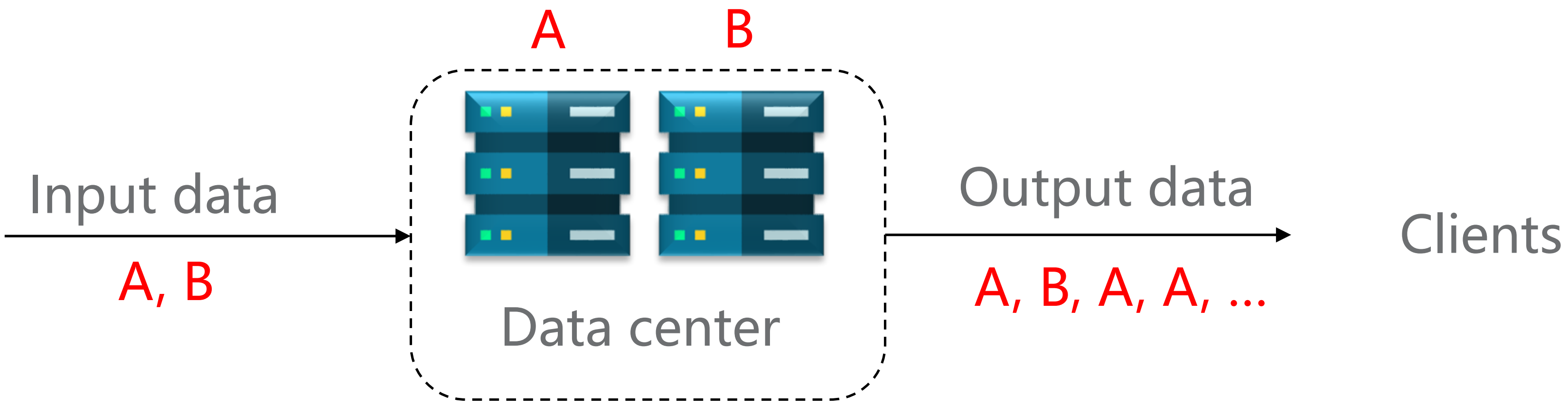
UNIVERSITY OF TARTU

# A code construction from finite projective planes

**Junming Ke**
*Institute of Mathematics and Statistics*

# Background



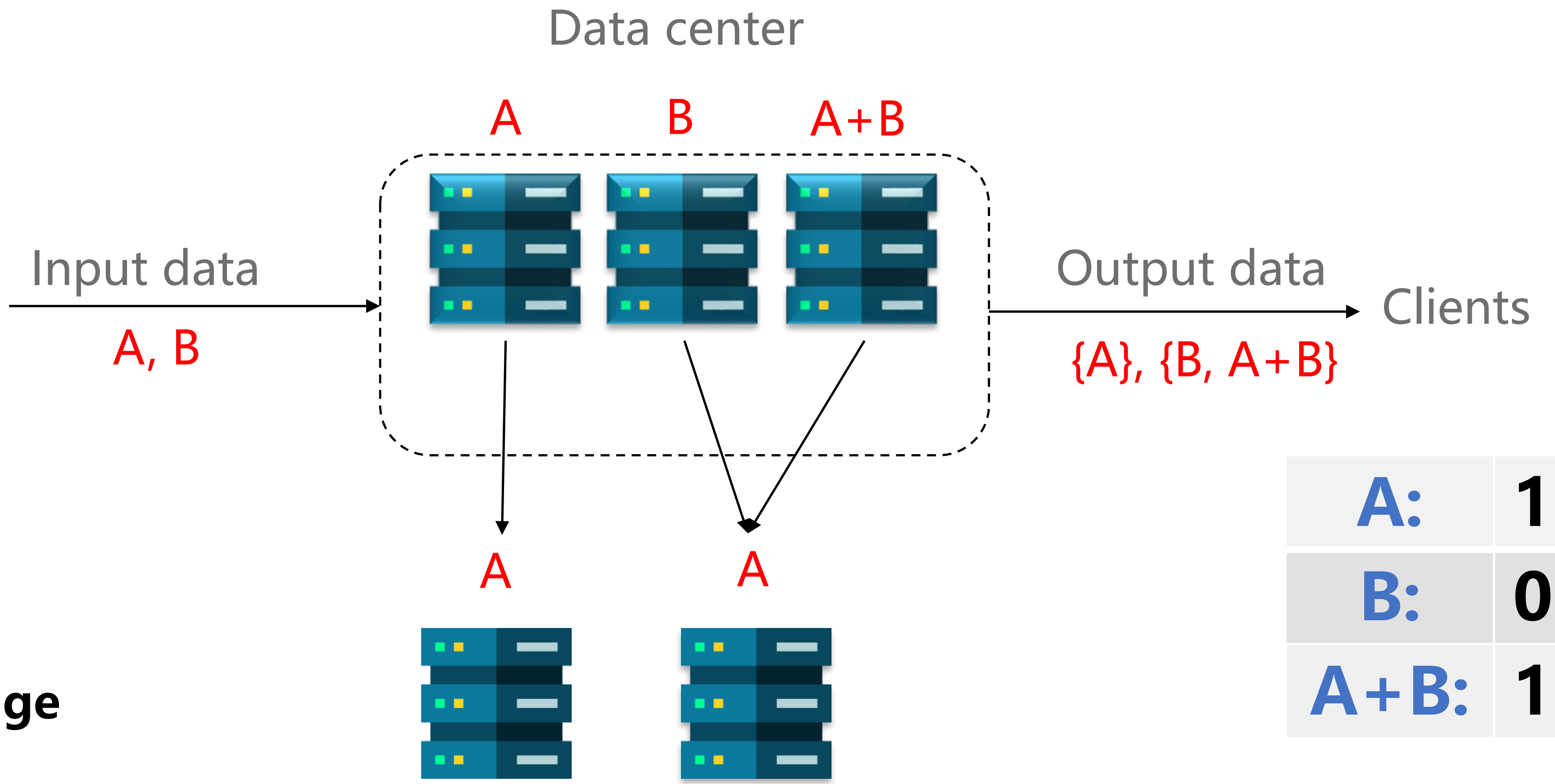

**Storage**

| | |
|---|---|
| A: | 10 |
| B: | 01 |

Two main drawbacks:

