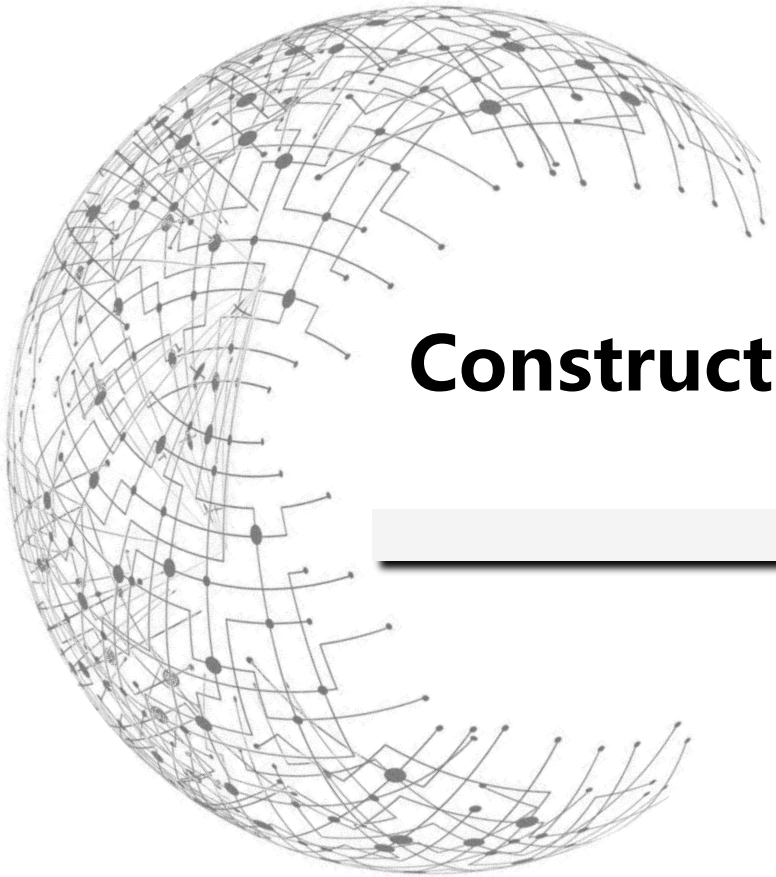
UNIVERSITY OF TARTU

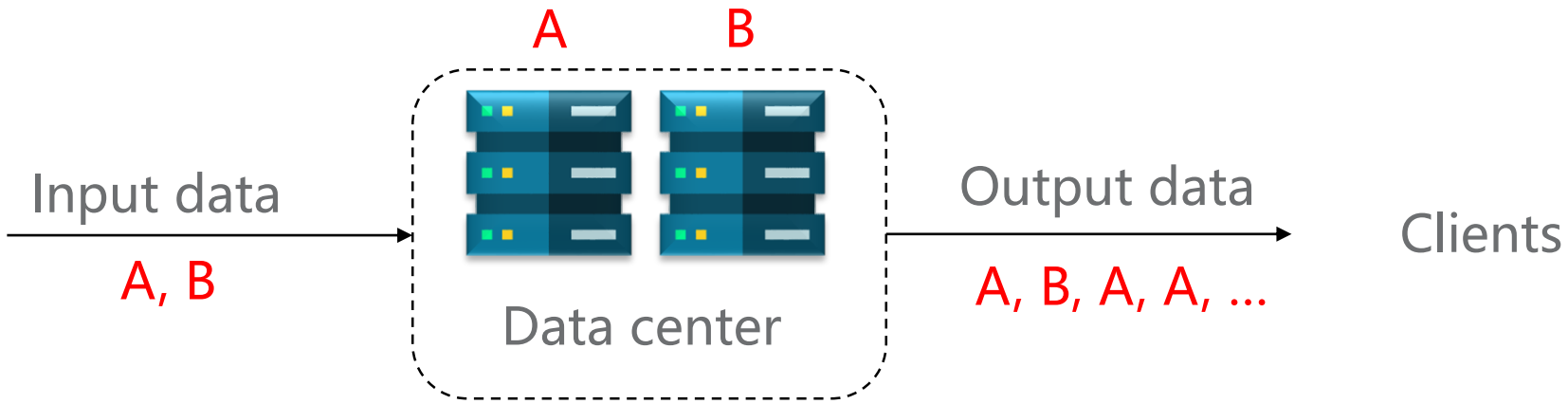


Constructing Update-Efficient Storage Codes via Finite Projective Planes

Junming Ke, Ago-Erik Riet

Joint Latvian-Estonian Theory Days 2022

Background



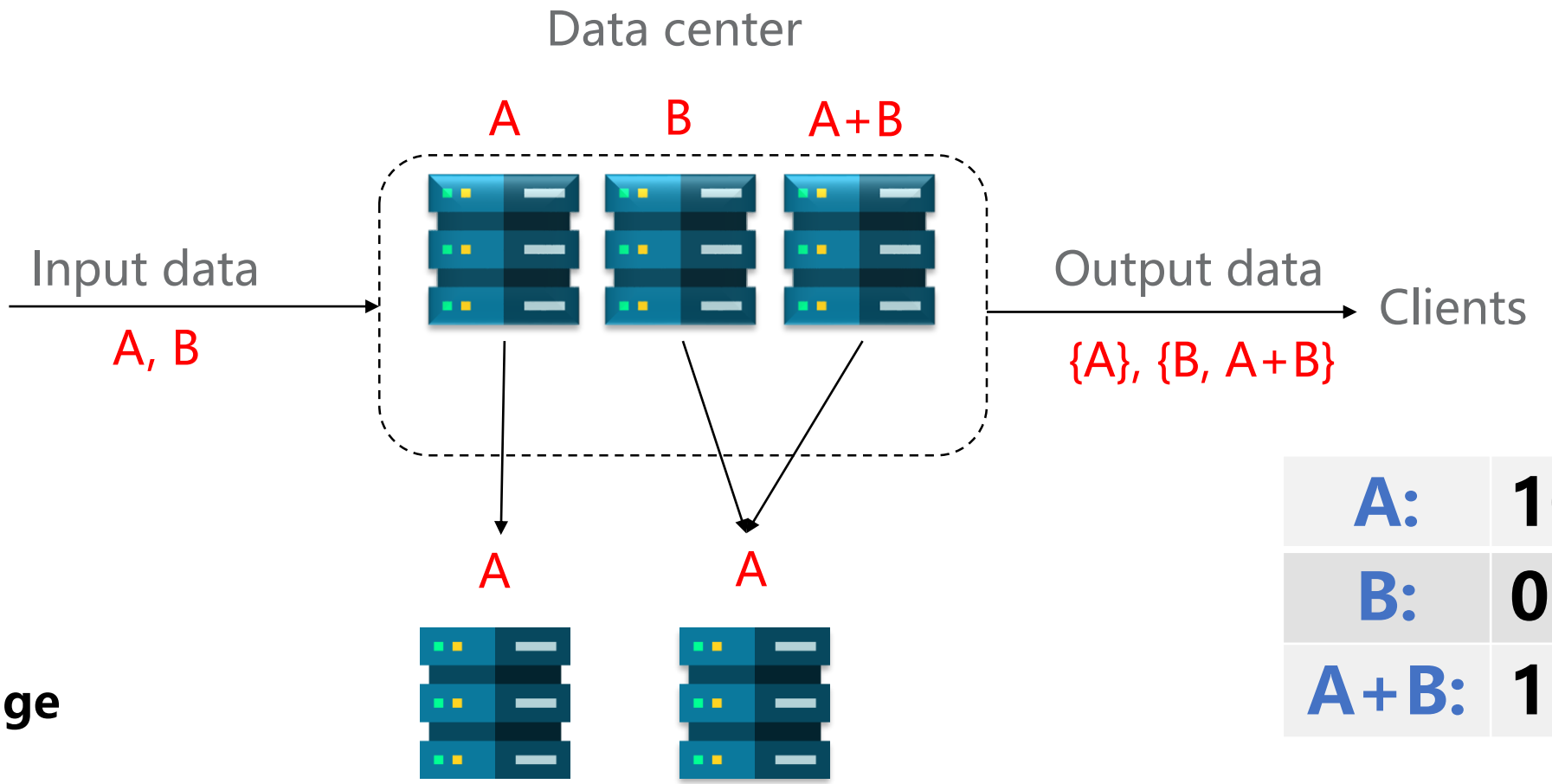
Storage

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.

