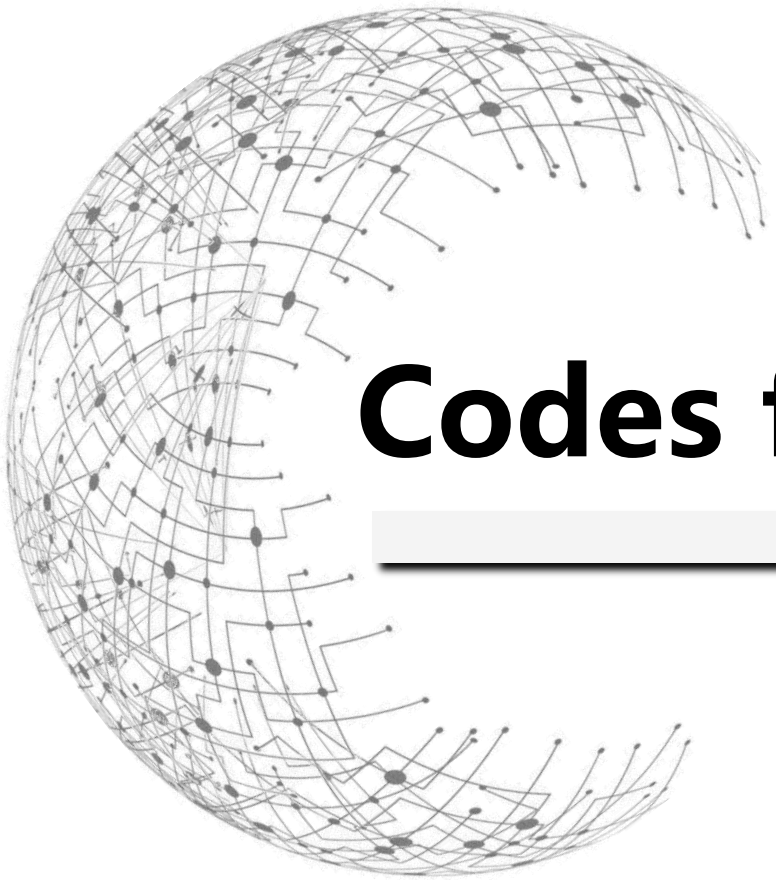
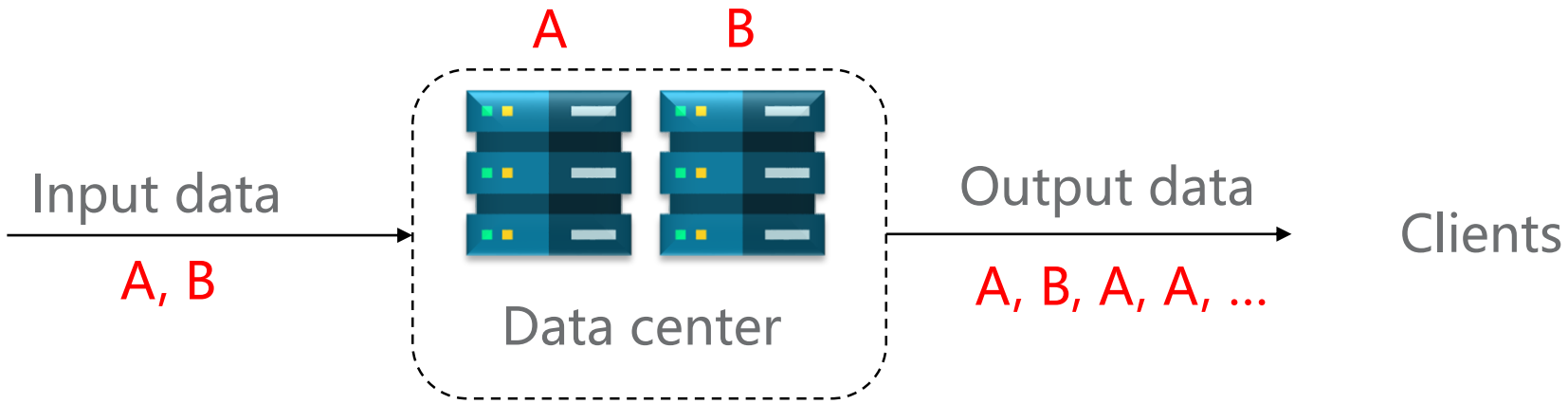
UNIVERSITY OF TARTU



