A Matroid Framework for Noncoherent Random Network Communications

Maximilien Gadouleau and Alban Goupil
CReSTIC, Université de Reims Champagne-Ardenne
Reims, France
E-mails:\{maximilien.gadouleau, alban.goupil\}@univ-reims.fr

Abstract

In this paper, we model different types of random network communications as the transmission of flats of matroids. This novel framework generalizes the models recently proposed for random linear network coding and store and forward. Using this framework, we first evaluate and compare the performance of different network protocols in the error-free case. We define and determine the rate, average delay, and throughput of such protocols, and we also investigate the possibilities of partial decoding before the entire message is received. Our matroid viewpoint also allows us to determine the true rate and combination power of random linear network coding. Second, we model the possible alterations of a message by the network as an operator channel, which generalizes the channels proposed for random linear network coding and store and forward. Error control is thus reduced to a coding theoretic problem on flats of a matroid. We also determine two distinct metrics between flats for error correction. We then introduce the notion of matroid codes and constant-rank matroid codes, and investigate the construction of constant-rank matroid codes via liftings. We prove that the previously proposed lifting operations are optimal for random linear network coding, while not necessarily optimal for store and forward. Third, we introduce a novel type of network coding, referred to as random affine network coding, based on affine combinations of packets. This technique offers the same combination power as random linear network coding while increasing the data rate thanks to a better embedding of messages into packets. We finally study the maximum cardinality of matroid codes for error correction in random affine network coding, and design a class of nearly optimal codes based on rank metric codes for which we propose a low-complexity decoding algorithm.
I. INTRODUCTION

During transmission through a network, the data are usually modified—either deliberately, as in network coding, or by the network constraints—without affecting their decoding. However, other modifications, such as packets in error or lost, corrupt the nature of the transmitted message. Recently, operator channels have been proposed to differentiate these two types of modifications for data transmission using random linear network coding (RLNC) [1] and store and forward (SAF) [2], respectively. For RLNC, it is shown that data transmission is equivalent to the communication of a linear subspace of a given vector space [1]; for SAF, however, a subset of a set is transmitted [2]. Using a bijection between subsets and binary vectors, data transmission using SAF is also modeled as a binary channel in [2]; however, we will only consider the subset approach henceforth. Using these operator channels, noncoherent error correction in RLNC and SAF can be reduced to coding theoretic problems on linear subspaces and subsets, respectively.

In this paper, we generalize the models described above by viewing random data transmission through a network as the communication of a flat of a matroid. Matroids [3] can be viewed as the combinatorial essence of independence, and hence are a generalization of linear independence; flats of a matroid can be viewed as generalizations of linear subspaces. Studying matroids allows to focus on the combinatorial aspects of independence and combinations, without assuming any underlying algebraic structure. First of all, we determine the matroids associated to RLNC and SAF. Then, using our matroid framework, we determine, evaluate, and compare the performances of different network protocols. We first define the data rate of a matroid as the ratio between the amount of information carried by the flat, i.e. the logarithm of the number of flats, over the size of the transmitted message through the network. We also investigate the average delay of a matroid, which reduces to the coupon collector problem for SAF. Combining these two parameters, we also define the throughput of a matroid as the proportion of useful information received by the destination. We then study the delay in more detail via the average number of independent packets in a given number of received packets. We hence demonstrate that this number tends to the optimum for RLNC when the field size increases, while the number of independent packets in SAF follows an exponential growth. We finally investigate the possibilities of partial decoding. We prove that partial decoding is highly unlikely in RLNC, while for SAF all packets are decodable. Therefore, RLNC follows a zero-one pattern: no packets can be decoded before receiving the total number of packets in a message, and once this amount is received, the whole message can be decoded. On the other hand, SAF follows an exponential growth in terms of partially decodable packets.

The study described above considers an error-free transmission through the network. In the presence
of errors, message alterations (packets lost, injected, or in error) correspond to modifications of the transmitted flat. The network can hence be viewed as an operator channel, which generalizes the channels defined in [1] and [2] for RLNC and SAF, respectively. We then introduce two metrics for error correction in random network communications. These metrics, referred to as the lattice metric and the modified lattice metric, respectively, are identified with previously proposed metrics for RLNC [4] and SAF [2]. We also place constant-weight codes [2] and constant-dimension codes [1] into the new framework of constant-rank matroid codes, which are codes on flats of a matroid sharing the same rank. An interesting construction of codes is via the lifting operation, defined as an isometry from an alphabet to the set of all flats of a given rank. We then show that a lifting of maximal cardinality always exists, and that the lifting introduced in [5] for RLNC is optimal. However, we prove that the lifting defined in [2] for SAF is not optimal, which confirms the result in [2] that liftings of Hamming metric codes are not optimal constant-weight codes.

Matroids have already been used in coding theory or network coding in [6]–[10]. We would like to emphasize how our work differs from the works in [6]–[8], [9], and [10]. In [7], [8], matroids are associated to linear binary codes, and using these matroids, properties such as the MacWilliams identity can be determined (see [6] for an expanded introduction on this approach). In [9], matroids associated to codes are applied to the problem of linear-programming decoding. However, our work first considers a matroid, and then studies codes on elements of that matroid. In [10], matroids are used to design networks on which network coding satisfies some interesting properties, and are hence unrelated to the network protocol. In our work, however, the matroid is independent of the network, but instead depends on the network protocol, whether it is RLNC, SAF, or another.