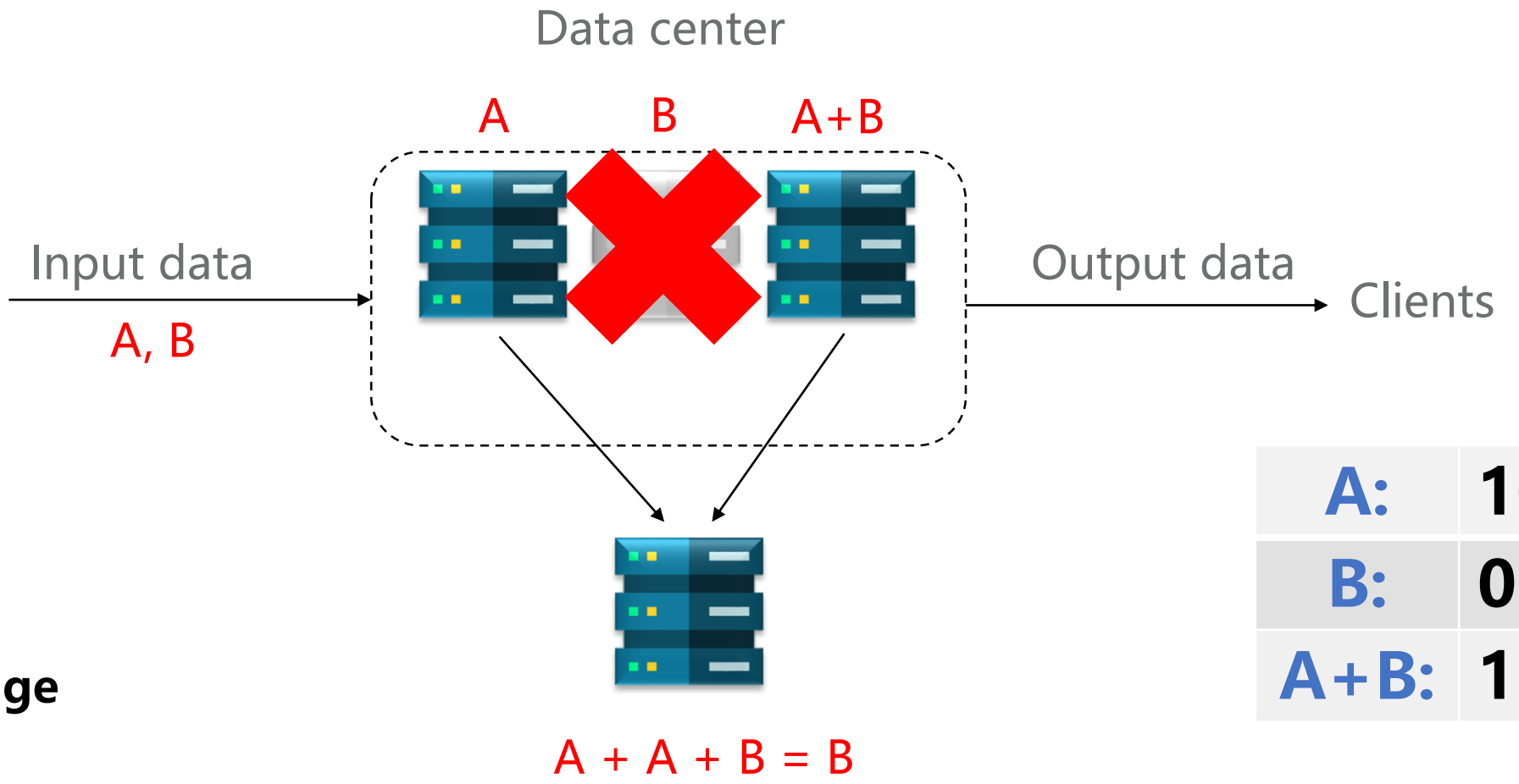
Background



Coded Storage

A:	10
B:	01
A+B:	11

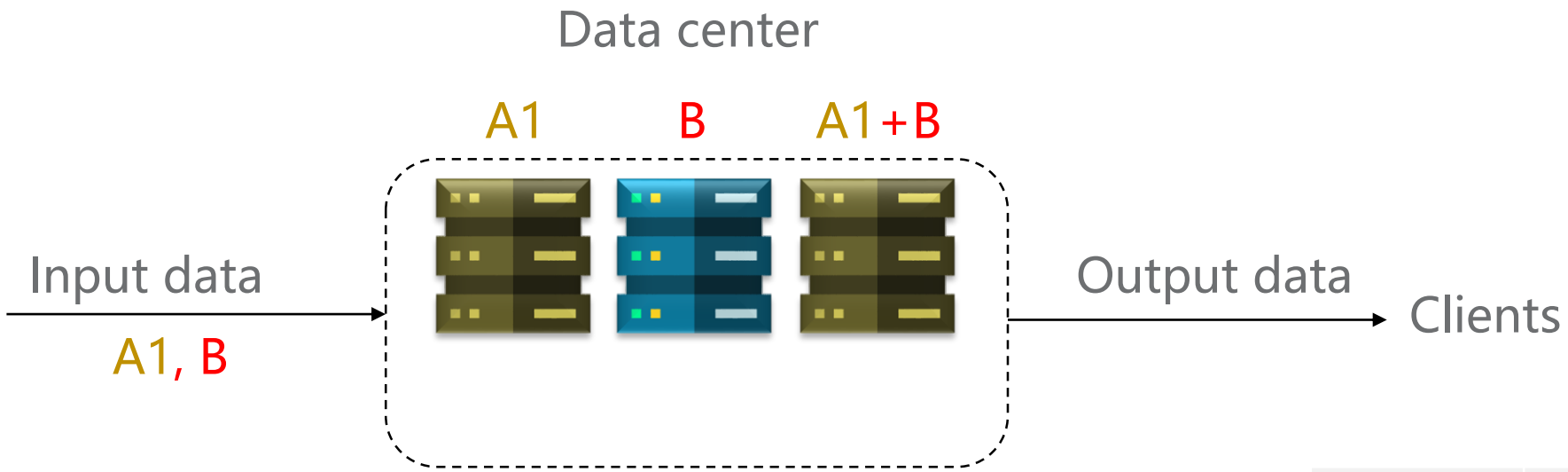
Repair



A:	10
B:	01
A+B:	11

Coded Storage

Update



A:	10
B:	01
A+B:	11

