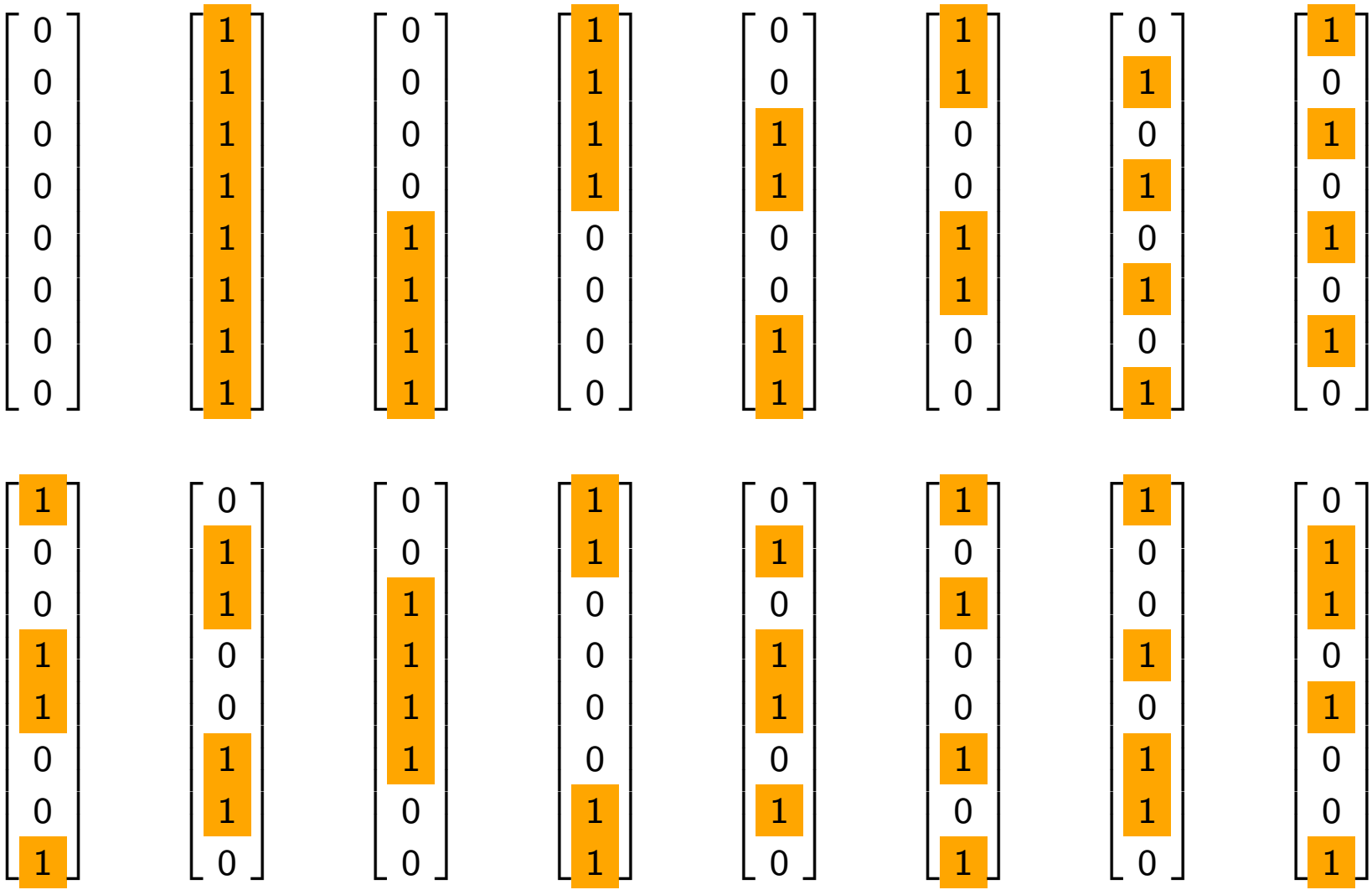
Error Correcting Codes according to Hamming

A contribution to Linear Algebra

by Nora Ganter, University of Melbourne

2020

Hamming's List of Words



Linear subspace property

Write $\mathcal{H} \subseteq \mathbb{F}_2^8$ for the set of vectors on the previous page.

