On Binary Matroid Minors and Applications to Data Storage over Small Fields

Matthias Grezet

University of Aalto

28th August 2017

Joint work with R. Freij-Hollanti, T. Westerbäck and C. Hollanti.

Aalto University
School of Science

Definition (LRC)

A linear $(n, k, d, r, \delta)-$**LRC** over $\mathbb{F}$ is a non-degenerate linear $(n, k, d)-$code C over $\mathbb{F}^E$ such that any coordinate $x \in E$ of C has locality (r, δ), meaning that there is $R \subset E$, called **the repair set** of x, such that

- $x \in R$
- $|R| \leq r + \delta - 1$
- $d_R \geq \delta$

Example

A $(10, 4, 4, 4, 3)$ binary linear code given by the generator matrix

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

Definition (Matroid)

A **matroid** $M = (\rho, E)$ is a finite set E with a rank function $\rho : 2^E \to \mathbb{Z}$ such that $\forall X, Y \subseteq E$

R1) $0 \leq \rho(X) \leq |X|$,

R2) $X \subseteq Y \Rightarrow \rho(X) \leq \rho(Y)$,

R3) $\rho(X) + \rho(Y) \geq \rho(X \cup Y) + \rho(X \cap Y)$.

Some useful tools:

- The **nullity function** $\eta : 2^E \to \mathbb{Z}, \eta(X) = |X| - \rho(X)$.
- The **closure operator** $\mathrm{cl} : 2^E \to 2^E, \mathrm{cl}(X) = X \cup \{e \in E - X : \rho(X \cup e) = \rho(X)\}$.
- The **cyclic operator** $\mathrm{cyc} : 2^E \to 2^E, \mathrm{cyc}(X) = \{e \in X : \rho(X - e) = \rho(X)\}$.

Cyclic flats

A subset $X \subseteq E$ is a **cyclic flat** if, for all $y \in E - X$ and $x \in X$, we have

$$\rho(X \cup y) > \rho(X) \text{ and } \rho(X - x) = \rho(X)$$

We denote by $\mathcal{Z}(M)$ the set of cyclic flats of M.

Proposition

$(\mathcal{Z}, \subseteq)$ is a lattice with $X \wedge Y = \mathbf{cyc}(X \cap Y)$ and $X \vee Y = \mathbf{cl}(X \cup Y)$.

Minors

Let $X, Y \subseteq E$.

- The **restriction** of M to Y is the matroid $M|Y = (\rho_{|Y}, Y)$, where $\rho_{|Y}(A) = \rho(A)$ for $A \subseteq Y$.
- The **contraction** of M by X is the matroid $M/X = (\rho_{/X}, E - X)$, where $\rho_{/X}(A) = \rho(A \cup X) - \rho(X)$ for $A \subseteq E - X$.
- A **minor** of M is the matroid $M|Y/X$.

LRC in LCF terms

We can rewrite the parameters of a $(n, k, d, r, \delta)-$LRC using the lattice of cyclic flats $\mathcal{Z}$ of the associated matroid.

- $n = |1_{\mathcal{Z}}|$
- $k = \rho(1_{\mathcal{Z}})$
- $d = \eta(1_{\mathcal{Z}}) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) \text{ and } Z \neq 1_{\mathcal{Z}}\}$
- repair sets are cyclic flats.

Uniform matroid

The **uniform matroid** $U_n^k = (\rho, [n]), \rho(X) = \min\{|X|, k\}$ for $X \subseteq [n]$.

Proposition

A linear code C is MDS if and only if M_c is the uniform matroid U_n^k.

Proposition

$$M \cong U_n^k \iff \mathcal{Z}(M) = \{\emptyset, E\}.$$

Theorem (Geelen, Gerards and Whittle, 2014. Conjectured by Rota in 1970)

For any finite field $\mathbb{F}$, there is a finite set $L(\mathbb{F})$ of matroids such that any matroid M is $\mathbb{F}$-representable if and only if it contains no element from $L(\mathbb{F})$ as a minor.

