Week 5

The dual code. Syndrome decoding

Version 2023-11-01. To accessible online version of this chapter

Synopsis. *Every linear code C has a dual code, $C^\perp$, and check matrices. While a generator matrix G is used to encode messages into codevectors, a check matrix H serves to detect errors — and to correct them using syndrome decoding.*

Motivation. The inner product of vectors

Let C be a linear code. Given a received vector $\underline{y}$, how to test whether $\underline{y} \in C$? Storing all codevectors of C is not an option for codes of large length and dimension, whose use is dictated by modern applications to low-noise channels. Storing just a generator matrix G of C is better in terms of storage space, but testing whether $\underline{y}$ is in the row space of G can be computationally demanding.

Some codes, however, are defined by a single *checksum* — recall the even weight code and the ISBN-10 code. A checksum of a given vector is easy to compute.

Extending the checksum approach, we introduce a *check matrix* which generates the *dual code*. It turns out that this construction helps to correct errors as well (not just detect). The first notion we need is:

Definition: inner product

For $\underline{u}, \underline{v} \in \mathbb{F}_q^n$, the scalar (element of $\mathbb{F}_q$) defined as $\underline{u} \cdot \underline{v} = \sum_{i=1}^n u_i v_i$ is called the **inner product** of the vectors $\underline{u}$ and $\underline{v}$.

Example: some inner products in $\mathbb{F}_2^3$

For $111, 101 \in \mathbb{F}_2^3$, one has

$$111 \cdot 111 = 1^2+1^2+1^2 = 1,\ 111 \cdot 101 = 1 \cdot 1+1 \cdot 0+1 \cdot 1 = 0,\ 101 \cdot 101 = 1^2+0^2+1^2 = 0.$$

If $C \subset \mathbb{F}_q^n$ is a set, $\underline{v} \in \mathbb{F}_q^n$, we may write $\underline{v} \cdot C$ to denote the set $\{\underline{v} \cdot \underline{c} \mid \underline{c} \in C\}$.

Properties of the inner product

(1) **Expression as a matrix product:** $\underline{u} \cdot \underline{v} = \underline{u}\,\underline{v}^T$.

Explanation: we write elements of $\mathbb{F}_q^n$ as row vectors. Thus, $\underline{u}$ is a row vector $(u_1, \ldots, u_n)$, and $\underline{v}^T$ is the transpose of $\underline{v}$, so a column vector $\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$. Multiplying $\underline{u}$, an $1 \times n$ matrix, and $\underline{v}^T$, an $n \times 1$ matrix, we obtain a 1×1 matrix, which we identify with a scalar in $\mathbb{F}_q$.

(2) **Symmetry:** $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$. (**Explanation:** this is easily seen from the definition.)

(3) **Bilinearity:** for a scalar $\lambda \in \mathbb{F}_q$ we have $(\underline{u} + \lambda \underline{w}) \cdot \underline{v} = \underline{u} \cdot \underline{v} + \lambda(\underline{w} \cdot \underline{v})$ and $\underline{u} \cdot (\underline{v} + \lambda w) = \underline{u} \cdot \underline{v} + \lambda(\underline{u} \cdot \underline{w})$. (**Explanation:** from linear algebra, the matrix product in $\underline{u}\,\underline{v}^T$ is bilinear.)

(4) **Non-degeneracy:** $\underline{u} \cdot \mathbb{F}_q^n = \{0\}$, if and only if $\underline{u} = 0$.

Explanation: let $\underline{\epsilon_i} = (0, \ldots, 0, 1, 0, \ldots, 0)$ be the vector with ith symbol 1 and all other symbols 0. Then $\underline{u} \cdot \underline{\epsilon_i} = u_i$. So if $\underline{u} \cdot \mathbb{F}_q^n = \{0\}$, then in particular $\underline{u} \cdot \underline{\epsilon_i} = 0$ hence $u_i = 0$, for all i, meaning that $\underline{u}$ is the zero vector. And if $\underline{u} = \underline{0}$, then $\underline{u} \cdot \underline{c} = 0$ for all $\underline{c} \in \mathbb{F}_q^n$.

The dual code

Definition: dual code

Given a code $C \subseteq \mathbb{F}_q^n$, we define the **dual code** $C^\perp$ as

$$C^\perp = \{\underline{v} \in \mathbb{F}_q^n \mid \underline{v} \cdot C = \{0\}\}.$$

We can say that $C^\perp$ consists of all vectors **orthogonal** to the code C (where $\underline{v}$ orthogonal to C means $\underline{v} \cdot C = \{0\}$).

Exercise. Using bilinearity of the inner product, show that $C^\perp$ is a *linear* code.

Recall that $Rep(n, \mathbb{F}_2) = \{00\ldots0, 11\ldots1\} \subseteq \mathbb{F}_2^n$ is the binary repetition code of length n. We now work out the code $Rep(n, \mathbb{F}_2)^\perp$ using the definition.

