Error-correcting codes

Uri Shaham

1 Error-Correcting Codes

1.1 Motivation

The channel coding theorem says that reliable communication is possible below capacity. Error-correcting codes are explicit ways to add redundancy so that the receiver can detect and correct corrupted symbols.

This lecture focuses on binary block codes and the geometry of Hamming space.

1.2 Block codes and rate

Definition 1.1 (Binary block code)**.** A binary block code of length n is a subset

$$\mathcal{C} \subseteq \{0,1\}^n.$$

Elements of $\mathcal{C}$ are codewords. If $|\mathcal{C}| = M$, the rate is

$$R = \frac{1}{n} \log M.$$

If $M = 2^k$, then $R = k/n$ and the code encodes k message bits into n transmitted bits.

The redundancy is $n - k$. Redundancy is not merely repetition; it is structured extra information that helps the receiver identify what went wrong.

1.3 Hamming distance and minimum distance

Definition 1.2 (Hamming distance)**.** For $x, y \in \{0,1\}^n$, the Hamming distance is

$$d_H(x,y) = |\{i : x_i \neq y_i\}|.$$

Definition 1.3 (Minimum distance)**.** The minimum distance of a code $\mathcal{C}$ is

$$d_{\min} = \min_{c,c' \in \mathcal{C},\ c \neq c'} d_H(c,c').$$

Minimum distance measures how far apart codewords are in Hamming space. Large distance gives room to absorb errors.

Theorem 1.4 (Detection and correction)**.** *A code with minimum distance $d_{\min}$ can detect up to $d_{\min} - 1$ errors. It can correct up to*

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

errors by nearest-neighbor decoding.

Proof sketch. If fewer than $d_{\min}$ errors occur, a transmitted codeword cannot be changed into another codeword, so the receiver can detect that something is wrong. For correction, Hamming balls of radius t around distinct codewords are disjoint when $2t < d_{\min}$. Thus a received word within distance t of a codeword has a unique nearest codeword. □

Example 1.5 (Repetition code)**.** The length-3 repetition code is

$$\mathcal{C} = \{000, 111\}.$$

Its minimum distance is 3. It can detect up to 2 errors and correct up to 1 error.

1.4 Linear codes

Definition 1.6 (Linear code)**.** A binary linear code is a subspace $\mathcal{C} \subseteq \mathbb{F}_2^n$, where $\mathbb{F}_2^n = \{0,1\}^n$. That means that the codewords are length n binary strings, and the XOR of two codewords is also a codeword. If $\dim(\mathcal{C}) = k$, then $|\mathcal{C}| = 2^k$ and the rate is k/n.

A linear code can be represented by a generator matrix.

Definition 1.7 (Generator matrix)**.** A $k \times n$ matrix G over $\mathbb{F}_2$ generates a linear code

$$\mathcal{C} = \{mG : m \in \mathbb{F}_2^k\}.$$

The message m is encoded as $c = mG$.

Linear codes can also be represented by parity checks.

Definition 1.8 (Parity-check matrix)**.** An $(n-k) \times n$ matrix H is a parity-check matrix for $\mathcal{C}$ if

$$\mathcal{C} = \{c \in \mathbb{F}_2^n : Hc^T = 0\}.$$

Definition 1.9 (Syndrome)**.** For a received word $y \in \mathbb{F}_2^n$, the syndrome is

$$s = Hy^T.$$

If $y = c + e$, where c is a codeword and e is an error vector, then

$$s = H(c+e)^T = Hc^T + He^T = He^T.$$

Thus the syndrome depends only on the error pattern, not on the transmitted codeword.

1.5 The Hamming $(7, 4)$ code

The Hamming $(7, 4)$ code is the canonical small example of a single-error-correcting code. It encodes $k = 4$ message bits into $n = 7$ transmitted bits, so its rate is

$$R = \frac{4}{7}.$$

It has minimum distance 3, so it corrects one error.

One systematic parity-check matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The columns of H are all distinct nonzero vectors in $\mathbb{F}_2^3$. This is what makes single-error correction possible: if one bit flips in position j, the syndrome equals column j of H.

A corresponding systematic generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

One checks that

$$HG^T = 0$$

over $\mathbb{F}_2$.

1.6 Worked decoding example

Let the message be

$$m = (1, 0, 1, 1).$$

Encoding gives

$$c = mG = (1, 0, 1, 1, 0, 1, 0).$$

Suppose bit 6 flips during transmission. The receiver obtains

$$y = (1, 0, 1, 1, 0, 0, 0).$$

Compute the syndrome:

$$s = Hy^T = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

This syndrome equals the sixth column of H, so the decoder concludes that bit 6 flipped. Flipping bit 6 back gives

$$\hat{c} = (1, 0, 1, 1, 0, 1, 0),$$

and the first four bits recover the message

$$\hat{m} = (1, 0, 1, 1).$$

1.7 Sphere packing and the Hamming bound

The Hamming ball of radius t around a codeword in $\{0,1\}^n$ has size

$$V(n,t) = \sum_{i=0}^{t} \binom{n}{i}.$$

If a code corrects t worst-case errors, these balls must be disjoint. Therefore:

Theorem 1.10 (Hamming bound)**.** *If a binary code of length n has M codewords and corrects t errors, then*

$$M \sum_{i=0}^{t} \binom{n}{i} \leq 2^n.$$

For a linear $[n,k,d]$ code with $t = \lfloor (d-1)/2 \rfloor$, this becomes

$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n.$$

For the Hamming $(7,4)$ code, $M = 16$ and $t = 1$, so

$$16\left(\binom{7}{0} + \binom{7}{1}\right) = 16(1+7) = 128 = 2^7.$$

The bound is met with equality. The Hamming $(7,4)$ code is therefore a perfect single-error-correcting code.

1.8 Worst-case errors versus random errors

Minimum distance is a worst-case guarantee: if at most t positions are corrupted, decoding succeeds regardless of which positions they are.

Shannon capacity is a random-noise guarantee: for a channel such as BSC(p), errors may exceed t occasionally, but good long codes can still achieve arbitrarily small probability of decoding error whenever

$$R < 1 - H_2(p).$$

These are complementary viewpoints:

coding theory studies explicit code geometry,

information theory studies fundamental limits.

1.9 Modern coding families, briefly

- **Reed-Solomon codes**: nonbinary algebraic codes used in storage, QR codes, and erasure correction.
- **LDPC codes**: sparse parity-check codes with efficient iterative decoding; important in modern communication systems.

- **Turbo codes**: concatenated codes with iterative decoding; historically important near-capacity codes.
- **Polar codes**: explicit capacity-achieving codes for symmetric binary-input memoryless channels.

The details differ, but the same themes persist: rate, redundancy, distance, noise model, and decoding complexity.