Locally Repairable Codes with Availability and Hierarchy: Matroid Theory via Examples

Ragnar Freij-Hollanti
Department of Communications and Networking
P.O.Box 13000, FI-00076 AALTO, Finland
Email: ragnar.freij@aalto.fi

Thomas Westerbäck and Camilla Hollanti
Department of Mathematics and Systems Analysis
P.O.Box 11100, FI-00076 AALTO, Finland
Emails: {firstname.lastname}@aalto.fi

Abstract—Recent research on distributed storage systems (DSSs) has revealed interesting connections between matroid theory and locally repairable codes (LRCs). The goal of this paper is to illustrate these as well as some new — rather technical in nature — results via simple examples. The examples embed all the essential features of LRCs, namely locality, availability, and hierarchy alongside with related generalized Singleton bounds.

I. INTRODUCTION

The need for large-scale data storage is continuously increasing. Within the past few years, distributed storage systems (DSSs) have revolutionized our traditional ways of storing, securing, and accessing data. Storage node failure is a frequent obstacle in large-scale DSSs, making repair efficiency an important objective. A bottleneck for repair efficiency, measured by the notion of locality [1], is the number of contacted nodes needed for repair. The key objects of study in this paper are locally repairable codes (LRCs), which are, informally speaking, storage systems where a small number of failing nodes can be recovered by boundedly many other (close-by) nodes. Repair-efficient LRCs are already in use for large-scale DSSs used by, for example, Facebook and Windows Azure Storage [2].

Another desired attribute, measured by the notion of availability [3], is the property of having multiple alternative ways to repair a node. This is particularly relevant for nodes containing so-called hot data that is frequently and simultaneously accessed by many users. Moreover, as failures are often spatially correlated, it is valuable to have each node repairable at several different scales. This means that if a node fails simultaneously with the set of nodes that should normally be used for repairing it, then there still exists a larger set of helper nodes that can be used to recover the lost data. This property is captured by the notion of hierarchy [4], [5] in the storage system.

In this paper, we consider the hierarchical availability of linear LRCs. Our main mathematical tools for analyzing linear LRCs come from matroid theory. A matroid is an abstract structure in algebraic combinatorics. Matroids have been successfully used to solve problems in many areas in mathematics and computer science [6], [7], [8], [9], [10].

This work was partially supported by the Academy of Finland grants #276031, #282938, #283262. The support from the European Science Foundation under the COST Action IC1104 is also gratefully acknowledged.

a) Related Work: Network coding techniques for large-scale DSSs were considered in [11]. Since then, a plethora of research on DSSs with a focus on linear LRCs and various localities has been carried out, see [12], [1], [13], [14], [15] among many others. Availability for linear LRCs was defined in [3]. The notion of hierarchical locality was first studied in [4], where bounds for the global minimum distance were also obtained.

Let us denote by \((n,k,d,r,\delta,t)\), respectively, the code length, dimension, global minimum distance, locality, local minimum distance, and availability. Bold-faced parameters \((n,k,d,r,\delta)\) for linear LRCs were generalized to matroids, and new results for both matroids and linear LRCs were given therein. Even more generally, the parameters \((n,k,d,r,\delta,\ell)\) for linear LRCs were generalized to polymatroids, and new results on the parameters \((n,k,d,r,\delta,\ell)\) for matroids and nonlinear LRCs were derived in [16].

b) Contributions and Notation: The main purpose of this paper is to give an overview of the connection between matroid theory and linear LRCs with availability and hierarchy via examples. In particular, we are focusing on how the parameters \((n,k,d,t)\) of a LRC can be analyzed using the lattice of cyclic flats of an associated matroid, and on a construction derived from matroid theory that provides us with linear LRCs. The results reviewed here were mostly derived in [17], [16]. In addition, we provide a glance at our recently submitted work [5]. The following notation will be used throughout the paper:

\begin{align*}
\mathbb{F} & : \text{ a field; } \\
\mathbb{F}_q & : \text{ the finite field of prime power size } q; \\
E & : \text{ a finite set; } \\
G & : \text{ a matrix over } \mathbb{F} \text{ with columns indexed by } E; \\
G(X) & : \text{ the matrix obtained from } G \text{ by the columns indexed by } X, \text{ where } X \subseteq E; \\
C(G) & : \text{ the vector space generated by the columns of } G; \\
R(G) & : \text{ the vector space generated by the rows of } G; \\
C & : \text{ linear code } C = R(G) \text{ over } \mathbb{F} \text{ generated by } G; \\
CX & : \text{ the punctured code of } C \text{ on } X, \text{ i.e., } \\
CX = R(G(X)), \text{ where } X \subseteq E; \\
2^S & : \text{ the collection of all subsets of a finite set } S; \\
[j] & : \text{ the set } \{1, 2, \ldots, j\} \text{ for an integer } j.
\end{align*}
The motivation to study punctured codes arises from hierarchy; the locality parameters at the different hierarchy levels correspond to the global parameters of the related punctured codes. This further leads to so-called restricted matroids.