Coded Storage

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:

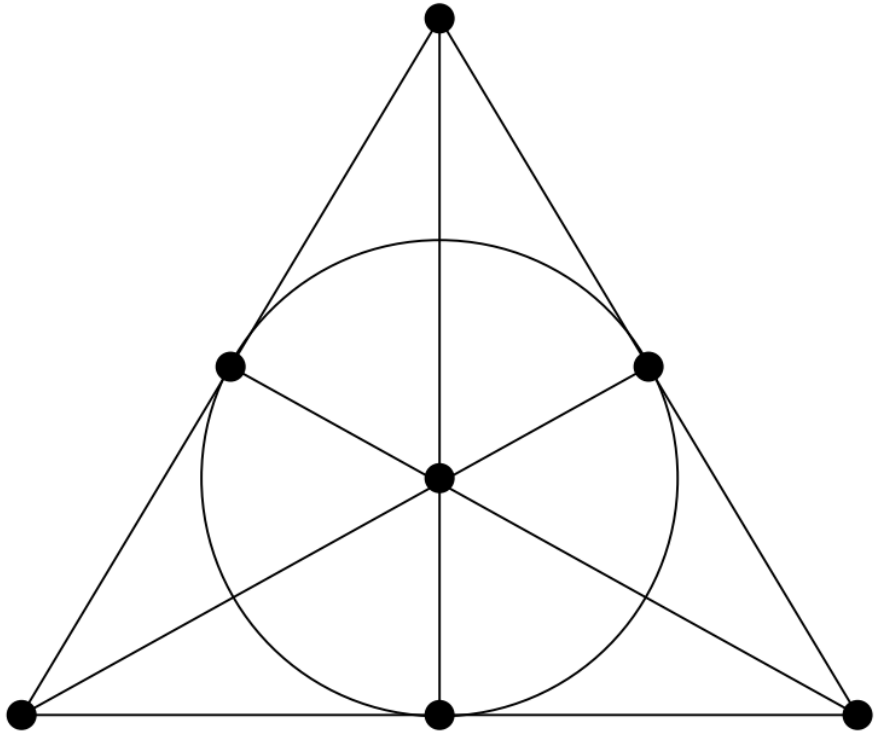
Let $(X, \mathcal{L})$ be a finite projective plane. Then all its lines have the same number of points.