By definition, $Rep(n, \mathbb{F}_2)^\perp = \{\underline{v} \in \mathbb{F}_2^n \mid \underline{v} \cdot 00\ldots0 = 0,\ \underline{v} \cdot 11\ldots1 = 0\}$. The first condition, $\underline{v} \cdot \underline{0} = 0$ is vacuous (holds for all vectors $\underline{v} \in \mathbb{F}_2^n$). The second condition, $\underline{v} \cdot 11\ldots1$, means $v_1 + v_2 + \ldots + v_n = 0$ in $\mathbb{F}_2$, i.e., $\underline{v} \in E_n$, the binary even weight code of length n. Thus:

Example: the dual code of the binary repetition code

$Rep(n, \mathbb{F}_2)^\perp = E_n$.

Check matrices

Definition: check matrix

A **check matrix** for a linear code C means a generator matrix for $C^\perp$.

One sometimes says *parity check matrix* (the term arose from applications of binary codes).

Theorem 5.1: properties of the dual code and a check matrix

If $C \subseteq \mathbb{F}_q^n$ is a linear code of dimension k, then:

i. $\dim C^\perp = n - k$;

ii. $C = \{\underline{v} \in \mathbb{F}_q^n : \underline{v}H^T = \underline{0}\}$ for any check matrix H of C.

Proof. We recall the *Rank-Nullity Theorem* from Linear Algebra: if M is a matrix with n columns, then

$$\mathrm{rank}(M) + \dim \mathrm{Nullspace}(M) = n,$$

where $\mathrm{rank}(M)$ is the dimension of the span of the rows of M, and $\mathrm{Nullspace}(M)$ can be written as $\{\underline{v} \in \mathbb{F}_q^n : M\underline{v}^T = \overline{0}\}$.

i. Consider the matrix $\left[C\right]$ made up of *all* codevectors of C used as rows. The $\mathrm{Nullspace}(\left[C\right])$ is the set $\{\underline{v} : \left[C\right]\underline{v}^T = \overline{0}\}$. Note that the column vector $\left[C\right]\underline{v}^T$ is $\begin{bmatrix} \underline{c}_1\underline{v}^T \\ \underline{c}_2\underline{v}^T \\ \vdots \end{bmatrix} = \begin{bmatrix} \underline{c}_1 \cdot \underline{v} \\ \underline{c}_2 \cdot \underline{v} \\ \vdots \end{bmatrix}$, which is zero if and only if the inner product $\underline{c} \cdot \underline{v}$ is 0 for all rows $\underline{c}$ of $\left[C\right]$, i.e., for all codevectors $\underline{c}$ of C. By definition of the dual code, this happens exactly when $\underline{v} \in C^\perp$, so $\mathrm{Nullspace}(\left[C\right]) = C^\perp$. By rank-nullity, $\dim C^\perp = n - \mathrm{rank}(\left[C\right])$. Since the rows of $\left[C\right]$ span C, one has $\mathrm{rank}(\left[C\right]) = \dim C = k$ and so $\dim C^\perp = n - k$.

ii. By definition H generates the code $C^\perp$; so by i., H has $n-k$ rows, $H = \begin{bmatrix} \underline{r}_1 \\ \vdots \\ \underline{r}_{n-k} \end{bmatrix}$. Thus, $\mathrm{rank}(H) = \dim C^\perp = n - k$, and so by rank-nullity, $\dim \mathrm{Nullspace}(H) = n - (n-k) = k$. Note that $C \subseteq \mathrm{Nullspace}(H)$: indeed, if $\underline{c} \in C$, then $\underline{r}_i\underline{c}^T = \underline{r}_i \cdot \underline{c} = 0$ for all i because $\underline{r}_i \in C^\perp$, which means that $H\underline{c}^T = \overline{0}$. Since $\dim C = \dim \mathrm{Nullspace}(H)$, it follows that $C = \mathrm{Nullspace}(H)$, which is $\{\underline{v} : H\underline{v}^T = \overline{0}\}$.

The law $(AB)^T = B^T A^T$ for the product of matrices implies that $(\underline{v}H^T)^T = H\underline{v}^T$, and so $H\underline{v}^T$ is zero iff $\underline{v}H^T$ is. Thus, $C = \{\underline{v} \in \mathbb{F}_q^n : \underline{v}H^T = \underline{0}\}$ as claimed. □

The syndrome of a vector

Definition: syndrome

Let H be a check matrix for a linear code $C \subseteq \mathbb{F}_q^n$. Let $\underline{y} \in \mathbb{F}_q^n$. The vector

$$S(\underline{y}) = \underline{y}H^T$$

is called the **syndrome** of $\underline{y}$. The linear map $S\colon \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ is the **syndrome map.**

Proposition 5.2: syndromes of vectors in the same coset

Let S be a syndrome map for a linear code $C \subseteq \mathbb{F}_q^n$. If $\underline{v}, \underline{y} \in \mathbb{F}_q^n$,

- $S(\underline{v}) = S(\underline{y}) \iff \underline{v}, \underline{y}$ are in the same coset of C;
- $S(\underline{v}) = \underline{0} \iff \underline{v} \in C$.