1. Nodes that store data A have a high load;
2. If A is broken, a data center cannot reconstruct A.

# Background

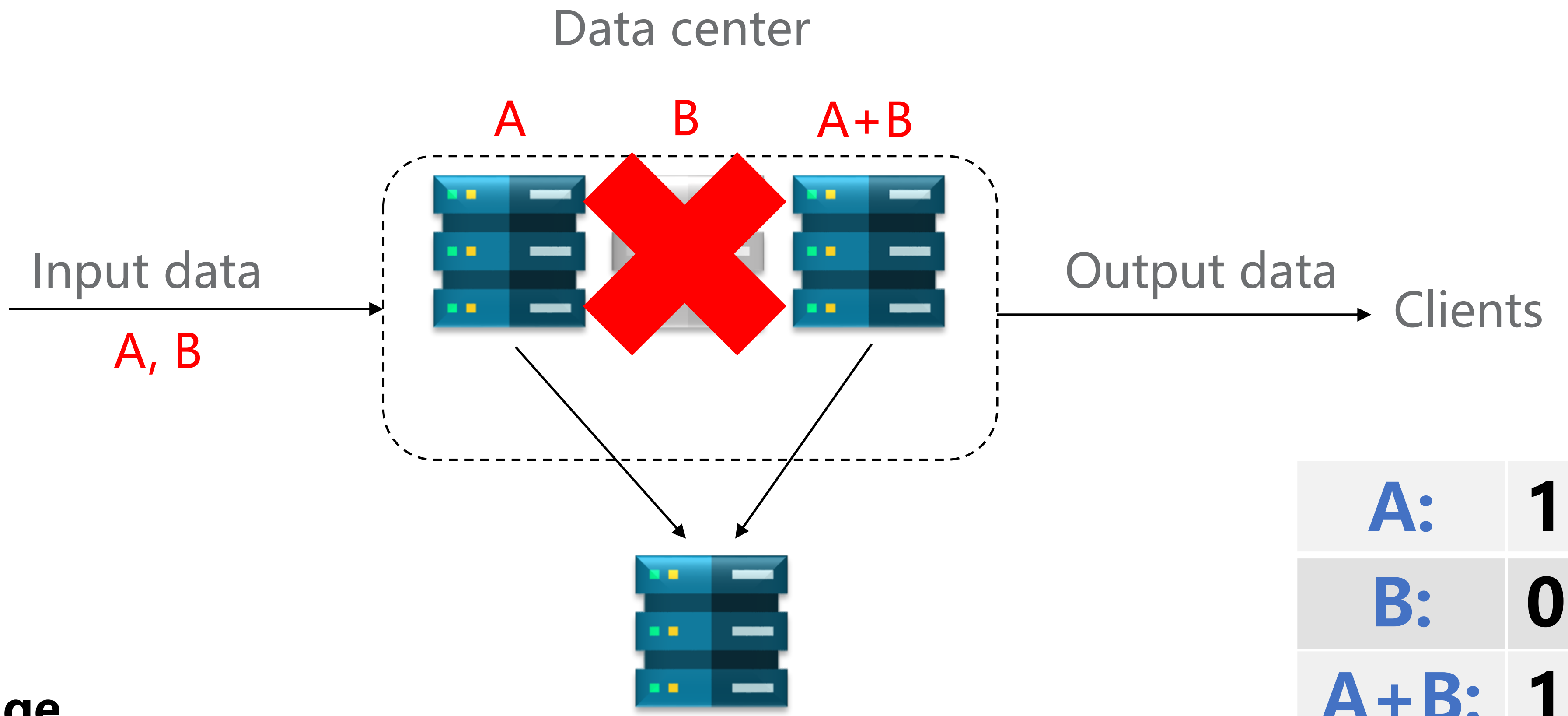



| | |
|---|---|
| A: | 10 |
| B: | 01 |
| A+B: | 11 |

**Coded Storage**

Nodes that store data A have a high load.

# Repair




| | |
|---|---|
| A: | 10 |
| B: | 01 |
| A+B: | 11 |

**Coded Storage**

A + A + B = B

If A is broken, a data center cannot reconstruct A. ✓

# Projective Planes

**Definition 1 (Finite projective plane [1])**:

Let $X$ be a finite set, and let $\mathcal{L}$ be a system of subsets of $X$. The pair $(X, \mathcal{L})$ is called a finite projective plane if it satisfies the following axioms.

**1.** There exists a 4-element set $F \subseteq X$ such that $|L \cap F| \leq 2$ holds for each set $L \in \mathcal{L}$.

**2.