Codes from Projective Planes

Junming Ke
University of Tartu
19 August, 2021

Background



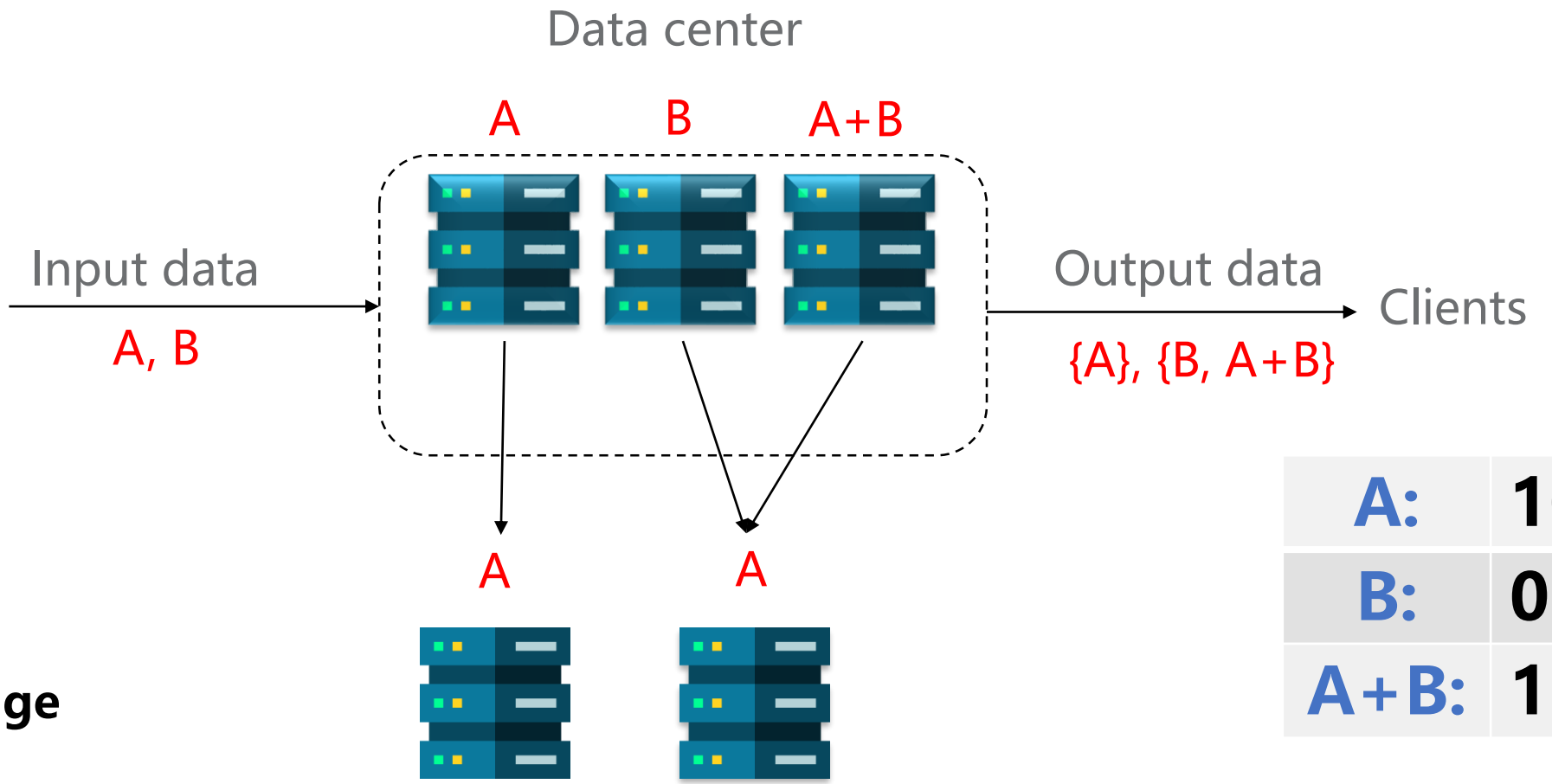
Storage

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

UNIVERSITY OF TARTU

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.

