Systematic generator matrices

Definition: A *systematic generator matrix* is of the form

$$G = [\ P \mid I\ ] = \begin{bmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Advantages of systematic generator matrices:

- Message symbols appear unscrambled in each codeword, in the rightmost positions $n-k, \ldots, n-1$.
- Encoder complexity is reduced; only check symbols need be computed:

$$c_j = m_0 g_{0,j} + m_1 g_{1,j} + \cdots + m_{k-1} g_{k-1,j} \quad (j = 0, \ldots, n-k-1)$$

- Check symbol encoder equations easily yield parity-check equations:

$$c_j - c_{n-k} g_{0,j} - c_{n-k+1} g_{1,j} - \cdots - c_{n-1} g_{k-1,j} = 0 \quad (m_i = c_{n-k+i})$$

- Systematic parity-check matrix is easy to find: $H = [\ I \mid -P^T\ ]$.

Systematic parity-check matrix

Let G be a $k \times n$ systematic generator matrix:

$$G = [\ P \mid I_k\ ] = \begin{bmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

The corresponding $(n-k) \times n$ systematic parity-check matrix is

$$H = [\ I_{n-k} \mid -P^T\ ] = \begin{bmatrix} 1 & 0 & \cdots & 0 & -p_{0,0} & \cdots & -p_{k-1,0} \\ 0 & 1 & \cdots & 0 & -p_{0,1} & \cdots & -p_{k-1,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -p_{0,n-k} & \cdots & -p_{k-1,n-k} \end{bmatrix}$$

(The minus signs are not needed for fields of characteristic 2, i.e., $\mathrm{GF}(2^m)$.)

Each row of H is corresponds to an equation satisfied by all codewords. These equations tell how to compute the check symbols $c_0, \ldots, c_{n-k-1}$ in terms of the information symbols $c_{n-k}, \ldots, c_{n-1}$.

Minimum weight and columns of H

$\mathbf{c}H^T = 0$ for every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$. Any *nonzero* codeword determines a linear dependence among a subset of *rows* of H^T. Then

$$\mathbf{c}H^T = 0 \implies 0 = (\mathbf{c}H^T)^T = H\mathbf{c}^T = c_0 h^0 + c_1 h^1 + \cdots + c_{n-1} h^{n-1}$$

is a linear dependence among a subset of the *columns* of H.

Theorem: The minimum weight of a linear block code is the smallest number of linearly dependent columns of any parity-check matrix.

Proof: Each linearly dependent subset of w columns corresponds to a codeword of weight w.

Recall that a set of columns of H is linearly dependent if one column is a linear combination of the other columns.

- A LBC has $w^* \leq 2$ iff one column of H is a multiple of another column.
- For binary Hamming codes, $w^* = 3$ because no columns of H are equal.

The Big Question: how to find H such that no $2t + 1$ columns are LI?

Computing minimum weight

The *rank* of H is the maximum number of linearly independent columns.

The rank can be determined in time $O(n^3)$ using linear operations, e.g., using Gaussian elimination.

Minimum distance is the smallest number of linearly dependent columns.

Finding the minimum distance is difficult (NP-hard). We might have to look at large numbers of subsets of columns.

Solution: design codes whose minimum distance can be proven to have desired lower bounds.

The dimension of the column space of H is $n-k$. Thus *any* $n-k+1$ columns are linearly dependent. Therefore for any linear block code,

$$d^* = w^* \leq n-k+1$$

This is known as the *Singleton bound*.

Exercise: Show that the Singleton bound holds for all (n,k) block codes, not just linear codes.

Maximum distance separable codes

Codes that achieve Singleton bound are called *maximum-distance separable* (MDS) codes.

Every repetition code satisfies the Singleton bound with equality:

$$d^* = n = (n-1) + 1 = (n-k) + 1$$

Another class of MDS codes are the simple parity-check codes:

$$d^* = 2 = 1 + 1 = (n-k) + 1$$

The best known *nonbinary* MDS codes are the Reed-Solomon codes over $\mathrm{GF}(Q)$. The RS code parameters are

$$(n, k, d^*) = (Q-1,\, Q-d^*,\, d^*) \implies n - k = d^* - 1\,.$$

Exercise: Show that the repetition codes and the simple parity-check codes are the only nontrivial *binary* MDS codes.