The rules for scalars from $\mathbb{F}_2 = GF(2)$ are:

$0 + 0 = 0 = 1 + 1 \qquad 0 + 1 = 1 = 1 + 0 \qquad 0\,\vec{v} = \vec{0} \qquad 1\,\vec{v} = \vec{v}.$

If you add any two vectors, you obtain a new vector with 1's in exactly the entries where the two original vectors differ:

"Vector addition over $\mathbb{F}_2$ is symmetric difference".

The symmetric difference of two vectors in $\mathcal{H}$ is again in $\mathcal{H}$.

Any two distinct vectors in $\mathcal{H}$ differ in either four or eight places.

Error Detection Matrix

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Matrix multiplication by rows:

$$M\vec{v} = \begin{bmatrix} \overrightarrow{row_0} \cdot \vec{v} \\ \overrightarrow{row_1} \cdot \vec{v} \\ \overrightarrow{row_2} \cdot \vec{v} \\ \overrightarrow{row_3} \cdot \vec{v} \end{bmatrix}$$

Example:

If $\vec{h} \in \mathcal{H}$, then $M\vec{h} = \vec{0}$.

Where is the error?

Matrix multiplication by columns:

$$M\vec{v} = v_0 \begin{bmatrix}1\\0\\0\\0\end{bmatrix} + v_1 \begin{bmatrix}1\\0\\0\\1\end{bmatrix} + v_2 \begin{bmatrix}1\\0\\1\\0\end{bmatrix} + v_3 \begin{bmatrix}1\\0\\1\\1\end{bmatrix} + v_4 \begin{bmatrix}1\\1\\0\\0\end{bmatrix} + v_5 \begin{bmatrix}1\\1\\0\\1\end{bmatrix} + v_6 \begin{bmatrix}1\\1\\1\\0\end{bmatrix} + v_7 \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

Inserting an error:

$$\vec{h} \in \mathcal{H} \qquad M\vec{h} = 0 \qquad M(\vec{h} + \vec{e_i}) = M\vec{e_i},$$

where $\vec{e_i}$ is the error in position i (standard basis vector).

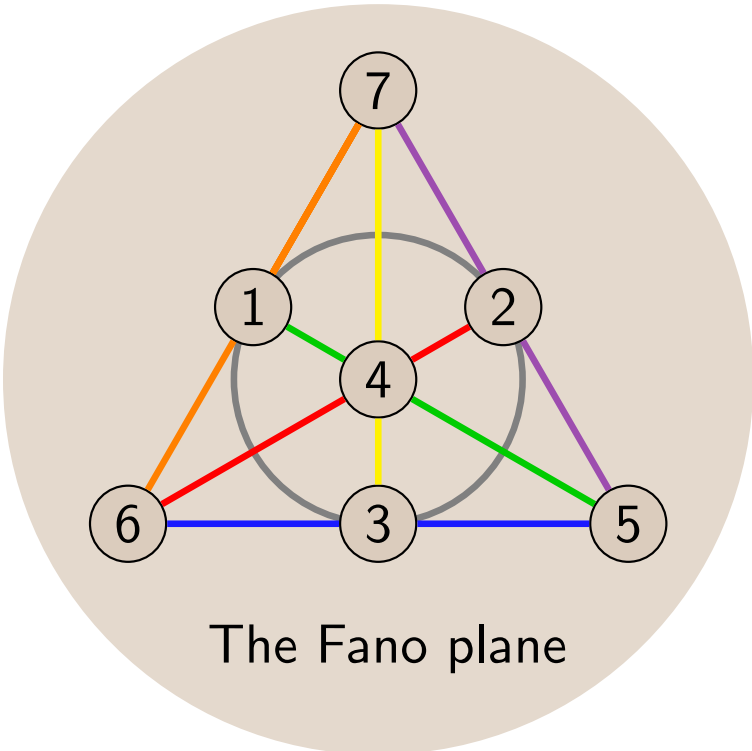
Here we used that matrix multiplication respects linear combinations.

Over $\mathbb{F}_2$ this means $M\vec{0} = \vec{0}$ and $M(\vec{v} + \vec{w}) = M\vec{v} + M\vec{w}$.