Proof. $\underline{y}H^T = \underline{v}H^T \iff (\underline{y} - \underline{v})H^T = \underline{0} \iff \underline{y} - \underline{v} \in C$. By definition of cosets, this means that $\underline{v}$ is in the coset of $\underline{y}$. In particular, $S(\underline{v}) = \underline{0}$ means $\underline{v} \in \underline{0} + C = C$. □

The use of syndromes in error detection and correction

If $S(\underline{y}) \neq 0$, $\underline{y}$ is not a codevector, so the syndrome map *detects* errors in a received vector.

To *correct* errors, we need to construct a decoder for the linear code C. If we know a check matrix H for C, we can improve the standard array decoder for C. We will write the same decoder differently; it will require much less memory but more calculations.

Algorithm 5.3: the syndrome decoder

Preparation. Construct a *table of syndromes*, with q^{n-k} rows, of the form

Coset leader $\underline{a}_i$	$S(\underline{a}_i)$

Start with the top row: the codeword $\underline{0}$ and its syndrome $S(\underline{0}) = \underline{0}$.
At each step, choose a vector $\underline{a}_i \in \mathbb{F}_q^n$ of smallest weight such that $S(\underline{a}_i)$ does not appear in the table; then $\underline{a}_i$ is a coset leader of a new coset.
Decoding.

- Receive a vector $\underline{y} \in \mathbb{F}_q^n$.
- Calculate $S(\underline{y}) = \underline{y}H^T$.

- In the table, find $\underline{a}_i$ with $S(\underline{a}_i) = S(\underline{y})$. Then $\underline{a}_i$ is the coset leader of $\underline{y} + C$.
- Return $\texttt{DECODE}(\underline{y}) = \underline{y} - \underline{a}_i$.

Remark. The syndrome decoder is based on a choice of one coset leader in every coset. This is the same as for the standard array decoder.

In fact, if the same coset leaders are chosen in both decoders, both decoders with yield *the same* function $\texttt{DECODE}\colon \mathbb{F}_q^n \to C$. They differ only in the way this function is computed.

The number of arithmetic operations required to calculate the syndrome $S(\underline{y}) = \underline{y}H^T$ can be of order n^2, whereas the standard array decoder requires $\sim n$ operations to look up a vector. On the other hand, the amount of memory required by the syndrome decoder is proportional to q^{n-k} which is better than q^n for the standard array. The advantage is especially significant for codes with high code rate $\dfrac{k}{n}$.

Nevertheless, for codes which have more algebraic structure (than just linear codes), decoding algorithms exist which require even less storage, but the computation complexity is higher compared to syndrome decoding. Some examples will appear from the next chapter onwards.

Example: example of syndrome decoding

Let C be the binary linear code with check matrix $H = \left[\begin{array}{cc|cccc} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$.

(a) Construct the table of syndromes for C using the matrix H.

(b) Using the table of syndromes, decode the received vector $\underline{y} = 111111$.

Solution.

(a) When calculating syndromes, it is useful to observe that the syndrome of a vector $0 \ldots 010 \ldots 0$ (with 1 in position i and 0s elsewhere) is equal to the ith column of H, transposed.

The syndrome map is linear, so the syndrome of a sum of two vectors is the sum of their syndromes, etc.

For example, $S(011000) = 0011 + 1000 = 1011$ (the sum of the second and the third columns of H, transposed).

vector	syndrome	leader?
000000	0000	yes
000001	0001	yes
000010	0010	yes
000100	0100	yes
001000	1000	yes
010000	0011	yes
100000	0110	yes

All vectors of weight 1 have different syndromes, so they all are coset leaders. We need more coset leaders, hence we start looking at vectors of weight 2, then weight 3:

000011	0011	no, syndrome already in the table
000101	0101	yes
001001	1001	yes
001010	1010	yes
001100	1100	yes
010100	0111	yes
011000	1011	yes
101000	1110	yes
001101	1101	yes
011100	1111	yes

When we try a vector, say of weight 2, and find that is syndrome is already in the table, we ignore that vector and try another one.

We found $16 = 2^{6-2}$ coset leaders so we stop.

(b) $S(111111) = 1010$ which is the syndrome of the coset leader 001010 in the table. Therefore, $\texttt{DECODE}(111111) = 111111 - 001010 = 110101$.