For example,

- $L(\mathbb{F}_2) = U_4^2$.
- $L(\mathbb{F}_3) = U_5^2, U_5^3, F_7$ and F_7^*.
- The list $L(\mathbb{F}_4)$ has seven elements.

Minors via cyclic flats

Minor obtained by contracting and restricting over two cyclic flats.

Proposition

Let $X, Y \in \mathcal{Z}(M)$ with $X \subseteq Y$. Then

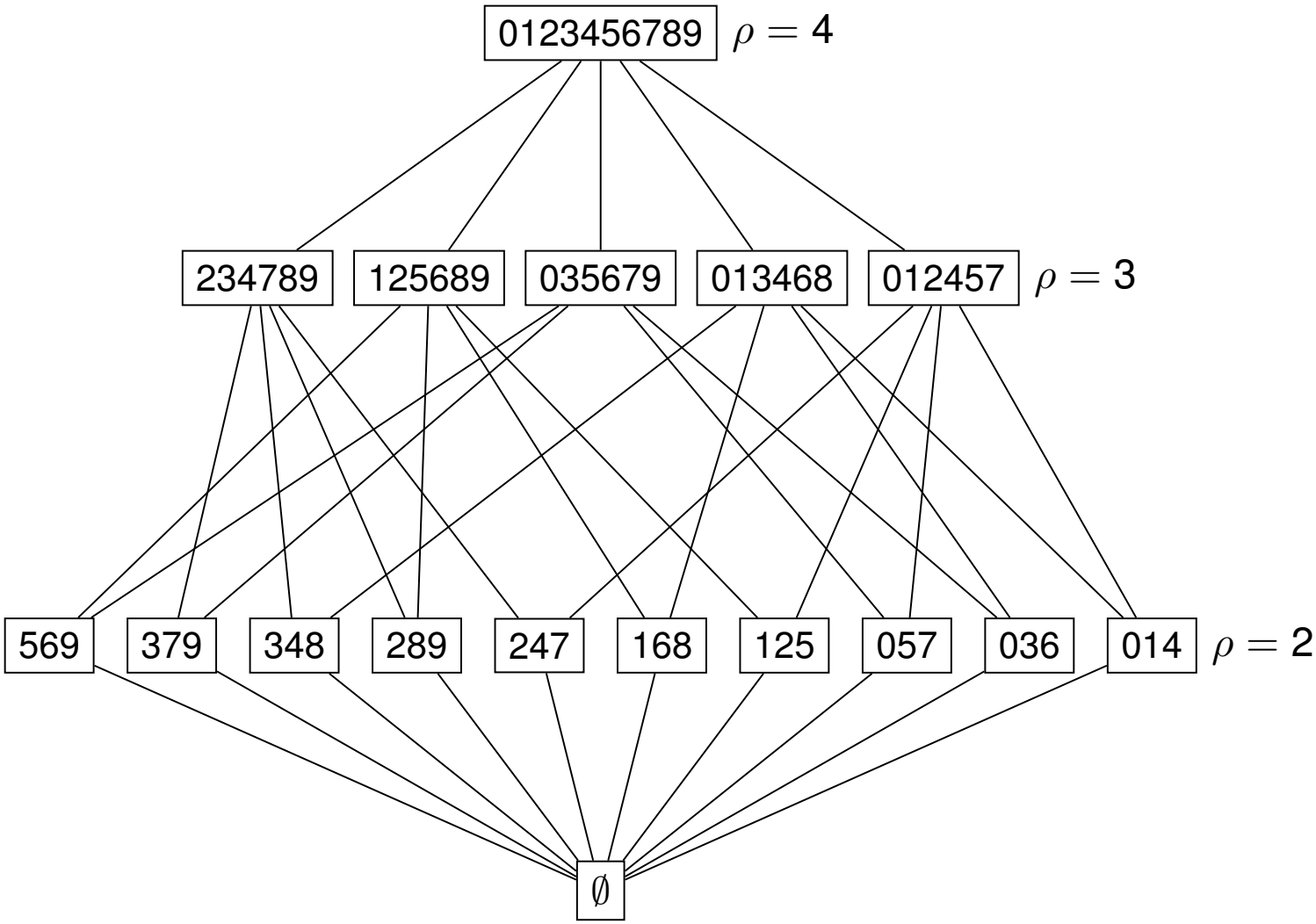
$$\mathcal{Z}(M|Y/X) = \{Z - X : X \subseteq Z \subseteq Y, Z \in \mathcal{Z}(M)\}$$

Arbitrary minor.