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.

Oval, Arc, and Conic

Definition 6:

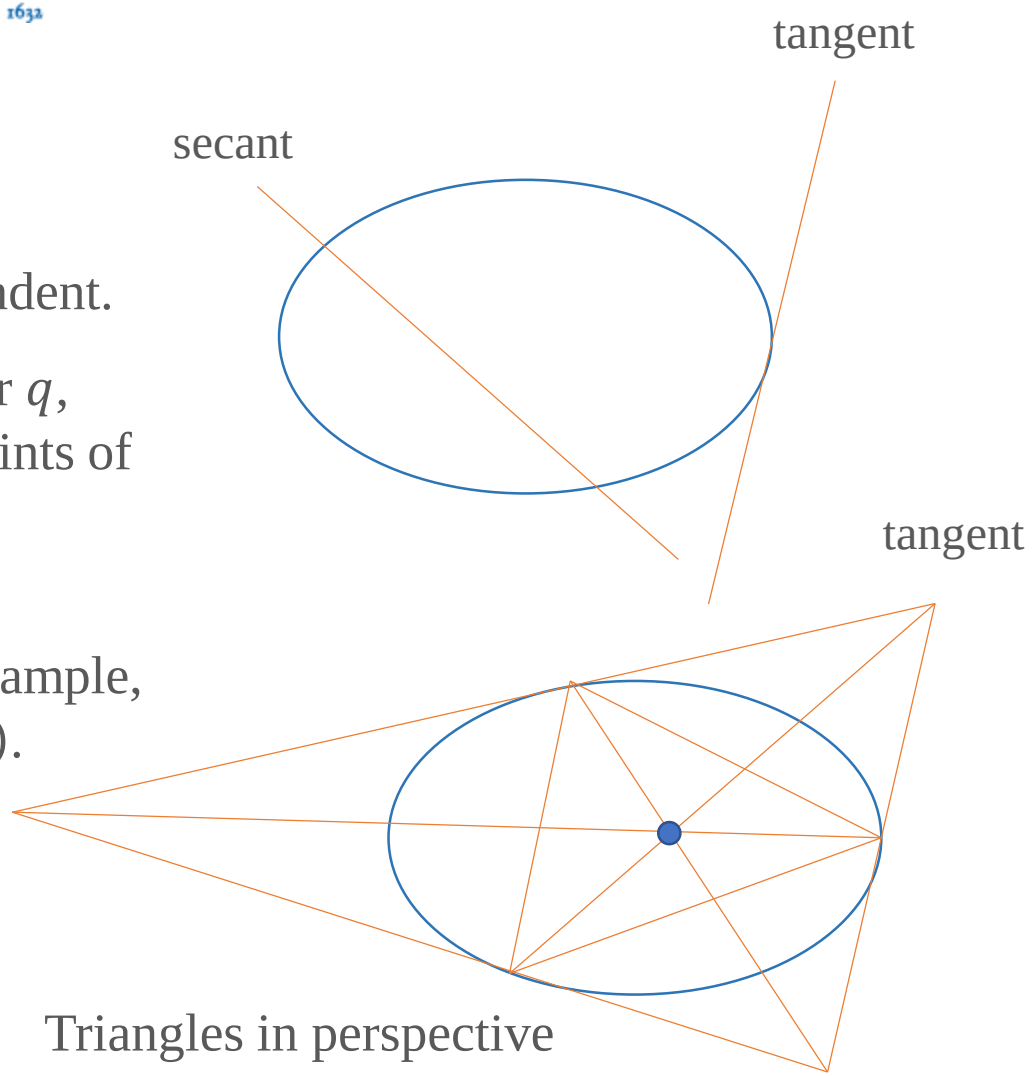
n-Arc in PG$(k-1,q)$: set of n points, every k linearly independent.

An oval O is a set of $q+1$ points in a projective plane of order q, with the property that every line is incident with at most two points of O.

A conic is a set of points of PG$(2,q)$ that are zeros of a non-degenerate homogeneous quadratic form (in 3 variables), for example, $C=\{\langle(x,y,z)\rangle | x^2=yz\}$. All conics are equivalent in PG$(2,q)$.

Segre's theorem:

An oval ($q+1$-Arc) in PG$(2,q)$, q odd, is a conic.



Triangles in perspective

[1] Roth, Ron M. "Introduction to coding theory." IET Communications 47 (2006).
[2] Ball, Simeon, and Zsuzsa Weiner. "An introduction to finite geometry." Preprint 162 (2011).

UNIVERSITY OF TARTU

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.

Bounds of Codes

Singleton Bound:

$$d \leq n - k + 1$$

MDS (maximum distance separable) code is $[n, k, n - k + 1]$ code.

Griesmer Bound:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

Equivalence:

Singleton (upper) bound (MDS codes) is equivalent with arcs in finite projective spaces.

Griesmer (lower) bound is equivalent with minihypers in finite projective spaces.

