \{000, 010\},\\
&\mathcal{C}_4 = \{000, 100\},\\
&\mathcal{C}_5 = \{000, 001, 010, 011\},\\
&\mathcal{C}_6 = \{000, 001, 100, 101\},\\
&\mathcal{C}_7 = \{000, 010, 100, 110\},\\
&\mathcal{C}_8 = \{000, 001, 010, 011, 100, 101, 110, 111\}
\end{aligned}
$$

Remark 5

The number of codes that are linear supspace are the number of ways choosing basis vectors. There are n vectors $\boldsymbol{v}$, and we choose $0, 1, \ldots, n$ vectors from them. So as the result there are

$$C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$$

codes $\mathcal{C}$ satisfying our problem.