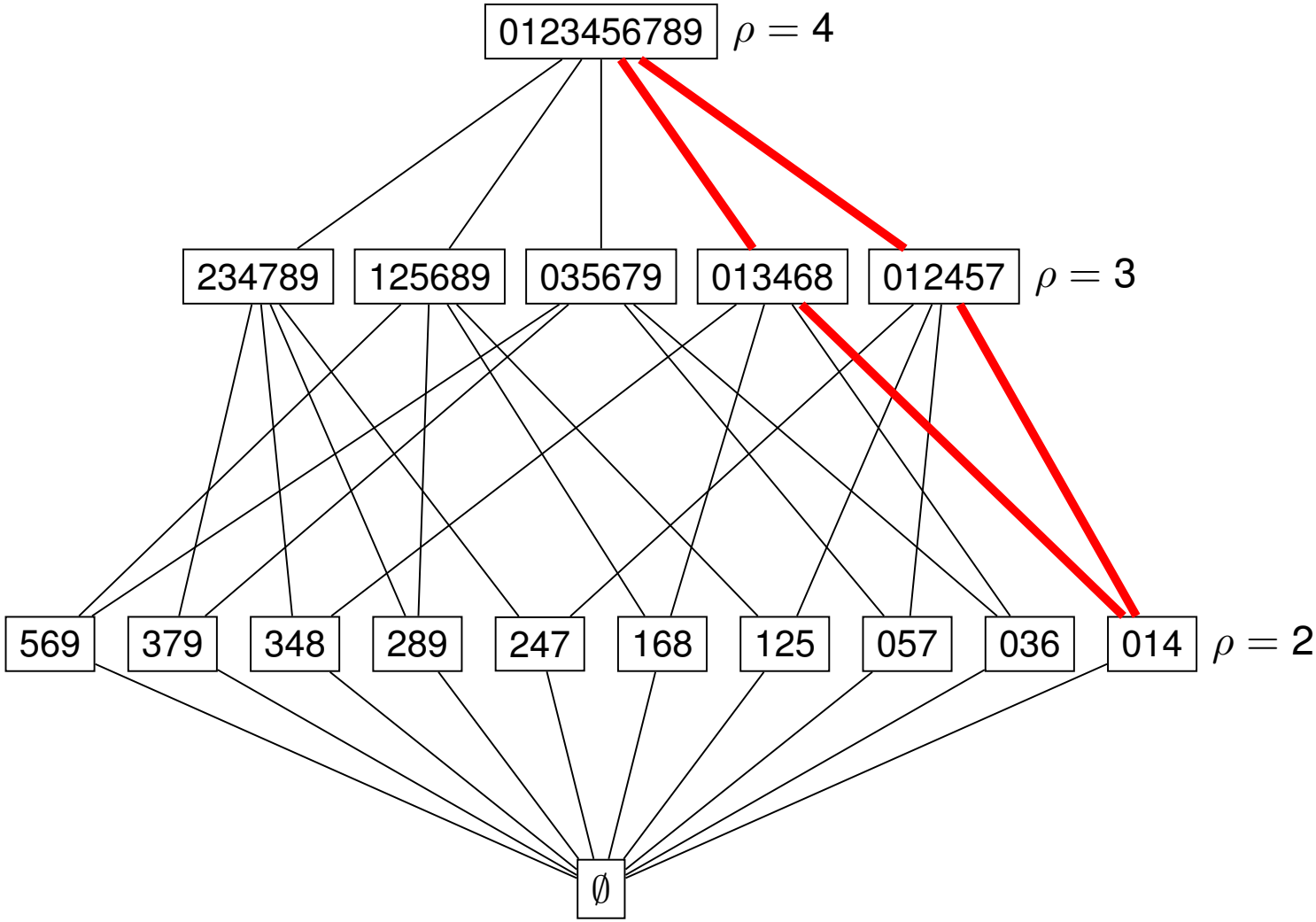
Theorem (G., Freij-Hollanti, Westerbäck, Hollanti)