Linear block codes: summary

- An (n, k) linear block code is a k-dimensional subspace of F^n. Sums, differences, and scalar multiples of codewords are also codewords.
- A group code over additive group G is closed under sum and difference.
- An (n, k) LBC over $F = \mathrm{GF}(q)$ has $M = q^k$ codewords and rate k/n .
- A linear block code $\mathcal{C}$ can be defined by two matrices.
  - Generator matrix G: rows of G are basis for $\mathcal{C}$, i.e., $\mathcal{C} = \{\mathbf{m}G : \mathbf{m} \in F^k\}$
  - Parity-check matrix H span $C^\perp$, hence $\mathcal{C} = \{\mathbf{c} \in F^n : \mathbf{c}H^T = 0\}$
- Hamming weight of an n-tuple is the number of nonzero components.
- Minimum weight w^* of a block code is the Hamming weight of the nonzero codeword of minimum weight.
- Minimum distance of every LBC equals minimum weight: $d^* = w^*$.
- Minimum weight of a linear block code is the smallest number of linearly dependent columns of any parity-check matrix.

Syndrome decoding

Linear block codes are much simpler than general block codes:

- Encoding is vector-matrix multiplication.

  (Cyclic codes are even simpler: polynomial multiplication/division.)

- Decoding is inherently nonlinear. Fact: linear decoders are very weak.

  However, several steps in the decoding process are linear:
  - syndrome computation
  - final correction after error pattern and location have been found
  - extracting estimated message from estimated codeword

Definition: The *error vector* or *error pattern* $\mathbf{e}$ is the difference between the received n-tuple $\mathbf{r}$ and the transmitted codeword $\mathbf{c}$:

$$\mathbf{e} \stackrel{\Delta}{=} \mathbf{r} - \mathbf{c} \implies \mathbf{r} = \mathbf{c} + \mathbf{e}$$

Note: The physical noise model may not be additive noise, and the probability distribution for the error $\mathbf{e}$ may depend on the data $\mathbf{c}$. We assume a channel error model determined by $\Pr(\mathbf{e})$.

Syndrome decoding (cont.)

Multiply both sides of the equation $\mathbf{r} = \mathbf{c} + \mathbf{e}$ by H:

$$\mathbf{s} \stackrel{\Delta}{=} \mathbf{r}H^T = (\mathbf{c}+\mathbf{e})H^T = \mathbf{c}H^T + \mathbf{e}H^T = \mathbf{0} + \mathbf{e}H^T = \mathbf{e}H^T .$$

The *syndrome* of the senseword $\mathbf{r}$ is defined to be $\mathbf{s} = \mathbf{r}H^T$.

The syndrome of $\mathbf{r}$ (known to receiver) equals the syndrome of the error pattern $\mathbf{e}$ (not known to receiver, must be estimated).

Decoding consists of finding the most plausible error pattern $\mathbf{e}$ such that

$$\mathbf{e}H^T = \mathbf{s} = \mathbf{r}H^T .$$

"Plausible" depends on the error characteristics:

- For binary symmetric channel, most plausible means smallest number of bit errors. Decoder estimates $\hat{\mathbf{e}}$ of smallest weight satisfying $\hat{\mathbf{e}}H^T = \mathbf{s}$.
- For bursty channels, error patterns are plausible if the symbol errors are close together.

Syndrome decoding (cont.)

Syndrome table decoding consists of these steps:

1. Calculate syndrome $\mathbf{s} = \mathbf{r}H^T$ of received n-tuple.
2. Find most plausible error pattern $\mathbf{e}$ with $\mathbf{e}H^T = \mathbf{s}$.
3. Estimate transmitted codeword: $\hat{\mathbf{c}} = \mathbf{r} - \mathbf{e}$.
4. Determine message $\hat{\mathbf{m}}$ from the encoding equation $\hat{\mathbf{c}} = \hat{\mathbf{m}}G$.

Step 4 is not needed for systematic encoders, since $\mathbf{m} = \hat{\mathbf{c}}[n-k : n-1]$.

Only step 2 requires nonlinear operations.

For small values of $n - k$, lookup tables can be used for step 2.

For BCH and Reed-Solomon codes, the error locations are the zeroes of certain polynomials over the channel alphabet.

These *error locator polynomials* are *linear* functions of the syndrome.

Challenge: find, then solve, the polynomials.