Minihyper:

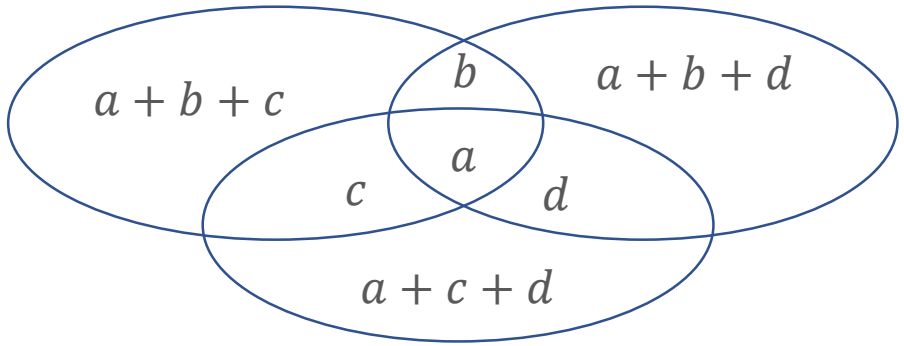
$\{f, m; k - 1, q\}$ – minihyper F is a set of f points in $PG(k - 1, q)$, F intersects every $(k - 2)$ −dimensional space in at least m points.

[1] Alderson, T. L., Aiden A. Bruen, and Robert Silverman. "Maximum distance separable codes and arcs in projective spaces." Journal of Combinatorial Theory, Series A 114.6 (2007): 1101-1117.

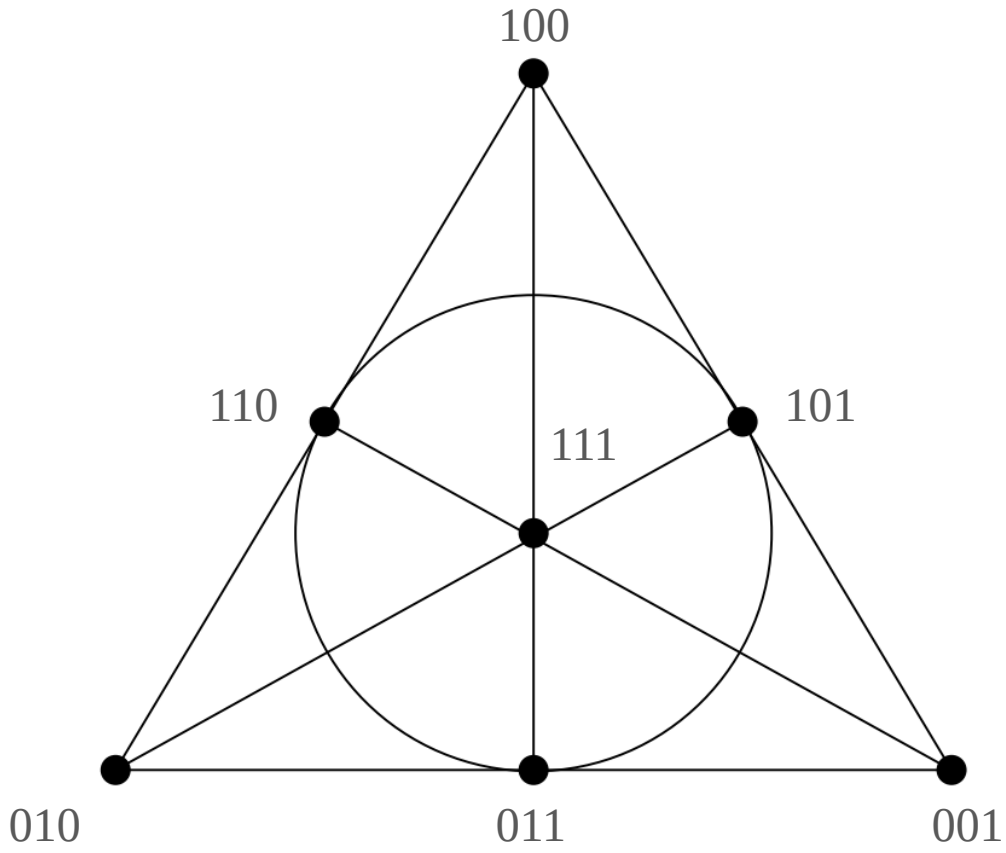
Hamming codes

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

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



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



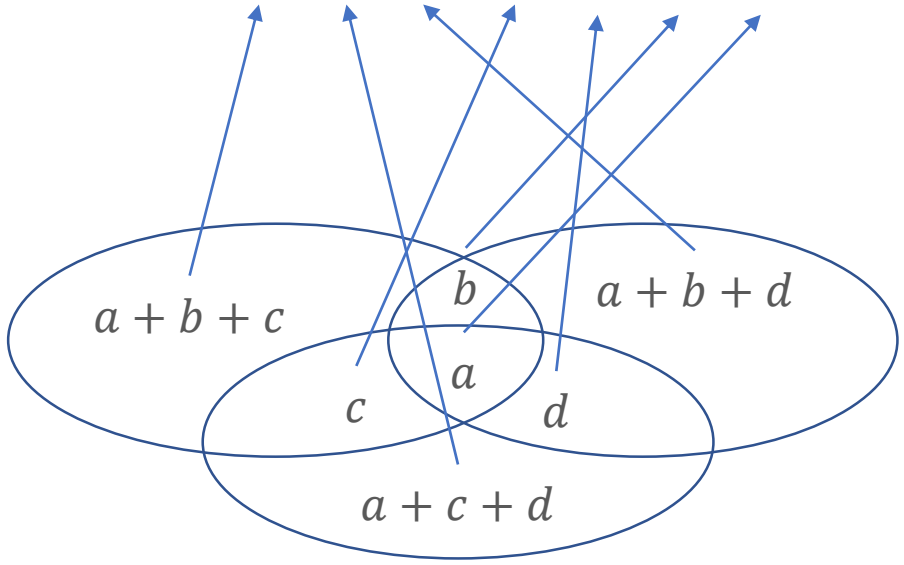
Labeling the Fano plane

[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.