We also point out that $G(E) = G$ and $C_E = C$. We will often index a matrix $G$ by $[n]$, where $n$ is the number of columns in $G$.

**Example 1.1:** Let $E = [7]$ and $C$ the linear code generated by the matrix $G$ over $F_2$, with columns indexed by $[7]$. Then, for $X = \{5, 6, 7\}$, we have $C_X = \{(000), (110), (101), (011)\}$ with the generator matrix $G(X)$.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \]

\[ G(X) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \]

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

Then, $C$ corresponds to a 9 node storage system, storing four files $(a, b, c, d)$, each of which is an element in an alphabet on which $F_3$ acts freely. In this system, node 1 stores $a$, node 2 stores $b$, node 9 stores $a + 2b + 2d$, and so on.

Two very basic properties of any DSS are that every node can be repaired by some other nodes and that every node contains some information. We therefore give the following definition.

**Definition 2.1:** A linear $[n, k, d]$-code $C$ over a field is a non-degenerate storage code if $d \geq 2$ and there is no zero column in a generator matrix $X$.

**b) Linear LRCs with Hierarchical Availability:** The very broad class of linear LRCs with $h$-hierarchical availability will be defined next.

**Definition 2.2:** Let $G$ be a matrix over $F$ indexed by $E$ and $C$ the linear code generated by $G$. Then, for $X \subseteq E$, $C_X$ is a linear $[n_X, k_X, d_X]$-code where

\[ n_X = |X|, \]
\[ k_X = \text{rank}(G(X)), \]
\[ d_X = \min\{|Y| : Y \subseteq X \text{ and } k_{X \setminus Y} < k_X\}. \]

**Example 2.2:** Consider the storage code $C$ from Example 2.1. Let $Y_1 = \{1, 2, 3, 5, 6, 7\}$, $X_1 = \{1, 2, 5\}$ and $X_2 = \{2, 6, 7\}$. Then $C_{Y_1}$, $C_{X_1}$ and $C_{X_2}$ are storage codes with

\[ n_{Y_1}, k_{Y_1}, d_{Y_1} = [6, 3, 3], \]
\[ n_{X_1}, k_{X_1}, d_{X_1} = [3, 2, 2], \]
\[ n_{X_2}, k_{X_2}, d_{X_2} = [3, 2, 2]. \]

The parameter $d_X$ is the minimum (Hamming) distance of $C_X$. We say that $C$ is an $[n, k, d]$-code with $[n, k, d] = [n_E, k_E, d_E]$.

**Definition 2.3:** Let $h \geq 1$ be an integer, and let

\[ (n, k, d, t) = [(n_1, k_1, d_1, t_1), \ldots, (n_h, k_h, d_h, t_h)] \]

be a $h$-tuple of integer 4-tuples, where $k_i \geq 1$, $n_i, d_i \geq 2$, and $t_i \geq 1$ for $1 \leq i \leq h$. Then, a coordinate $x$ of a linear $[n, k, d] = [n_0, k_0, d_0]$-LRC $C$ indexed by $E$ has $h$-level hierarchical availability $(n, k, d, t)$ if there are $t_i$ coordinate sets $X_1, \ldots, X_{t_i} \subseteq E$ such that

\[ (i) \ x \in X_i \text{ for } i \in [t_1], \]
\[ (ii) \ i, j \in [t_1], i \neq j \Rightarrow X_i \cap X_j = \{x\}, \]
\[ (iii) \ n_{X_i} \leq n_1, \ k_{X_i} = k_1 \text{ and } d_{X_i} \geq d_1 \text{ for the punctured } [n_{X_i}, k_{X_i}, d_{X_i}]\text{-code } C_{X_i} \text{, for } i \in [t_1], \]
\[ (iv) \text{ for } i \in [t_1], x \text{ has } (h - 1)\text{-level hierarchical availability } [(n_2, k_2, d_2, t_2), \ldots, (n_h, k_h, d_h, t_h)] \text{ in } C_{X_i}. \]

The code $C$ above as well as all the related subcodes $C_{X_i}$ should be non-degenerate. For consistency of the definition, we say that any symbol in a non-degenerate storage code has 0-level hierarchical availability.