Syndrome decoding: example

An $(8,4)$ binary linear block code $\mathcal{C}$ is defined by systematic matrices:

$$H = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \Longrightarrow G = \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Consider two possible messages:

$$\mathbf{m}_1 = [0\,1\,1\,0] \qquad \mathbf{m}_2 = [1\,0\,1\,1]$$
$$\mathbf{c}_1 = [0\,1\,1\,0\,0\,1\,1\,0] \qquad \mathbf{c}_2 = [0\,1\,0\,0\,1\,0\,1\,1]$$

Suppose error pattern $\mathbf{e} = [0\,0\,0\,0\,0\,1\,0\,0]$ is added to both codewords.

$$\mathbf{r}_1 = [0\,1\,1\,0\,0\,0\,1\,0] \qquad \mathbf{r}_2 = [0\,1\,0\,0\,1\,1\,1\,1]$$
$$\mathbf{s}_1 = [1\,0\,1\,1] \qquad \mathbf{s}_2 = [1\,0\,1\,1]$$

Both syndromes equal column 6 of H, so decoder corrects bit 6.

$\mathcal{C}$ is an expanded Hamming code with weight enumerator $A(x) = 1 + 14x^4 + x^8$.

Standard array

Syndrome table decoding can also be described using the *standard array*.

The *standard array* of a group code $\mathcal{C}$ is the coset decomposition of F^n with respect to the subgroup $\mathcal{C}$.

0	c_2	c_3	$\cdots$	c_M
e_2	$c_2 + e_2$	$c_3 + e_2$	$\cdots$	$c_M + e_2$
e_3	$c_2 + e_3$	$c_3 + e_3$	$\cdots$	$c_M + e_3$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
e_N	$c_2 + e_N$	$c_3 + e_N$	$\cdots$	$c_M + e_N$

- The first row is the code $\mathcal{C}$, with the zero vector in the first column.
- Every other row is a coset.
- The n-tuple in the first column of a row is called the *coset leader*.

  We usually choose the coset leader to be the most plausible error pattern, e.g., the error pattern of smallest weight.

Standard array: decoding

An (n, k) LBC over $\mathrm{GF}(Q)$ has $M = Q^k$ codewords.

Every n-tuple appears exactly once in the standard array. Therefore the number of rows N satisfies

$$MN = Q^n \implies N = Q^{n-k}.$$

All vectors in a row of the standard array have the same syndrome.

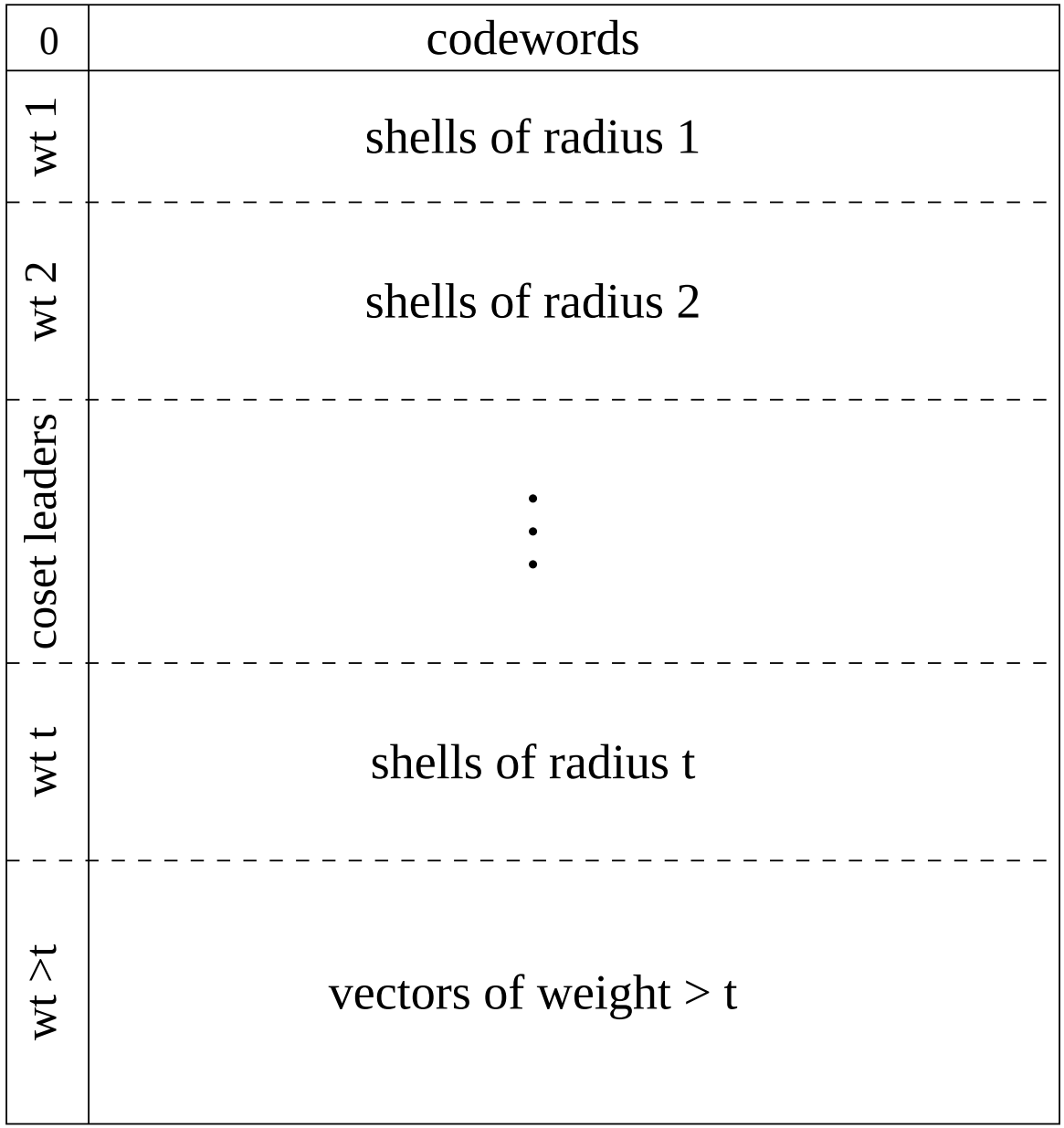
Thus there is a one-to-one correspondence between the rows of the standard array and the Q^{n-k} syndrome values.

