To send a message of 0’s and 1’s from my computer on Earth to Mr. Spock’s computer on the planet Vulcan we use codes which include redundancy to correct errors.
Definition. A linear code $C$ is a vector subspace $C$ of $\mathbb{F}_q^n$.

Here $\mathbb{F}_q$ denotes the field with $q$ elements. If the dimension of $C$ as a vector space over $\mathbb{F}_q$ is $k$, we call $C$ an $[n,k]$-code.

Since all codes we consider are linear, we will drop the word "linear" and just call them "codes".

Here $q$ will be 2 mostly. Such codes are called "binary." If $q=3$, the code is "ternary."

Definition. The Hamming weight of a codeword $x$ is $|x| = \text{the number of components of } x \text{ which are non-zero}$. The distance between is defined to be $|x-y|$.
Definition. If $C$ is an $[n,k]$ code such that the minimum distance of a non-zero code word from 0 is $d$, we say that $C$ is an $[n,k,d]$-code.

The following is part of Theorem 31.2, Gallian, p. 525. It assumes you decode a received vector as the nearest codeword using the Hamming distance.

Theorem. If $d = 2e+1$, an $[n,k,d]$-code $C$ corrects $e$ or fewer errors.

Proof. If $x \in C$ is sent and $u$ received, with at most $e$ errors made, then $u$ is closer to $x$ than any other codeword $y \in C$. Here $u$ is in the big vector space, not necessarily in the code $C$. It has errors. To prove $u$ closer to $x$ than $y$:

$$e + d(u,y) \geq d(u,x) + d(u,y) \geq d(x,y) \geq 2e+1,$$

which implies $d(u,y) \geq e+1$.

1st $\geq$ true since: $u$ has distance at most $e$ from $x$.

2nd $\geq$ is triangle inequality for Hamming distance (Gallian, p.524)

Last $\geq$ true since $2e+1 = $ minimum distance between any 2 codeword in $C$.

As $d(u,x) \leq e$, we see $x$ is closer to $u$ than any other codeword $y$ with $y \neq x$, as we just showed that $d(u,y) \geq e+1$. So we decode $u$ as $x$, the correct answer.
More Definitions.

Since an \([n,k]\) binary code \(C\) is a \(k\)-dimensional vector space over \(\mathbb{F}_2\), \(C\) has a \(k\)-element basis, we can form a matrix whose rows are the basis vectors. This is called a **generator matrix** \(G\) of the code \(C\). A generator matrix of an \([n,k]\) code is a \(k \times n\) matrix with elements in \(\mathbb{F}_2\).

Codewords in \(C\) have the form \(vG\), where \(v\) is a row vector with its \(k\) entries from \(\mathbb{F}_2\).

Since \(C\) has more than one basis, it also has many generator matrices.

The **standard generator matrix** has the form \(G = (I_k \ A)\), where the first \(k\) columns are the \(k \times k\) identity matrix \(I_k\).

With the generating matrix in standard form, with no errors, decoding is easy, just take the first \(k\) entries of the code word.
A parity check matrix \( H \) of a \([n,k]\) code \( C \) is a matrix with \( n \) columns and rank \( n-k \) such that \( x \in C \) if and only if \( x \, H = 0 \).

(Most texts take transpose \( H \) instead.)

If \( G = (I_k \, A) \), then

\[
H = \begin{pmatrix}
-A \\
I_{n-k}
\end{pmatrix}.
\]

Parity check decoding is described in our text, pages 528-553.

Next: Where does all our theory of finite fields come in?
Defn. A linear cyclic code is a linear code \( C \) with the property that if \( c = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \) is a code word then so is \( (c_{n-1}, c_0, \ldots, c_{n-3}, c_{n-2}) \).

Let \( R \) denote the factor ring
\[
R = \mathbb{F}_q \langle x \rangle / \langle x^n - 1 \rangle.
\]
Represent elements of \( R \) by polynomials with coefficients in \( \mathbb{F}_q \) of degree < \( n \).
Identify codeword \( c = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \) with \( c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \).

Theorem. A linear code \( C \) in \( R \) is cyclic if and only if it is an ideal in the ring \( R = \mathbb{F}_q \langle x \rangle / \langle x^n - 1 \rangle \).

Proof.
First note that a subspace \( W \) of \( R \) is an ideal if \( xW \subseteq W \), because this \( \implies \)
\[
x^j W \subseteq W, \text{ for all } j=2,3,\ldots.
\]
Thus \( RW \subseteq W \).

Now suppose that \( C \) is an ideal and \( c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C \). Then \( C \) contains
\[
x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n
\]
\[
= c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} \pmod{\langle x^n - 1 \rangle}.
\]
The last happens because \( x^n \) is congruent to 1 modulo \( \langle x^n - 1 \rangle \).
So \( C \) is cyclic.

Problem A. Suppose that \( C \) is cyclic, and show that \( C \) is an ideal.
Question. What are the ideals \( A \) in the ring \( R = \mathbb{F}_q[x]/<x^n - 1> \)?

Answer. They are principal ideals \(<g(x)>\), where \( g(x) \) divides \( x^n - 1 \). We call \( g(x) \) the generator of \( A \).