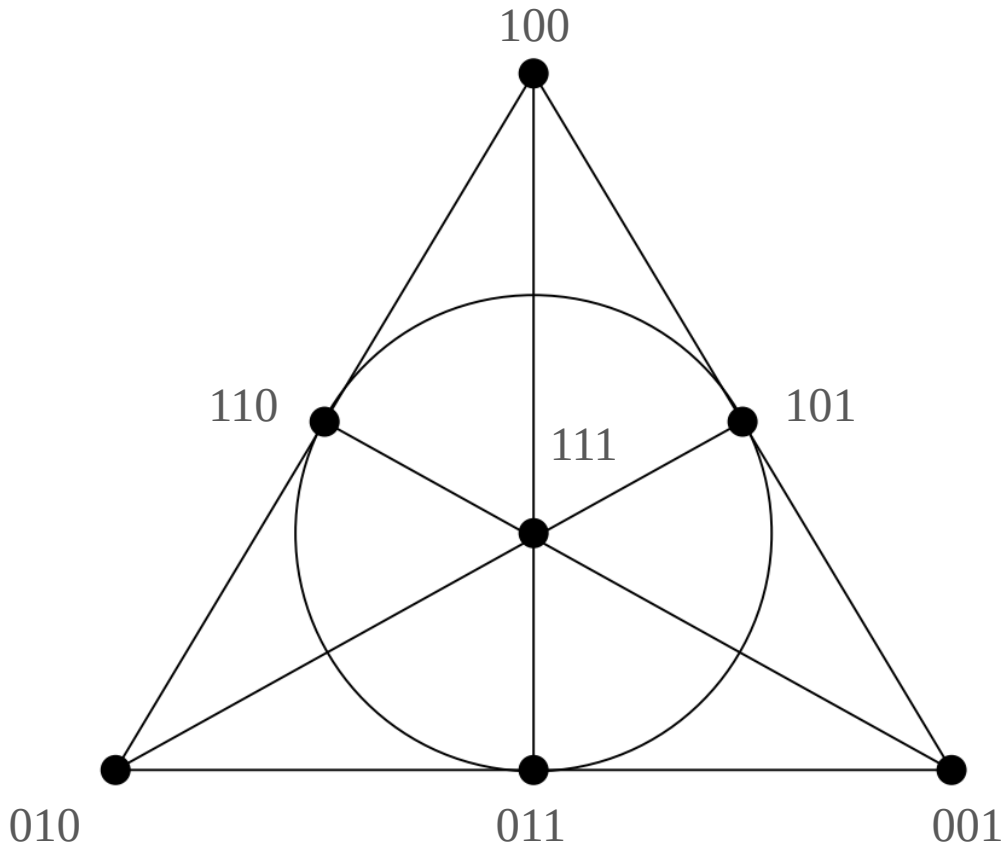
UNIVERSITY OF TARTU

Hamming codes

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



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

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

1 2 3 4 5 6 7

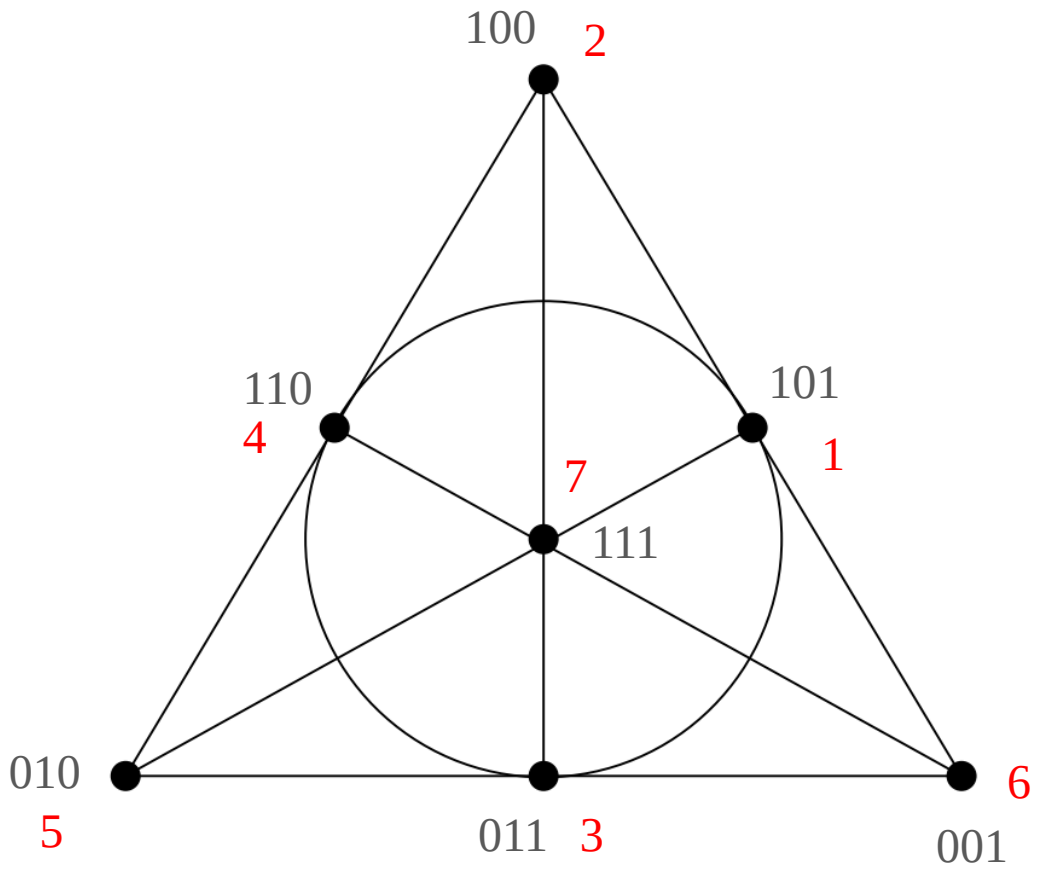
1, 3, 4
2, 4, 5
3, 5, 6
4, 6, 7
1, 5, 7
1, 2, 6
2, 3, 7