Example

The Fano Plane $\mathcal{F}$

The phenomenon at the heart of this construction is the smallest example of a projective geometry, known as the Fano Plane.



The Fano plane

	1	2	3	4	5	6	7
Line 1		■			■		■
Line 2			■	■			■
Line 3	■			■	■		
Line 4	■					■	■
Line 5		■		■		■	
Line 6	■	■	■				
Line 7			■		■	■	

$\mathcal{F}$ with a choice of numbering and resulting incidence table.
Different numbering would amount to a shuffles of the columns.

The (7,4) Hamming code

The (7,4)-Hamming code is a subspace of $\mathbb{F}_2^7$ consisting of the incidence vectors of:

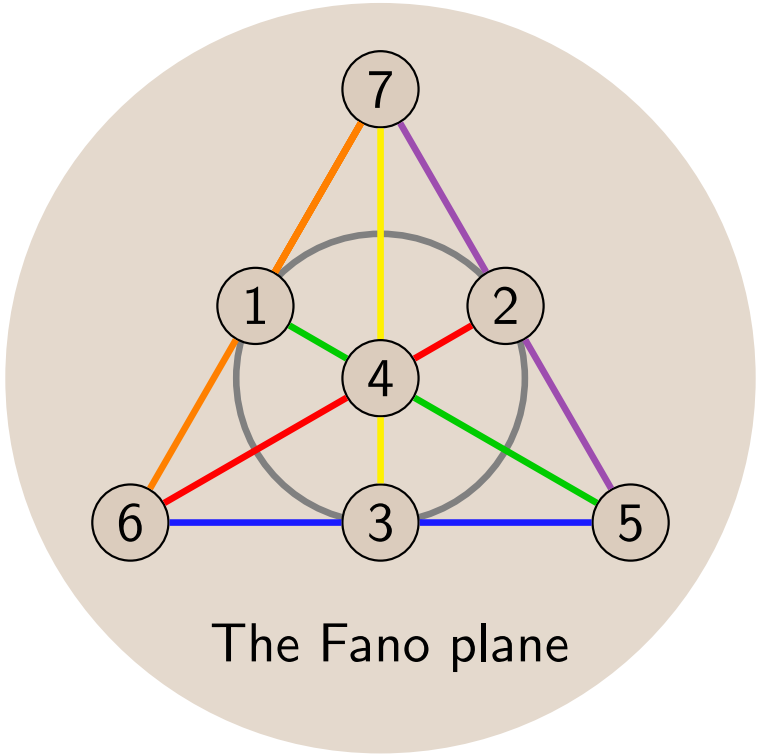
1. the lines in $\mathcal{F}$
2. the line complments in $\mathcal{F}$
3. the entire Fano plane $\mathcal{F}$
4. the empty set.

Example:

$$\begin{bmatrix}0\\1\\0\\1\\0\\1\\0\end{bmatrix} \quad \begin{bmatrix}1\\0\\1\\0\\1\\0\\1\end{bmatrix} \quad \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\end{bmatrix} \quad \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\end{bmatrix}$$

Line 5 | complement of line 5 | $\mathcal{F}$ | $\emptyset$

Features of the Fano Plane



The Fano plane

1. Each line has three points.
2. Each point has three lines.
3. Through any two distinct points goes exactly one line.
4. Any two distinct lines meet in exactly one point.
5. The symmetric difference of two lines is a line complement.
6. The symmetric difference of two line complements is a line complement.
7. The symmetric difference of a line and the complement of a different line is a line.

From seven to eight: adding a parity check digit

The (7,4) Hamming code forms a linear subspace of $\mathbb{F}_2^7$.

In particular, two distinct words in this code differ in at least three spots. Single bit errors are detected and corrected using the matrix

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

It can be upgraded to detect (but not correct) double bit errors by introducing a parity check digit in position zero.

Incidence vectors of lines and of $\mathcal{F}$ each acquire an entry 1 in position zero, line complements and $\vec{0}$ acquire a zero.

The resulting subspace is $\mathcal{H} \subseteq \mathbb{F}_2^8$. It is known as the (8,4) Hamming code.