**Example 2.3:** Let $C$ be the code generated by the matrix $G$ in Example 2.1 and $x = 2$. Then $x$ has 2-level hierarchical availability

\[ (n, k, d, t) = [(6, 3, 3, 1), (3, 2, 2, 2)]. \]

This follows from Example 2.2 where $C_{Y_1}$ implies the $(6, 3, 3, 1)$-availability, and the $(3, 2, 2, 2)$-availability is implied by $C_{X_1}$ and $C_{X_2}$.

**Definition 2.4:** A subset $X \subseteq E$ has $h$-level hierarchical availability $(n, k, d, t)$ in $C$, if every $x \in X$ has $h$-level hierarchical availability $(r, a, d, t)$ in $C$.

An information set of a linear $[n, k, d]$-code $C$ is defined as a set $X \subseteq E$ such that $k_X = |X| = k$. Hence, $X$ is an information set of $C$ if and only if there is a generator matrix $G$ of $C$ such that $G(X)$ equals the identity matrix, i.e., $C$ is systematic in the coordinate positions indexed by $X$ when generated by $G$. In terms of storage systems, this means that the nodes in $X$ together store all the information of the DSS.

**Example 2.4:** Two information sets of the linear code $C$ generated by $G$ in Example 1.1 are $\{1, 2, 3, 4\}$ and $\{1, 2, 6, 7\}$. 

International Zurich Seminar on Communications (IZS), March 2 – 4, 2016
III. MATROIDS AND LINEAR CODES

In this section we give some basics about matroids and their connection to linear codes. For more information on matroids we refer the reader to [18].

a) Matroid Fundamentals: Matroids were introduced by Whitney in 1935 [19] in order to capture fundamental properties of independence common to various areas of mathematics.

Definition 3.1: A (finite) matroid $M = (I, E)$ is a finite set $E$ and a collection of subsets $I \subseteq 2^E$ such that

(I.1) $\emptyset \in I$,
(I.2) $Y \in I, X \subseteq Y \Rightarrow X \in I$,
(I.3) For all pairs $X, Y \in I$ with $|X| < |Y|$, there exists $y \in Y \setminus X$ such that $X \cup \{y\} \in I$.

The subsets in $I$ are the independent sets of the matroid.

Any matroid $G$ is associated with a matroid $M[G] = (I, E)$, where the columns of $G$ are indexed by $E$ and a subset $X$ of $E$ is independent if and only if the column vectors indexed by $X$ in $G$ are linearly independent.

Example 3.1: Let $G$ be the matrix given in Example 2.1. Then, when $M[G] = (I, [9])$, we have

$$\{3, 4, 6\}, \{1, 2, 3, 8\}, \{2, 3, 4, 6\} \in I,$$

and $\{1, 2, 3, 7\} \notin I$.

A matroid $M$ is linear if there exists a matrix $G$ such that $M = M[G]$. If a matroid $M$ can be represented by a matrix over a specific field $F$, then $M$ is $F$-linear.

Example 3.2: The matroid that arises from the matrix $G$ in Example 2.1 is linear. In particular, it is $F$-linear for any field $F$ with characteristic $\neq 2$, ensuring that $2 \neq 0$ in $F$.

The $F$-linearity of a matroid may depend on the field $F$. Further, many matroids are not linear over any field, and it is strongly believed (but not proven) that this is true for asymptotically almost all matroids.

An alternative, but equivalent definition of a matroid is the following.

Definition 3.2: A (finite) matroid $M = (\rho, E)$ is a finite set $E$ together with a function $\rho : 2^E \to \mathbb{Z}$ such that for all subsets $X, Y \subseteq E$

(R.1) $0 \leq \rho(X) \leq |X|$,  
(R.2) $X \subseteq Y \Rightarrow \rho(Y) \leq \rho(Y)$,  
(R.3) $\rho(X) + \rho(Y) \geq \rho(X \cup Y) + \rho(X \cap Y)$.

The rank function $\rho$ and the independents sets $I$ of a matroid on a ground set $E$ are linked as follows: For $X \subseteq E$,

$$\rho(X) = \max\{|Y| : Y \subseteq X \text{ and } Y \in I\},$$

and $X \in I$ if and only if $\rho(X) = |X|$.

For a linear matroid $M[G] = (\rho, E)$, the rank $\rho(X)$ equals the rank of $G(X)$ over the ground field $F$.