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

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

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

$$\boldsymbol{HA^T = AH^T = 0}$$



Labeling the Fano plane

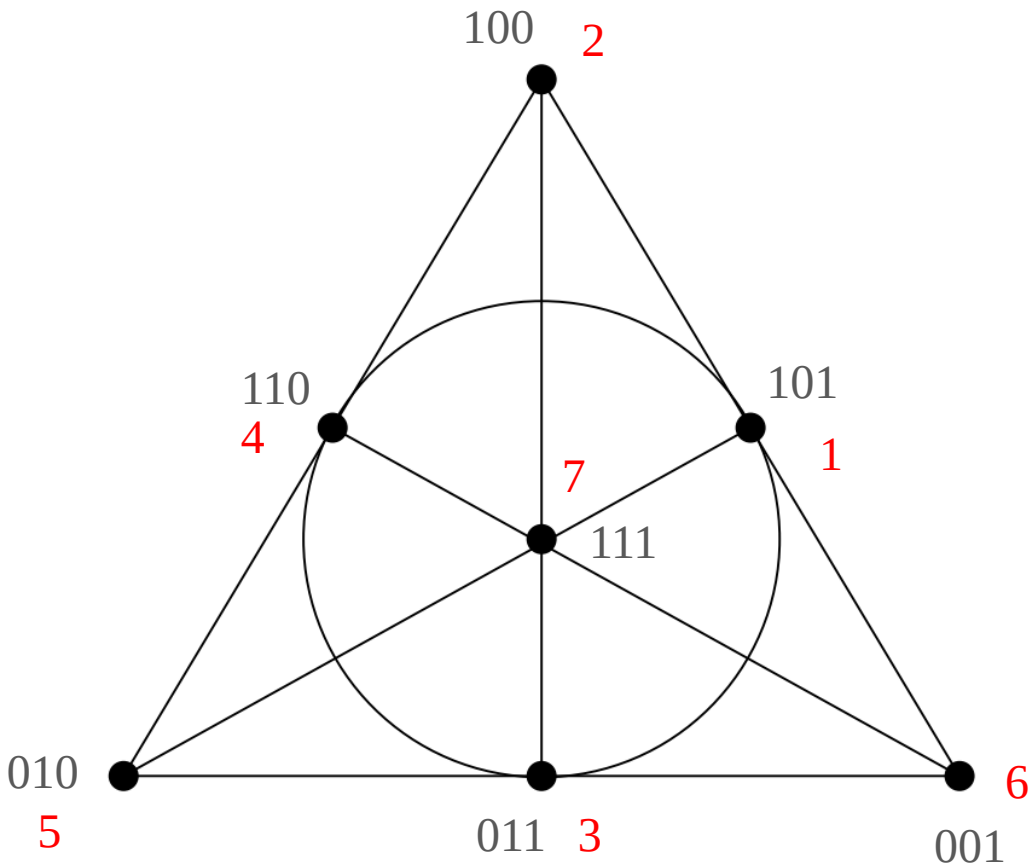
Hamming codes

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

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

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.

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.

Codeword

Let G be the generator matrix of $[n, k, d]$ code over F_q:

- $n = q^2 + q + 1$,
- $k = \binom{q+1}{2} + 1$,
- $d = q + 1$.

Theorem:

If $w(c) = q + 1$, then c = incidence vector of a line, up to a scalar multiple.

The second smallest weight is $2q$, are the difference of two lines, up to scalar multiple.

When q is constrained, the other small-weight codewords can also be determined.

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

We will consider the **dual codes**. The generator matrix is shown below (is one of the parity-check matrix of G).

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

[1] Fack, Veerle, et al. "Small weight codewords in the codes arising from Desarguesian projective planes." Designs, Codes and Cryptography 46.1 (2008): 25-43.

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:

$$(1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0)$$

Example with $q = 3$:

$$(1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)$$

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

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.

Sparsity

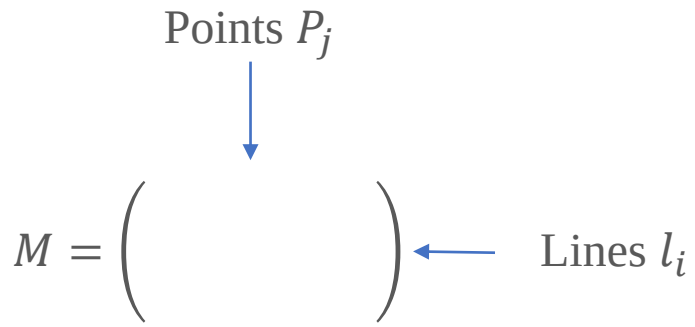
Low-density parity-check (LDPC) codes:

- Proposed by Gallager, 1960,
- Allow the noise threshold to be very close to the theoretical maximum,
- Achieve List Decoding Capacity [1].