** Any two distinct sets $L_1, L_2 \in \mathcal{L}$ intersect in exactly one element, i.e. $|L_1 \cap L_2| = 1$.

**3.** For any two distinct elements $x_1, x_2 \in X$, there exists exactly one set $L \in \mathcal{L}$ such that $x_1 \in L$ and $x_2 \in L$.

Two parallel lines will be intersected.

[1] Nešetřil, Jaroslav, and Jiří Matoušek. Invitation to discrete mathematics. Vol. 21. Oxford University Press, 2009.

# Projective Planes

**Proposition 2:**

Let $(X, \mathcal{L})$ be a finite projective plane. Then all its lines have the same number of points.

**Definition 3:**

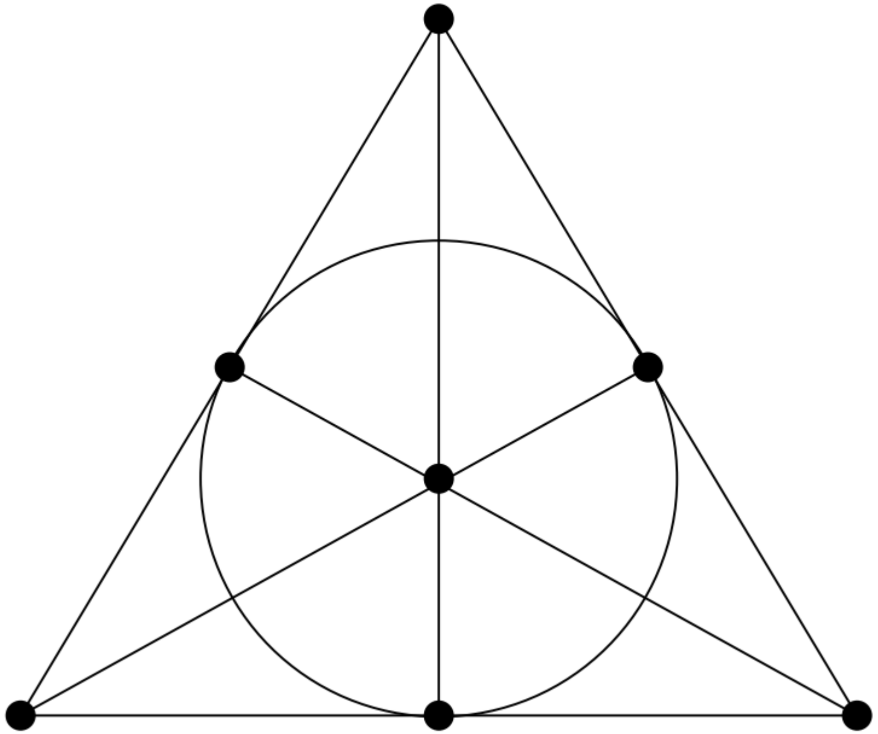
The order of a finite projective plane $(X, \mathcal{L})$ is the number $n = |L| - 1$, where $L \in \mathcal{L}$ is a line.

**Proposition 4:**

1. Exactly $n + 1$ lines pass through each point of $X$.

2. $|X| = n^2 + n + 1$.

3. $|\mathcal{L}| = n^2 + n + 1$.