Decoding using the standard array is simple: decode senseword $\mathbf{r}$ to the codeword at the top of the column that contains $\mathbf{r}$.

The decoder subtracts the coset leader from the received vector to obtain the estimated codeword.

The *decoding region* for a codeword is the column headed by that codeword.

Standard array and decoding regions



Standard array: example

The systematic generator and parity-check matrices for a $(6, 3)$ LBC are

$$G = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \implies H = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

The standard array has 6 coset leaders of weight 1 and one of weight 2.

000000	001110	010101	011011	100011	101101	110110	111000
000001	001111	010100	011010	100010	101100	110111	111001
000010	001100	010111	011001	100001	101111	110100	111010
000100	001010	010001	011111	100111	101001	110010	111100
001000	000110	011101	010011	101011	100101	111110	110000
010000	011110	000101	001011	110011	111101	100110	101000
100000	101110	110101	111011	000011	001101	010110	011000
001001	000111	011100	010010	101010	100100	111111	110001

See http://www.stanford.edu/class/ee387/src/stdarray.pl for the short Perl script that generates the above standard array. This code is a *shortened* Hamming code.

Standard array: summary

The standard array is a conceptional arrangement of all n-tuples.

0	c_2	c_3	$\cdots$	c_M
e_2	$c_2 + e_2$	$c_3 + e_2$	$\cdots$	$c_M + e_2$
e_3	$c_2 + e_3$	$c_3 + e_3$	$\cdots$	$c_M + e_3$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
e_N	$c_2 + e_N$	$c_3 + e_N$	$\cdots$	$c_M + e_N$

- The first row is the code $\mathcal{C}$, with the zero vector in the first column.
- Every other row is a coset.
- The n-tuple in the first column of a row is called the *coset leader*.
- Senseword $\mathbf{r}$ is decoded to codeword at top of column that contains $\mathbf{r}$.
- The *decoding region* for codeword is column headed by that codeword.
- Decoder subtracts coset leader from $\mathbf{r}$ to obtain estimated codeword.

Syndrome decoding: summary

Syndrome decoding is closely connected to standard array decoding.

1. Calculate syndrome $\mathbf{s} = \mathbf{r}H^T$ of received n-tuple.
2. Find most plausible error pattern $\mathbf{e}$ with $\mathbf{e}H^T = \mathbf{s}$.

   This error pattern is the coset leader of the coset containing $\mathbf{r}$.
3. Estimate transmitted codeword: $\hat{\mathbf{c}} = \mathbf{r} - \mathbf{e}$.

   The estimated codeword $\hat{\mathbf{c}}$ is the entry at the top of the column containing $\mathbf{r}$ in the standard array.
4. Determine message $\mathbf{m}$ from the encoding equation $\mathbf{c} = \mathbf{m}G$.

   In general, $\mathbf{m} = \mathbf{c}R$, where R is an $n \times k$ pseudoinverse of G.
   If the code is systematic, then $R = [\, 0_{(n-k)\times k} \mid I_{k\times k} \,]^T$.

Only step 2 requires nonlinear operations. Step 2 is conceptually the most difficult.

Surprisingly, most computational effort is spent on syndrome computation.