LDPC codes are constructed by using the **sparse parity-check matrix.**

Another code with sparse **generator matrix** is **Convolutional code.**

The incidence matrix of projective plane can provide **Moderate Density** generator and parity-check **matrices.**



- $M_{ij} = 1$ iff $P_j \in l_i$,
- $M_{ij} = 0$ iff $P_j \notin l_i$,

The relative Hamming weight of each row:

$$\frac{q+1}{q^2+q+1} \approx \frac{1}{q}$$

[1] Mosheiff, Jonathan, et al. "LDPC codes achieve list decoding capacity." 2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2020.
[2] Bariffi, Jessica, et al. "Moderate Density Parity-Check Codes from Projective Bundles." arXiv preprint arXiv:2103.09722 (2021).

Update efficiency

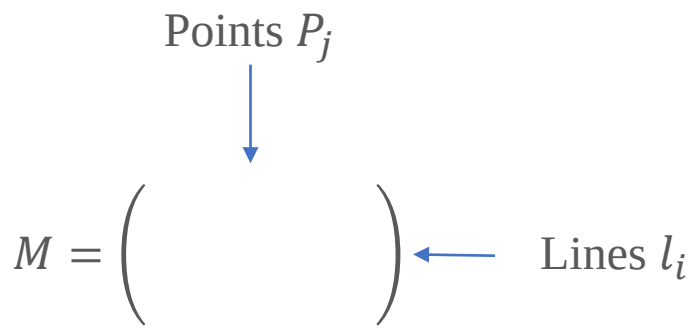
The update efficiency u_i of a data symbol a_i is **the number of coded symbols** that need to be updated when updating a_i.

Or, the update efficiency u_i of a data symbol a_i is **the weight of the i-th row** of G.

The update efficiency u of the code given by G is

$$\boldsymbol{u = \max_i u_i}.$$

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



- $M_{ij} = 1$ iff $P_j \in l_i$,
- $M_{ij} = 0$ iff $P_j \notin l_i$,

The relative Hamming weight of each row:

$$\frac{q+1}{q^2+q+1} \approx \frac{1}{q}$$

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

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

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

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

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

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

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

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

Repair algorithm

Algorithm A:

While possible, do:

Find a projective line with exactly one erased point or coded symbol (corresponding to a server that is down), and repair this coded symbol or server from the other points (coded symbols or servers) of the line.

Specifically, the coded symbol is repaired to minus the sum of the other coded symbols of the line (over $\mathbb{F}_q$).

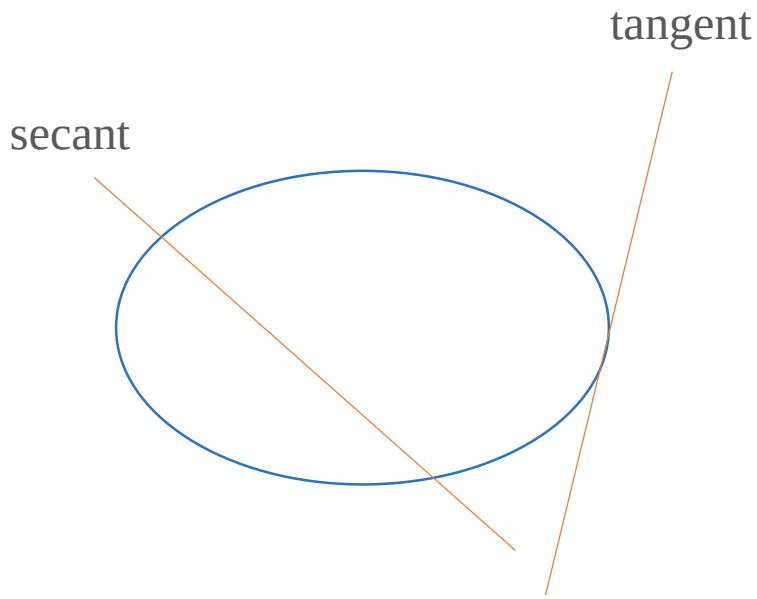
$$A_3 = \begin{pmatrix} 1&1&0&0&1&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&1&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&1&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0&1&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0&1&0&1&0&0 \\ 0&0&0&0&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&0&1 \\ 1&0&0&0&0&0&0&1&1&0&0&1&0 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1 \\ 1&0&1&0&0&0&0&0&0&1&1&0&0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

Example:

Suppose the set of erased coded symbols is $\{b_1, b_2, b_3, b_4, b_8\}$. At first, **Algorithm A** cannot repair b_1 or b_4, as each line through b_1 or b_4 (each repair group) has an erased symbol. But after repairing $\{b_2, b_3, b_8\}$ respectively from, say, repair groups $\{b_9, b_{10}, b_{13}\}$, $\{b_5, b_{12}, b_{13}\}$, $\{b_7, b_{11}, b_{13}\}$ (here putting total load 3 on server b_{13}), symbols b_1, b_4 can then be repaired from, say, repair groups $\{b_2, b_5, b_7\}$, $\{b_3, b_8, b_{10}\}$.

Stopping sets

The **stopping sets** here are precisely the **sets without tangents** in geometry, that is, sets of projective points intersecting no line in exactly one point.



Sets without tangents are closed under unions, like stopping sets, there is a unique largest set without tangents S that is a subset of a given set T of failed servers.

Example:

Suppose the set of erased coded symbols contains the set $\{b_2, b_3, b_5, b_6, b_7, b_8\}$. This is a stopping set (as it is the union of two lines through b_1, without b_1), so any line meeting this set meets it in at least 2 points. **Algorithm A** never manages to repair any of those servers.

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

UNIVERSITY OF TARTU

Thanks for your attention