The Fano plane, PG(2,2)

[1] Nešetřil, Jaroslav, and Jiří Matoušek. Invitation to discrete mathematics. Vol. 21. Oxford University Press, 2009.

# Linear Codes

**Definition 5:**

A code of length $n$ is a set of $n$-tuples (called codewords) of a set (called the alphabet).

Linear $[n, k, d]$ code $C$ over $F_q$ is $k$-dimensional subspace of $V(n, q)$, $d$ is the minimal number of positions in which two distinct codewords differ.

**Example:**

{000, 111} is [3, 1, 3] code.

{000, 011, 101, 110} is [3, 2, 2] code.

**Generator matrix** of $[n, k, d]$ code $C$

$$G = (g_1 \dots g_n)$$

$G = (k \times n)$ matrix of rank $k$,

Rows of $G$ form basis of $C$,

Codeword of $C$ = linear combination of rows of $G$.

**Parity check matrix** $H$ for $C$

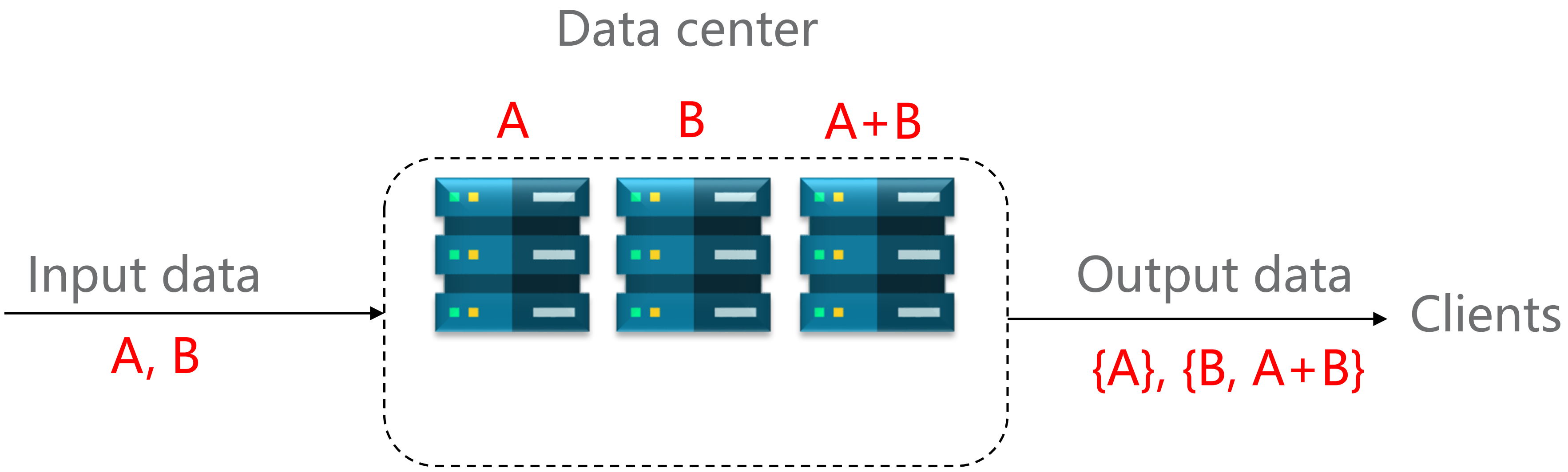
$(n-k) \times n$ matrix of rank $n-k$,

We have $c \in C \Leftrightarrow c \cdot H^T = \bar{0}$.

$$\boldsymbol{HG^T = GH^T = 0}$$

[1] Roth, Ron M. "Introduction to coding theory." IET Communications 47 (2006).
[2] Etzion, Tuvi, and Leo Storme. "Galois geometries and coding theory." Designs, Codes and Cryptography 78.1 (2016): 311-350.

# Generator Matrix




$$[A\ B]\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix} = [A\ B\ A+B]$$

**Coded Storage**

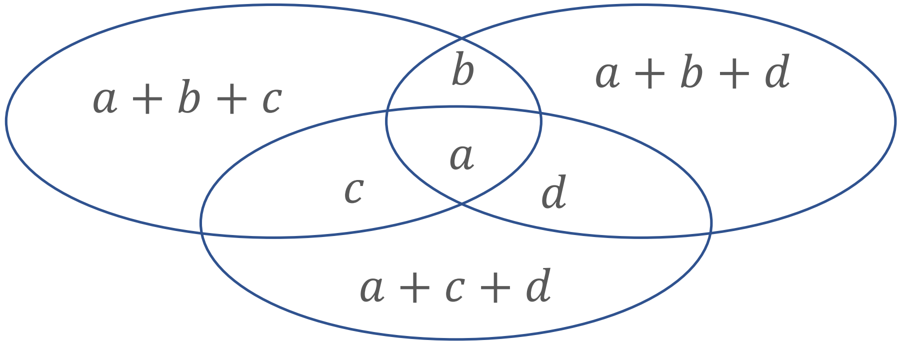
$$\boldsymbol{G} = \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}, \boldsymbol{H} = [1\ 1\ 1]$$

$$\boldsymbol{H}\boldsymbol{G}^T = \boldsymbol{G}\boldsymbol{H}^T = \boldsymbol{0}$$