Example 3.3: Let $G$ be the matrix given in Example 1.1. Then, $\rho(3, 4, 6) = 3$, $\rho(3, 4, 5) = 2$ and $\rho(7) = 4$ for the linear matroid $M[G] = (\rho, [7])$.

The restriction of $M = (\rho, E)$ to a subset $X$ of $E$ is the matroid $M|X = (\rho|_X, X)$, where

$$\rho|_X(Y) = \rho(Y), \text{ for } Y \subseteq X.$$


For any linear matroid $M[G] = (\rho, E)$ and subset $X \subseteq E$, the restriction of $M[G]$ to $X$ equals the linear matroid on $G(X)$, i.e.,

$$M[G]|X = M[G(X)].$$

An important property of $M[G]|X$ is that

$$M[G]|X = M[G_X]$$

for every matrix $G_X$ whose row space equals the row space of $G(X)$.

Example 3.4: Let $G$ be the matrix given in Example 1.1. Then, for $X = \{5, 6, 7\}$, $M[G]|X = M[G_X]$ where

$$G_X = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$
b) Linear Matroids and Codes: There is a straightforward connection between linear codes and matroids. Indeed, let \( C \) be a linear code generated by a matrix \( G \). Then \( C \) is associated with the matroid \( M[G] = (\rho, E) \). As two different generator matrices of \( C \) have the same row space, they will generate the same matroid. Therefore, without any inconsistency, we denote the associated linear matroid of \( C \) by \( M_C = (\rho_C, E) \). In general, there are many different codes \( C \neq C' \) with the same matroid structure \( M_C = M_{C'} \).

A property of linear codes that depends only on the matroid structure of the code is called matroid invariant. For example, the collection of information sets and the parameters \([n, k, d] \) of a code are matroid invariant properties.

In addition to the parameters \([n, k, d] \) of a linear code \( C \), we are also interested in the length, rank and minimum distance of the punctured codes, since these correspond to the locality parameters at the different hierarchy levels. A punctured code can be analyzed using matroid restrictions, since \( M_{C[X]} = M_C |X \) for every coordinate subset \( X \). Thus, the parameters \([n, k, d, |X|] \) of \( C_X \) are also matroid invariant properties for \( C \).

**Proposition 3.1**: Let \( C \) be a linear \([n, k, d] \)-code and \( X \subseteq E \). Then for \( M_C = (\rho_C, E) \).

(i) \( n_X = |X| \),
(ii) \( k_X = \rho_C(X) \),
(iii) \( d_X = \min\{|Y| : Y \subseteq X, \rho_C(X \setminus Y) < \rho_C(X)\} \),
(iv) \( X \) is an information set of \( M_C \) if and only if \( \rho(X) = |X| = k \).

**Example 3.6**: Let \( C \) denote the \([n, k, d] \)-code generated by the matrix \( G \) given in Example 2.1. Then \([n, k, d] = [9, 4, 3] \), where the value of \( d \) arises from the fact that \( \rho_G([9] \setminus \{i, j\}) = 4 \) for \( i, j = 1, 2, \ldots, 7 \), and \( \rho_G([9] \setminus \{4, 8, 9\}) = 3 \). Two information sets of \( C \) are \([1, 2, 3, 4] \) and \([1, 2, 6, 8] \).

Not every property of a linear code is matroid invariant, an important counter-example being the covering radius [20].

**IV. CYCLIC FLATS AND LINEAR \([n, k, d, t] \)-LRCs**

Our main matroid theoretical tool in this paper for analyzing linear LRCs is the lattice of cyclic flats, together with the rank function restricted to this lattice.

a) The Lattice of Cyclic Flats: A collection of sets \( P \subseteq 2^E \) ordered by inclusion defines a poset \((P, \subseteq) \). Let \( X \) and \( Y \) denote two elements of \( P \). The elements \( X \) and \( Y \) have a join if there is an element \( Z \in P \), denoted by \( X \lor Y \), such that \( X \subseteq Z, Y \subseteq Z \), and if \( W \in P, X \subseteq W, Y \subseteq W \), then \( Z \subseteq W \).

Dually, the elements \( X \) and \( Y \) have a meet if there is an element \( Z \in P \), denoted by \( X \land Y \), such that \( Z \subseteq X, Z \subseteq Y \), and if \( W \in P, W \subseteq X, W \subseteq Y \), then \( W \subseteq Z \).

The poset \((P, \subseteq) \) is a lattice if every pair of elements in \( P \) has a join and a meet. The bottom and top elements of a finite lattice \((P, \subseteq) \) always exist, and are denoted by \( \bot_P = \bigwedge_{X \in P} X \) and \( \top_P = \bigvee_{X \in P} X \), respectively.