If
\[
g(x) = c_0 + c_1x + \cdots + c_rx^r
\]
has degree \( r \), then the corresponding code is an \([n,n-r]\)-code and a generator matrix for the code (as defined above) is the \((n-r)\times n\) matrix:
\[
\begin{pmatrix}
  c_0 & c_1 & c_2 & \cdots & c_r & 0 & 0 & \cdots & 0 \\
  0 & c_0 & c_1 & \cdots & c_{r-1} & c_r & 0 & \cdots & 0 \\
  0 & 0 & c_0 & \cdots & c_{r-2} & c_{r-1} & c_r & \cdots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & 0 & \cdots & c_0 & c_1 & c_2 & \cdots & c_r
\end{pmatrix}
\]

Problem B. Show that the code above has dimension \( n-r \).

Hint. The cosets of the vectors \( g(x)x^j, j=0,\ldots,n-r-1, \) are linearly independent in the ring \( R \). These vectors span the ideal \( A = <g(x)> \) since elements of \( A \) have the form \( f(x)g(x) \), for some polynomial \( f(x) \) of degree less than or equal to \( n-r-1 \).
Example 1. The Hamming [7, 4, 3]-code.

\[ x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } \mathbb{F}_2[x]. \]

Take \( g(x) = x^3 + x + 1 \) to generate our ideal I in R corresponding to the code.

The codewords in C in \( \mathbb{F}_2^7 \) are listed below:

\[
\begin{array}{cccccccc}
0 0 0 0 0 0 0 & 1 1 1 1 1 1 1 \\
1 1 0 1 0 0 0 & 0 0 1 0 1 1 1 \\
0 1 1 0 1 0 0 & 1 0 0 1 0 1 1 \\
0 0 1 1 0 1 0 & 1 1 0 0 1 0 1 \\
0 0 0 1 1 0 1 & 1 1 1 0 0 1 0 \\
1 0 0 0 1 1 0 & 0 1 1 1 0 0 1 \\
0 1 0 0 0 1 1 & 1 0 1 1 1 0 0 \\
1 0 1 0 0 0 1 & 0 1 0 1 1 1 0 \\
\end{array}
\]

Problem C. Explain why the listed code words are correct.

A generator matrix of the preceding code is

\[
\begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
\end{pmatrix}.
\]

This is not the same as that used by Gallian, in Examples 1 and 9 pages 522 and 531.
Problem D. Explain why our Hamming [7,4,3] code is the same as that of Gallian, Examples 1 and 9, pages 522 and 531.

Suppose \( g(x)h(x) = x^{n-1} \), in \( \mathbb{F}_2[x] \), with \( g(x) \) of degree \( r \), the generator polynomial of a code \( C \) and \( h(x) \) of degree \( k=n-r \). Then we get a parity check matrix for the code from the matrix of the polynomial \( h(x) = h_0 + h_1x + \cdots + h_kx^k \) as follows

\[
\begin{pmatrix}
  h_k & 0 & \cdots & 0 \\
h_{k-1} & h_k & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots \\
h_0 & h_1 & \cdots & h_k \\
  0 & h_0 & \cdots & h_{k-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \cdots & h_0
\end{pmatrix}
\]

Problem E. i) Show that the preceding matrix is indeed a parity - check matrix for our code with generator polynomial \( g(x) \) as described above. ii) Find the parity check matrix for the Hamming [7,4,3] code above.
There is a method for constructing codes that correct lots of errors called BCH codes. See Dornhoff and Hohn, *Applied Modern Algebra*, page 442 for the mathematical details.

Gallian includes some history of the subject on pages 537 ff.

Another reference is Vera Pless, *Introduction to the Theory of Error-Correcting Codes*.

Recall that we obtained the Hamming $[7,4,3]$ code by looking at the generator polynomial $g(x) = x^3 + x + 1$. This is the minimal polynomial of an element $g$ of $\mathbb{F}_8$ whose other roots are $g^2$ and $g^4$. So we could say that any polynomial $f(x)$ is in our code $C$ iff $f(g^j) = 0$, $j = 1, 2, 4$. For any polynomial whose roots include the roots of $g(x)$ must be divisible by $g(x)$.

**Definition.** A primitive $n$th root of 1 in a field $K$ is a solution $g$ to $g^n = 1$ such that $g^m \neq 1$, for $1 \leq m < n$.

**Theorem.** (Bose-Chaudhuri and Hoquenghem - around 1960)
Suppose $g.c.d.(n,q)=1$. Let $g$ be a primitive $n$th root of 1 in $\mathbb{F}_{q^m}$. Suppose the generator polynomial $g(x)$ of a cyclic code of length $n$ over $\mathbb{F}_q$ has $g, g^2, ..., g^{d-1}$ among its roots.
Then the minimum distance of a code element from 0 is at least $d$.
For a proof see Dornhoff and Hohn, pages 442-3.
A Reed-Solomon code is a BCH code with \( n=q-1 \).

These codes are used by the makers of CD players, NASA, ....

These can be used to correct amazing numbers of errors. If you suppose \( q=2^8 \) so that \( n=255 \), a 5-error-correcting code has
\[
g(x) = (x-g)(x-g^2) \cdots (x-g^{10}) \text{ of degree 10.}
\]

Elements of \( \mathbb{F}_8 \) are 8-dimensional vectors over \( \mathbb{F}_2 \).
This code can be used as a code of length
\[
8*255=2040 \text{ over } \mathbb{F}_2,
\]
which can correct any 33 consecutive errors.

See Dornhoff and Hohn, p. 444.

Feedback shift registers are of use in encoding and decoding cyclic codes.