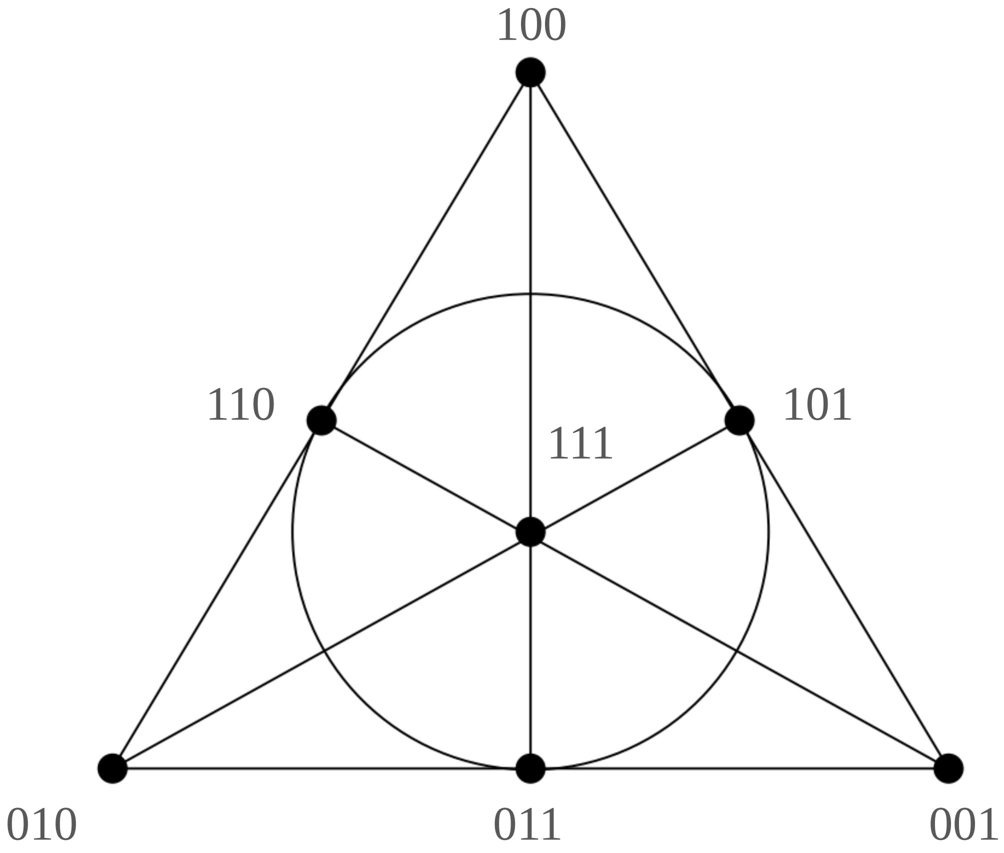
# Hamming codes

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

The parity check matrix of $[7, 4, 3]$ Hamming codes




Venn diagram of $[7, 4, 3]$ Hamming codes




Labeling the Fano plane

[1] Nešetřil, Jaroslav, and Jiří Matoušek. Invitation to discrete mathematics. Vol. 21. Oxford University Press, 2009.
[2] Lavrauw, Michel, Leo Storme, and Geertrui Van de Voorde. "Linear codes from projective spaces." Error-Correcting Codes, Finite Geometries, and Cryptography, AMS Contemporary Mathematics (CONM) book series 523 (2010): 185-202.