UNIVERSITY OF TARTU

Projective Planes

Proposition 2:

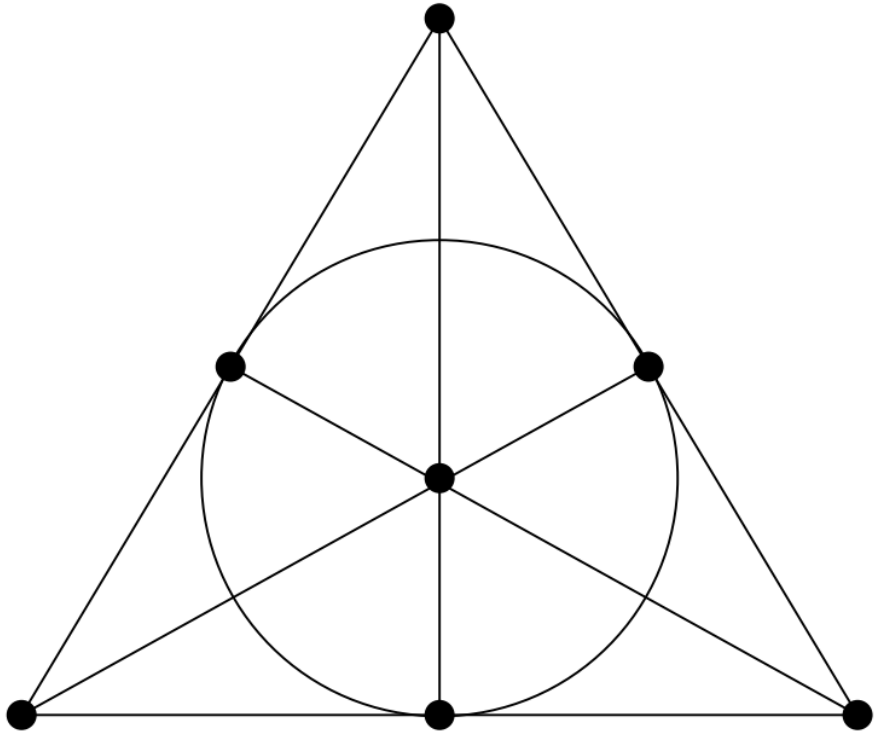
Let $(X, \mathcal{L})$ be a finite projective plane. Then all its lines have the same number of points.

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.

UNIVERSITY OF TARTU

Oval, Arc, and Conic

Definition 6:

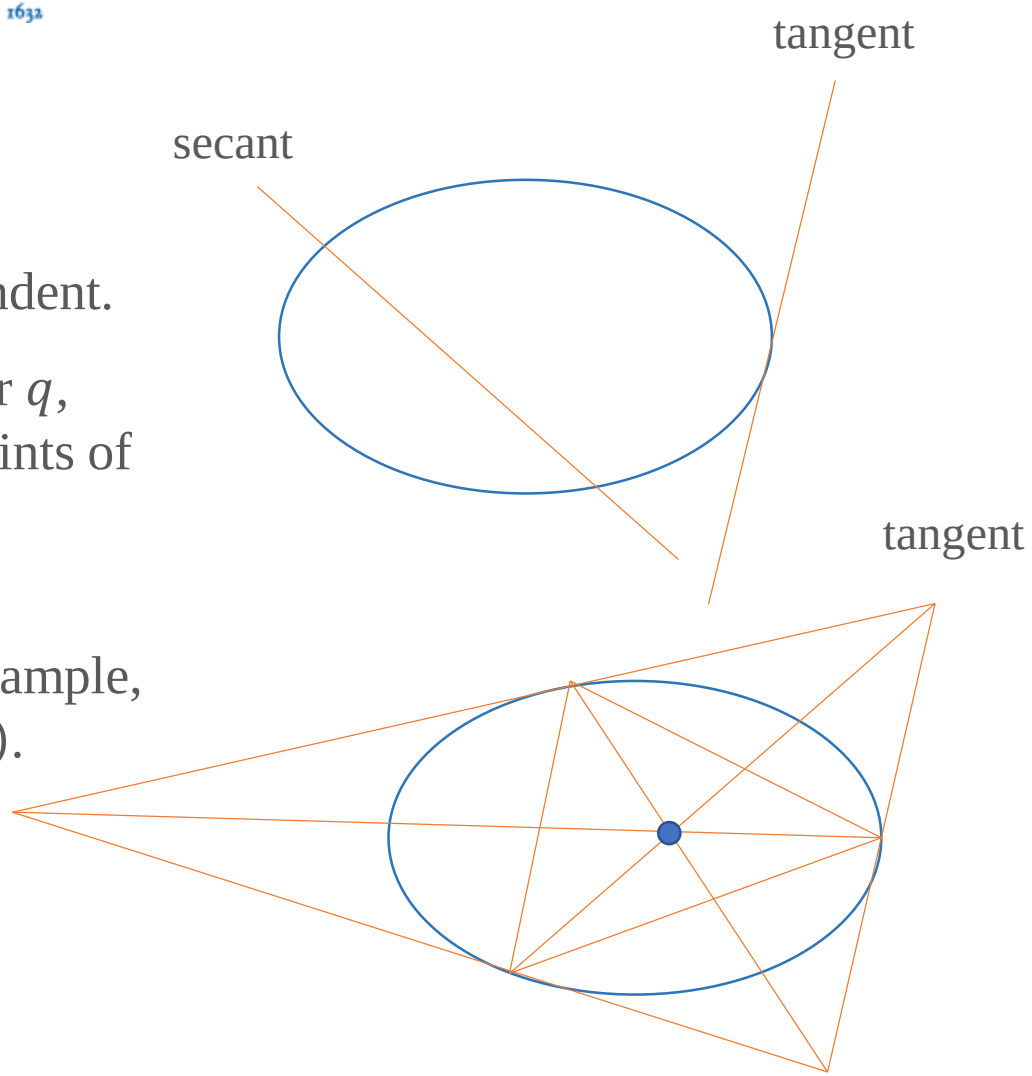
n-Arc in $PG(k-1,q)$: set of n points, every k linearly independent.

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 $[3, 2, 3]$ code.

$\{000, 011, 101, 110\}$ is $[3, 4, 2]$ 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.

UNIVERSITY OF TARTU

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.

UNIVERSITY OF TARTU

Incidence Matrix

Incidence Matrix:

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

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

***p*-Rank:**

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

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

Example: the incidence matrix of $PG(2,3)$ is

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

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

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

[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.

UNIVERSITY OF TARTU

Codeword

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

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

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

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.

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

[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.

UNIVERSITY OF TARTU

Sparsity

Low-density parity-check (LDPC) codes:

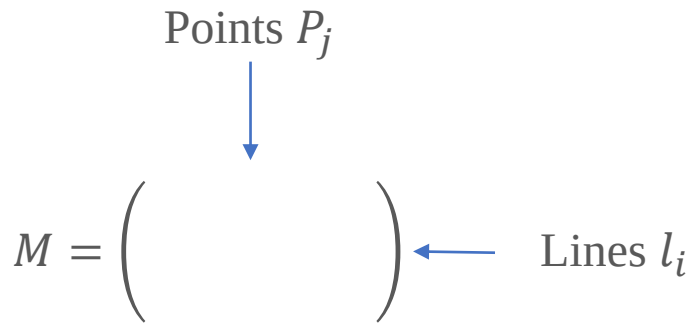
- Proposed by Gallager, 1960,
- Allow the noise threshold to be very close to the theoretical maximum,
- Achieve List Decoding Capacity [1].

LDPC codes are constructed by using the **sparse matrix.**

The incidence matrix of projective plane can provide a **sparse matrix.**

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

The **comparisons** of these codes are worth to be investigated.



- $M_{ij} = 1$ 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.

UNIVERSITY OF TARTU
1632

Cyclic

Cyclic codes:

Codes closed under cyclic shifts of codewords.

Example with $q = 2$:

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

Small 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 small 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.

UNIVERSITY OF TARTU

Thanks for your attention