Let $X \subseteq Y \subseteq E$. Then

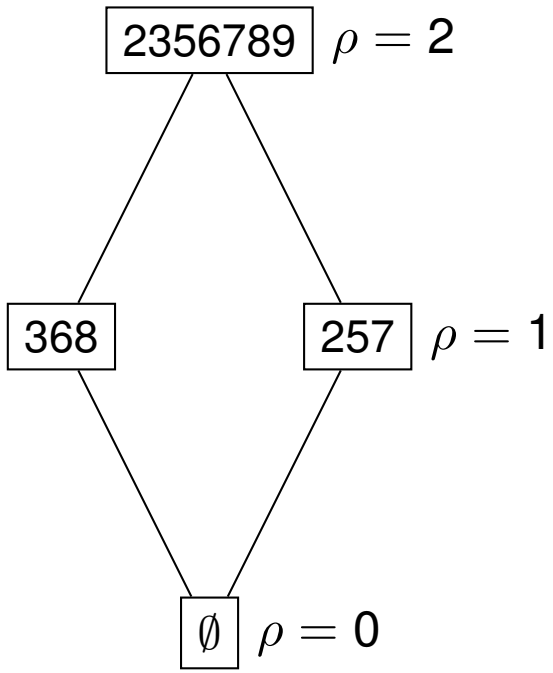
$$\mathcal{Z}(M|Y/X) = \left\{\mathbf{cl}(X \cup \mathbf{cyc}(Z \cap Y)) \cap (Y - X) : Z \in \mathcal{Z}(M)\right\}$$


0123456789
$\rho = 4$
234789
125689
035679
013468
012457
$\rho = 3$
569
379
348
289
247
168
125
057
036
014
$\rho = 2$
$\emptyset$

$M_G/\{0,1,4\}$


0123456789
$\rho = 4$
234789
125689
035679
013468
012457
$\rho = 3$
569
379
348
289
247
168
125
057
036
014
$\rho = 2$
∅

The lattice of cyclic flats of $M/\{0,1,4\}$.



Uniform minors

Theorem (G., Freij-Hollanti, Westerbäck, Hollanti)

Let $X, Y \in \mathcal{Z}(M)$ with $X \lessdot Y$. Let $n = |Y| - |X|$ and $k = \rho(Y) - \rho(X)$. Then

$$M|Y/X \cong U_n^k$$

Corollary

Let M be a matroid that contains no U_n^k minors. Then, for every edge $X \lessdot Y$ in the Hasse diagram of $\mathcal{Z}(M)$, we have