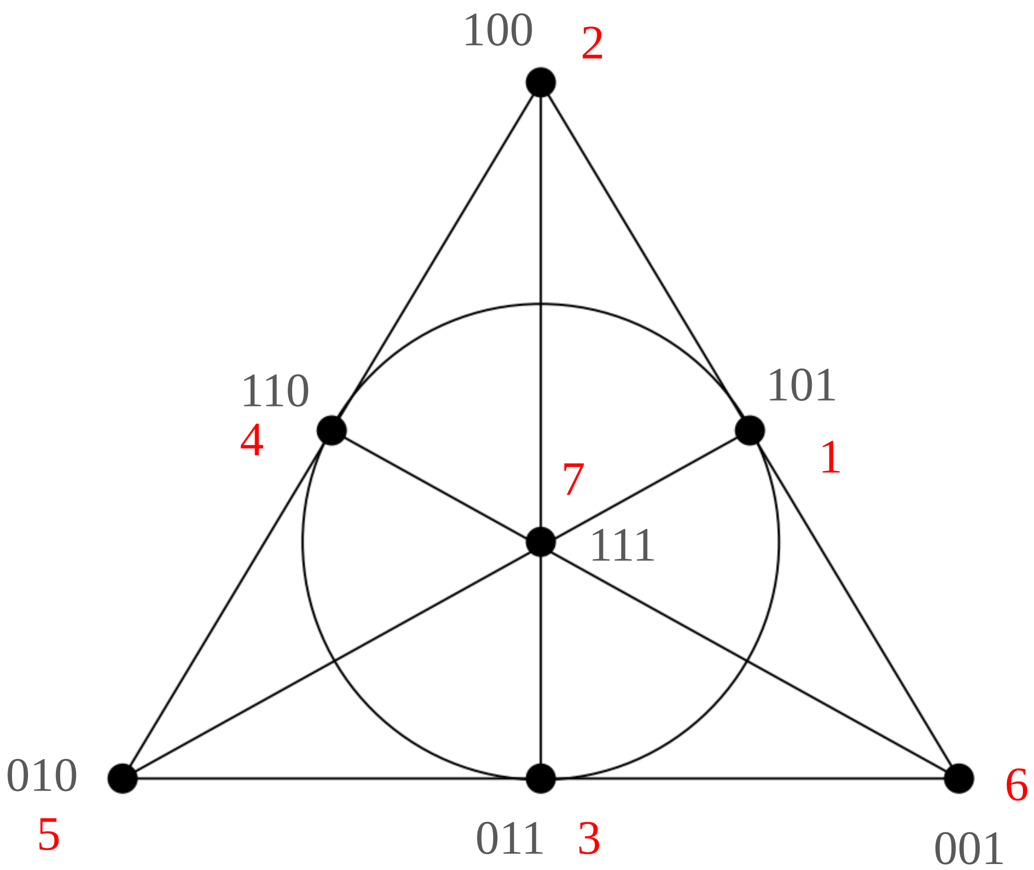
# Hamming codes

$$
\begin{array}{cc}
 & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\
A = & \begin{bmatrix}
1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\end{array}
\quad
\begin{array}{c}
1,3,4 \\ 2,4,5 \\ 3,5,6 \\ 4,6,7 \\ 1,5,7 \\ 1,2,6 \\ 2,3,7
\end{array}
$$

Incidence matrix of $[7,4,3]$ Hamming codes

Reorder the columns of $H$ in order to get the cyclic form of $A$.

$$
H = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1
\end{bmatrix}
\qquad \boldsymbol{HA^T = AH^T = 0}
$$