Now, recall that for a matroid \( M = (\rho, E) \) and \( X \subseteq E \), the collection of cyclic flats of \( M \) is denoted by \( Z(M) \), and consists of all \( X \subseteq E \) such that \( \rho(X \setminus \{x\}) = \rho(X) \) for all \( x \in X \) and \( \rho(X \cup \{y\}) > \rho(X) \) for all \( y \in E \setminus X \). Two basic properties of the cyclic flats of a matroid are given in the following proposition.

**Proposition 4.1 (21)**: Let \( M = (\rho, E) \) be a matroid and \( Z \) the collection of cyclic flats of \( M \). Then,

(i) \( \rho(X) = \min\{|F| : F \in Z, X \subseteq F\} \), for \( X \subseteq E \),
(ii) \( (Z, \subseteq) \) is a lattice, \( X \lor Y = \text{cl}(X \cup Y) \) and \( X \land Y = \text{cyc}(X \cap Y) \) for \( X, Y \in Z \).

**Proposition 4.1 (i)** shows that a matroid is uniquely determined by its cyclic flats and their ranks.

**Example 4.1**: Let \( M_C = (\rho_C, E) \) be the matroid associated to the linear code \( C \) generated by the matrix \( G \) given in Example 2.2. The lattice of cyclic flats \((Z, \subseteq) \) of \( M_C \) is given in the figure below, where the cyclic flat and its rank are given at each node.

In [21], Theorem 3.2 gives an axiom scheme for matroids via cyclic flats and their ranks. This gives a compact way to construct matroids with prescribed local parameters, which we have exploited in [17].

b) Properties of Linear LRCs via the Lattice of Cyclic Flats: The results given in this section can be found in [17], [5].

For a linear \([n, k, d] \)-code \( C \) with \( M_C = (\rho_C, E) \) and \( Z = Z(M_C) \), and for a coordinate \( x \), we have

(i) \( d \geq 2 \iff 1_x = E \),
(ii) \( C(x) \neq \{0_x\} \) for every \( x \in E \).

Hence, by Definition 2.1, the following propositions are straightforward.

**Proposition 4.2**: Let \( C \) be a linear \([n, k, d] \)-code and \( Z \) denote the collection of cyclic flats of the matroid \( M_C = (\rho_C, E) \). Then \( C \) is a non-degenerate storage code if and only if \( 0_x = \emptyset \) and \( 1_x = E \).

**Proposition 4.3**: Let \( C \) be a non-degenerate storage code and \( M_C = (\rho_C, E) \). Then, for \( X \subseteq E \), \( C_X \) is a non-degenerate storage code if and only if \( X \) is a cyclic set of \( M_C \).
If $X$ is a cyclic flat of a matroid $M$, then $Z(M|X) = \{F \in Z(M) : F \subseteq X\}$. Therefore, studying the parameters $(n, k, d, t)$ of the punctured codes $C_{X,1}$ amounts to studying the order ideals $\{F \in Z(M) : F \subseteq X\}$ in the lattice of cyclic flats $Z(M)$. 

c) Constructions of Linear $(n, k, d, t)$-LRCs: In [17], a construction of a broad class of linear LRCs is given via matroid theory and especially the lattice of cyclic flats. Further, results on nonlinear 1-level linear LRCs was examined in [17], and $F$-LRCs was examined in [17].

Moreover, results on nonlinear 1-level linear LRCs and other objects related to linear LRCs are not as well studied as of yet. However, some results on nonlinear 1-level linear LRCs are given in [16].

In addition, looking at cyclic sets $X'$ within a cyclic flat $X$ can give us repair groups with $n'_{X'} \leq n_X, r'_{X'} = r_X, d'_{X'} = d_X$. This will be of use when looking at information set locality instead of all-symbol locality.

of matroids, in particular polymatroids, are used to derive corresponding results for matroids and linear LRCs. The most general Singleton bound in the regime $t \neq 1$, $h = 1$, with all-symbol locality and information-symbol availability is 

$$d_1 \leq n - k + 1 - \left( \frac{t_1(k - 1) + 1}{t_1(t_1 - 1) + 1} \right) (d_1 - 1),$$

also given in [16].

As a natural next step, the notions of hierarchy and availability should be studied further from the matroid theoretic perspective, and the related level-specific generalized Singleton bounds should follow. Moreover, adoptions of our methods to account for field size should be studied.

References