$$\rho(Y) - \rho(X) < k \quad \text{or} \quad \eta(Y) - \eta(X) < n - k$$

Proposition

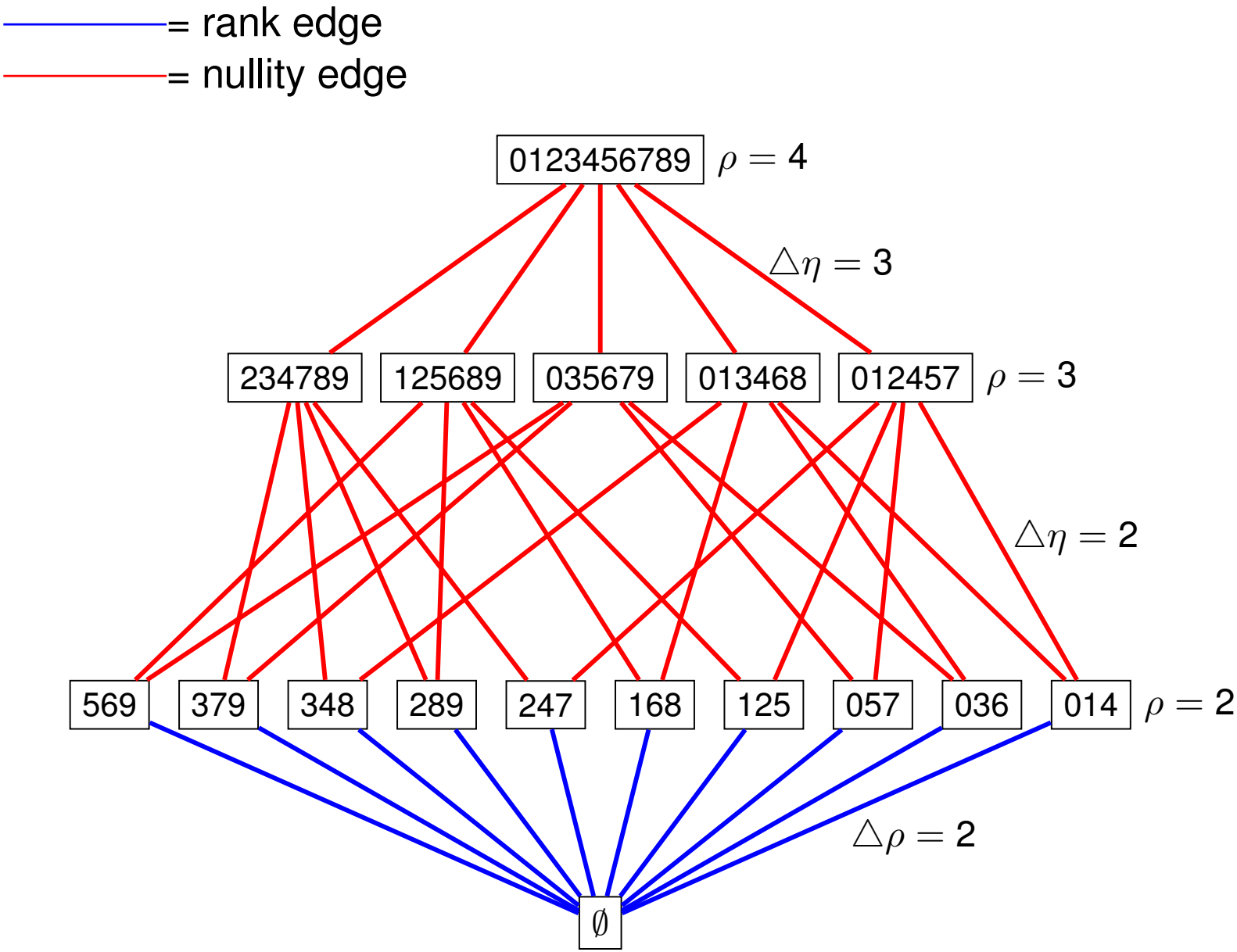
Let M be a matroid that contains no U_4^2 minors. Then, for $X \lessdot Y$, we have,

$$\rho(Y) - \rho(X) = 1 \quad \text{or} \quad \eta(Y) - \eta(X) = 1$$

Theorem (G., Freij-Hollanti, Westerbäck, Hollanti)

Let C be a non-degenerate binary (n, k, d, r, δ)-LRC with $\delta > 2$. Then $\mathcal{Z}(M_C)$ satisfies the following:

1. *$\emptyset$ and $[n]$ are cyclic flats.*
2. *Every covering relation $Z \lessdot [n]$ is a nullity edge with number $\geq d - 1$.*
3. *For every $i \in [n]$, there is $R \in \mathcal{Z}$ with $i \in R$ such that*
   1. *Every covering relation $Y \lessdot R$ is a nullity edge with number $\geq \delta - 1$*
   2. *Every cyclic flat Y with $Y \lessdot R$ has size $\leq r - 1$.*


= rank edge
= nullity edge
0123456789
$\rho = 4$
$\triangle\eta = 3$
234789
125689
035679
013468
012457
$\rho = 3$
$\triangle\eta = 2$
569
379
348
289
247
168
125
057
036
014
$\rho = 2$
$\triangle\rho = 2$
$\emptyset$

LRCs

Matroids

LRCs over $\mathbb{F}$

Avoid specific minors

Thank you

$\rightarrow$ Conditions on (n, k, d, r, δ) ?

Conditions on $\mathcal{Z}(M)$