Labeling the Fano plane

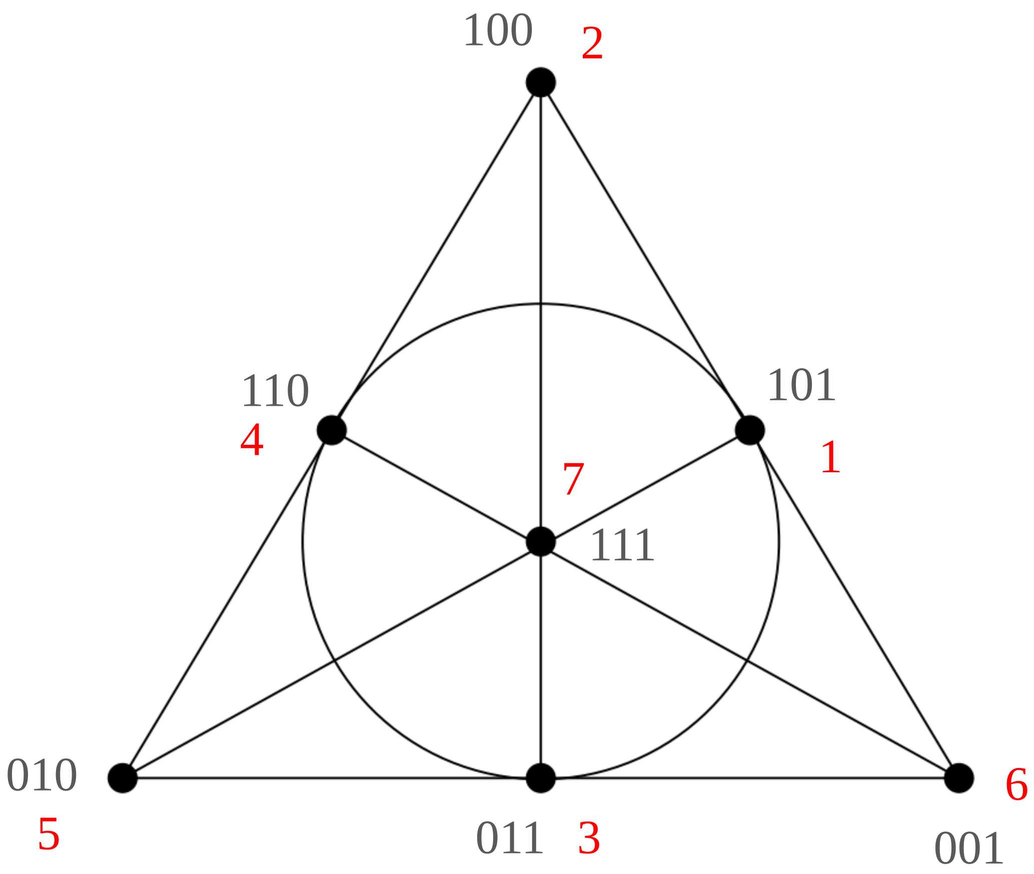
## Hamming codes

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

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

Generator matrix of $[7, 4, 3]$ Hamming codes

Moorhouse basis

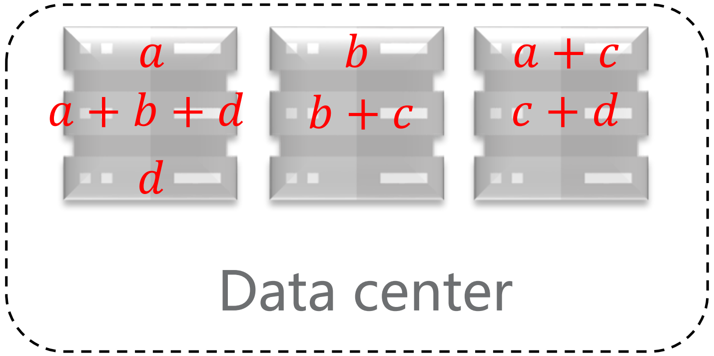



Labeling the Fano plane

[1] Moorhouse, G. Eric. "Bruck nets, codes, and characters of loops." Designs, Codes and Cryptography 1.1 (1991): 7-29.

# Encoding

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




Input data

$$[a, b, c, d] * \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$= [a, b, a+c, a+b+d, b+c, c+d, d]$$

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

Assume the first column is broken [$a$].
We can reconstruct it by [$b + a + b + d + d$]
or [$a + c + c + d + d$].

[1] Moorhouse, G. Eric. "Bruck nets, codes, and characters of loops." Designs, Codes and Cryptography 1.1 (1991): 7-29.

# Incidence Matrix

**Incidence Matrix:**

$$A_q = (a_{ij})$$

$$a_{ij} = \begin{cases} 1, \text{if the point } i \text{ is incident with the hyperplane } j \\ 0, \text{otherwise} \end{cases}$$

***p*-Rank:**

The rank of the incidence matrix of points and hyperplanes in the $\mathrm{PG}(t, p^n)$ is $\binom{p+t-1}{t}^n + 1$.

In $\mathrm{PG}(2, q)$, $q$ odd: $\binom{q+1}{2} + 1 = \frac{q(q+1)}{2} + 1$.

*Example:* An incidence matrix $A_3$ of $\mathrm{PG}(2,3)$ is

$$A_3 = \begin{pmatrix} 1&1&0&0&1&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&1&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&1&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0&1&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0&1&0&1&0&0 \\ 0&0&0&0&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&0&1 \\ 1&0&0&0&0&0&0&1&1&0&0&1&0 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1 \\ 1&0&1&0&0&0&0&0&0&1&1&0&0 \\ 0&1&0&1&0&0&0&0&0&0&1&1&0 \\ 0&0&1&0&1&0&0&0&0&0&0&1&1 \\ 1&0&0&1&0&1&0&0&0&0&0&0&1 \end{pmatrix}.$$

The rank of $A_3$ is $\frac{3(3+1)}{2} + 1 = 7$.

$$H_3 = \begin{pmatrix} 1&1&0&0&1&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&1&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&1&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0&1&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0&1&0&1&0&0 \\ 0&0&0&0&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&0&1 \end{pmatrix}.$$

[1] Smith, Kempton JC. "On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry." Journal of Combinatorial Theory 7.2 (1969): 122-129.
[2] Moorhouse, G. Eric. "Bruck nets, codes, and characters of loops." Designs, Codes and Cryptography 1.1 (1991): 7-29.

# Cyclic

**Cyclic codes:**

Codes closed under cyclic shifts of codewords.

**Example** with $q = 2$:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Short description:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

**Example** with $q = 3$:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We can always find the short description when $q = n^2 + n + 1$ according to the perfect difference set.

