32031 Feedback Quiz, 2022/23, Week 05: The dual code

Open-book. 10–15 minutes. Not for credit. To be marked in class.

- The inner product $\underline{x} \cdot \underline{y}$ of vectors $\underline{x}, \underline{y} \in \mathbb{F}_q^n$ is defined as $\underline{x} \cdot \underline{y} = \sum_{i=1}^n x_i y_i$.
- If $C \subseteq \mathbb{F}_q^n$ is a linear code, the dual code $C^\perp$ is $\{\underline{v} \in \mathbb{F}_q^n : \underline{v} \cdot \underline{c} = 0 \text{ for all } \underline{c} \in C\}$ (that is: $C^\perp$ consists of all vectors orthogonal to C).
- By a theorem from the course, $\dim C^\perp = n - \dim C$.
- A generator matrix H for $C^\perp$ is called a *check matrix* for C. By a theorem from the course, $C = \{\underline{c} \in \mathbb{F}_q^n : \underline{c}H^T = \underline{0}\}$.
- Recall: ISBN10 = $\{\underline{x} \in \mathbb{F}_{11}^{10} : 1x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} = 0 \text{ in } \mathbb{F}_{11}\}$.

Question 1 (*warm-up*) The dimension of the ISBN-10 code is:

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11

Question 2 You can see from the definition of ISBN10 that the vector $\underline{v} = 123456789X$ belongs to $(\text{ISBN10})^\perp$. Does $\underline{v}$ belong to ISBN10?

○ Yes ○ No

Question 3 ♣ From Question 1 you can hopefully conclude that $\dim(\text{ISBN10})^\perp = 1$. Use this fact and the vector $\underline{v}$ from Question 2 to write down a vector $w \in (\text{ISBN10})^\perp$ where the sixth symbol is 5:

$\underline{w} = \square\square\square\square\square\boxed{5}\square\square\square\square$.

Question 4 ♣ (*correcting an **erasure** in an ISBN*) Recover the missing symbol in an ISBN:

0198 $\square$ 38030

CORRECTED

32031 Feedback Quiz, 2022/23, Week 05: The dual code

Open-book. 10–15 minutes. Not for credit. To be marked in class.

- The inner product $\underline{x} \cdot \underline{y}$ of vectors $\underline{x}, \underline{y} \in \mathbb{F}_q^n$ is defined as $\underline{x} \cdot \underline{y} = \sum_{i=1}^n x_i y_i$.
- If $C \subseteq \mathbb{F}_q^n$ is a linear code, the dual code $C^\perp$ is $\{\underline{v} \in \mathbb{F}_q^n : \underline{v} \cdot \underline{c} = 0 \text{ for all } \underline{c} \in C\}$ (that is: $C^\perp$ consists of all vectors orthogonal to C).
- By a theorem from the course, $\dim C^\perp = n - \dim C$.
- A generator matrix H for $C^\perp$ is called a *check matrix* for C. By a theorem from the course, $C = \{\underline{c} \in \mathbb{F}_q^n : \underline{c}H^T = \underline{0}\}$.
- Recall: ISBN10 = $\{\underline{x} \in \mathbb{F}_{11}^{10} : 1x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} = 0 \text{ in } \mathbb{F}_{11}\}$.

Question 1 (*warm-up*) The dimension of the ISBN-10 code is:

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ☒ 9 ○ 10 ○ 11

Explanation: The first 9 symbols $x_1, \ldots, x_9$ of an ISBN codevector are arbitrary elements of $\mathbb{F}_1 1$, and the last symbol x_{10} is uniquely determined by $x_1, \ldots, x_9$ according to the formula $x_{10} = 1x_1 + 2x_2 + \cdots + 9x_9$, to make sure that the checksum is 0. Hence the code consists of $11^9 \times 1$ codevectors, and $k = \log_{11}(11^9) = 9$.

Question 2 You can see from the definition of ISBN10 that the vector $\underline{v} = 123456789X$ belongs to $(\text{ISBN10})^\perp$. Does $\underline{v}$ belong to ISBN10?

☒ Yes ○ No

Explanation: We need to check if $\underline{v} \cdot \underline{v} = 0$ in $\mathbb{F}_{11}$. This amounts to calculating $1 \times 1 + 2 \times 2 + \cdots + 10 \times 10$ modulo 11. One can use brute force, e.g., 1^2 is 1 in $\mathbb{F}_{11}$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$, $5^2 = 3$, $1 + 4 + 9 + 5 + 3 = 22 = 0$, and $6^2 + 7^2 + 8^2 + 9^2 + 10^2 = (-5)^2 + (-4)^2 + (-3)^2 + (-2)^2 + (-1)^2$ gives the same result, 0. One can also use the formula $1^2 + 2^2 + \cdots + k^2 = k(k+1)(2k+1)/6$ which for $k = 10$ gives $10(11)(21)/6$ which is a multiple of 11

Question 3 ♣ From Question 1 you can hopefully conclude that $\dim(\text{ISBN10})^\perp = 1$. Use this fact and the vector $\underline{v}$ from Question 2 to write down a vector $w \in (\text{ISBN10})^\perp$ where the sixth symbol is 5:

$\underline{w} =$ | X | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |.

Explanation: Since the code $(\text{ISBN10})^{\perp}$ is one-dimensional, and $\underline{v} = 123456789X$ is a non-zero vector which belongs to $(\text{ISBN10})^{\perp}$, every vector in $(\text{ISBN10})^{\perp}$ must be proportional to $\underline{v}$. So $\underline{w} = \lambda \underline{v}$ for some $\lambda \in \mathbb{F}_{11}$. In particular, $5 = \lambda \times 6$ in $\mathbb{F}_{11}$. It follows that $\lambda = -1$ and so $\underline{w} = -\underline{v}$, as shown above.

Question 4 ♣ (*correcting an **erasure** in an ISBN*) Recover the missing symbol in an ISBN:

$$\mathbf{0198\ \boxed{5}\ 38030}$$

Explanation: **Note:** Different valid ISBNs appear in different versions of this question. They should all be ISBNs of real books — check yours!
Calculate the checksum: $1(0)+2(1)+3(9)+4(8)+5(\boxed{?})+6(3)+7(8)+8(0)+9(3)+10(0) = 162+5?$ which is $8+5?$ in $\mathbf{F}_{11}$. So $5? = 3$ in $\mathbf{F}_{11}$. Trial and error gives $? = 5$: indeed, $5 \times 5 = 3$ in $\mathbf{F}_{11}$.