**Three properties:**

- Cyclic,
- Every two different rows will intersect at exactly one point, $M_i \cdot M_{i'} = 1$ for every $i \neq i'$.
- The Hamming weight of each row is $q + 1$.

[1] Chowla, S. "On difference sets." Proceedings of the National Academy of Sciences of the United States of America 35.2 (1949): 92.
[2] Pless, Vera. "Cyclic projective planes and binary, extended cyclic self-dual codes." Journal of Combinatorial Theory, Series A 43.2 (1986): 331-333.

# Repair locality

The **locality** of a coded symbol $b_j$ is the minimum $r_j$ such that $b_j$ is a function of some other $r_j$ coded symbols

$$b_{i_1}, \dots, b_{i_r} \in \{b_1, \dots, b_n\} \setminus \{b_j\}.$$

Then $\{b_{i_1}, \dots, b_{i_r}\}$ is a **repair group** for $b_j$.

The **repair locality** $r$ of the code is $r = \max_j r_j$.

The repair locality $r$ of the linear code from finite projective plane $\mathrm{PG}(2, q)$ is $q$ with respect to the codeword length $q^2 + q + 1$.

Note: exactly $n + 1$ points in one line.

*Example:* An incidence matrix $A_3$ of $\mathrm{PG}(2,3)$ is

$$A_3 = \begin{pmatrix}
1&1&0&0&1&0&1&0&0&0&0&0&0\\
0&1&1&0&0&1&0&1&0&0&0&0&0\\
0&0&1&1&0&0&1&0&1&0&0&0&0\\
0&0&0&1&1&0&0&1&0&1&0&0&0\\
0&0&0&0&1&1&0&0&1&0&1&0&0\\
0&0&0&0&0&1&1&0&0&1&0&1&0\\
0&0&0&0&0&0&1&1&0&0&1&0&1\\
1&0&0&0&0&0&0&1&1&0&0&1&0\\
0&1&0&0&0&0&0&0&1&1&0&0&1\\
1&0&1&0&0&0&0&0&0&1&1&0&0\\
0&1&0&1&0&0&0&0&0&0&1&1&0\\
0&0&1&0&1&0&0&0&0&0&0&1&1\\
1&0&0&1&0&1&0&0&0&0&0&0&1
\end{pmatrix}.$$

$$H_3 = \begin{pmatrix}
1&1&0&0&1&0&1&0&0&0&0&0&0\\
0&1&1&0&0&1&0&1&0&0&0&0&0\\
0&0&1&1&0&0&1&0&1&0&0&0&0\\
0&0&0&1&1&0&0&1&0&1&0&0&0\\
0&0&0&0&1&1&0&0&1&0&1&0&0\\
0&0&0&0&0&1&1&0&0&1&0&1&0\\
0&0&0&0&0&0&1&1&0&0&1&0&1
\end{pmatrix}.$$

UNIVERSITY OF TARTU

# Repair availability

The (repair) **availability** of a coded symbol $c_j$ is its maximum number $t_j$ of pairwise disjoint repair groups;

The **repair availability** of the code given by generator matrix G is $t = \min_j t_j$.

The repair availability of the linear code from finite projective plane $\mathrm{PG}(2, q)$ is $q + 1$ with respect to the codeword length $q^2 + q + 1$.

Note: exactly $n + 1$ lines pass through each point.

*Example:* An incidence matrix $A_3$ of $\mathrm{PG}(2,3)$ is

$$A_3 = \begin{pmatrix} 1&1&0&0&1&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&1&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&1&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0&1&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0&1&0&1&0&0 \\ 0&0&0&0&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&0&1 \\ 1&0&0&0&0&0&0&1&1&0&0&1&0 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1 \\ 1&0&1&0&0&0&0&0&0&1&1&0&0 \\ 0&1&0&1&0&0&0&0&0&0&1&1&0 \\ 0&0&1&0&1&0&0&0&0&0&0&1&1 \\ 1&0&0&1&0&1&0&0&0&0&0&0&1 \end{pmatrix}.$$

$$G_3^{(1)} = \begin{pmatrix} 1&1&0&0&1&-1&0&0&0&-1&0&-1&0 \\ 1&1&0&0&1&0&0&-1&0&0&-1&0&-1 \\ 0&1&1&0&0&0&-1&1&0&-1&0&-1&0 \\ 0&0&1&1&0&-1&0&0&1&-1&0&-1&0 \\ 0&0&0&1&1&0&-1&0&0&1&-1&0&-1 \\ 0&0&0&0&1&1&-1&-1&1&0&0&0&-1 \end{pmatrix}.$$

UNIVERSITY OF TARTU

1632

# Thanks for your attention