The advantages of our matroid framework are listed below.

- First, this framework is very general, and offers a unified approach for distinct problems such as SAF and RLNC. It offers to focus on the combinatorial properties of network protocols, in terms of both combinations and encoding. Also, associating a protocol to a matroid provides with a new tool to study and compare the performances of different protocols.

- Second, different properties of a protocol arising from matroid theory can be discovered. For example, we demonstrate how RLNC can be viewed as a matroid on only a fraction of all possible packets, and we hence determine its true combination power. The lattice distance also illustrates the easiest way to alter a message, hence highlighting the sensibility of network coding to errors.

- Third, the advantages of using an operator channel still apply to our general framework. Although the matroid depends on the protocol, it is independent of the actual network, rendering our approach...
noncoherent and robust to network topology changes. Moreover, errors on the message level, such as packets lost or injected, and errors on the packet level (bits or symbol errors) can be detected and corrected using the same class of codes. The problem of error control can be eventually tackled using methods from algebraic coding, such as binary constant-weight codes or rank metric codes.

- Fourth, our model offers a wealth of alternatives to the protocols already proposed in the literature, as many different types of matroids have been previously discovered and studied. One of these alternatives is detailed below.

We introduce a new way to combine packets for network coding, referred to as random affine network coding (RANC), where packets are viewed as points instead of vectors and new packets are created via affine combinations of the old ones. The associated matroid is the affine geometry and the flats are thus affine subspaces of an affine space. Unlike RLNC which only considers a fraction of all packets, RANC works on all possible packets, thus offering a higher rate, the same average delay, and hence a throughput increase. Moreover, using RANC does not result in any significant raise in computational complexity at the source, the intermediate nodes, or the destination. We then investigate error control for RANC with codes on affine subspaces. We derive bounds on the maximum cardinality of such codes and determine a nearly optimal class of codes based on liftings of rank metric codes. We finally design a decoding algorithm for these codes based on, and with the same order of complexity as the decoder proposed in [1] for RLNC. The rate gain of affine network coding is therefore preserved when error correction is considered, and at no cost in terms of complexity.

The rest of the paper is organized as follows. Section II reviews some necessary backgrounds on matroids and error correction models for RLNC and SAF. In Section III we introduce the model based on matroids for error-free communications. In Section IV we evaluate and compare the different performance parameters of matroids. In Section V we model the alterations of the message into an operator channel, and study the metrics used for error correction in random network communications. Section VI introduces and investigates random affine network coding. Finally, Section VII details possible extensions of our work.

II. PRELIMINARIES

A. Matroids

We review below the definition and major properties of matroids and their flats. Although the concepts introduced below arise from matroid theory, they can all be viewed as generalizations of well-known concepts in linear algebra. For an extensive account on matroid theory, the interested reader is referred
to [3]. For any set $E$, we denote the set of subsets of $E$ with cardinality $0 \leq i \leq |E|$ as $\mathcal{P}(E, i)$ and its power set as $\mathcal{P}(E) = \bigcup_{i=0}^{|E|} \mathcal{P}(E, i)$. A matroid is a pair $\mathcal{M} = (E, \mathcal{I})$, where $E$ and $\mathcal{I} \subseteq \mathcal{P}(E)$ are referred to as the ground set and the independent sets of $\mathcal{M}$, respectively. The independent sets can be viewed as generalizations of linearly independent vectors and satisfy the following axioms:

- $\emptyset \in \mathcal{I}$,
- if $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$,
- if $I_1, I_2 \in \mathcal{I}$ with $|I_1| > |I_2|$, then there exists $e \in I_1 \setminus I_2$ such that $I_2 \cup \{e\} \in \mathcal{I}$.

The third axiom, referred to as the independence augmentation axiom, is crucial as it guarantees that any family of independent elements can be extended to form a basis (a maximal family of independent elements). Clearly, all bases have the same cardinality. To any matroid is associated a rank function $\text{rk}(A)$ for all $A \in \mathcal{P}(E)$, defined as the maximum number of independent elements in $A$. For any two subsets $A, B \subseteq E$, we have the submodular inequality

$$ \text{rk}(A \cup B) + \text{rk}(A \cap B) \leq \text{rk}(A) + \text{rk}(B). \quad (1) $$

The rank of a matroid is simply the rank of its ground set, and is the number of elements in any basis. The closure $\text{cl}(A)$ of a subset $A$ of the ground set is then defined as the maximal subset of $E$ containing $A$ and satisfying $\text{rk}(\text{cl}(A)) = \text{rk}(A)$. The closure can be viewed as a generalization of the span of a set of vectors and the rank can be viewed as a generalization of the dimension of the linear subspace spanned by a set of vectors.

A flat is a set equal to its closure, and hence it can be viewed as a generalization of the concept of linear subspace. In particular, we refer to any flat of rank $r - 1$ in a matroid of rank $r$ as a hyperplane. By extension, we refer to any family of $k$ independent elements in a flat of rank $k$ as a basis of that flat. The set of flats of a matroid is closed under intersection. Furthermore, the set of flats ordered by inclusion forms a lattice, where the meet of two flats is their intersection, and their join is the closure of their union. Amongst the many interesting properties of such a lattice, we remark that for any flats $a$ and $b$ such that $\text{rk}(a) \geq \text{rk}(b)$ and any flat $f_0$ in the interval $[a, b] = \{f : a \subseteq f \subseteq b\}$, there exists a flat $f_1$, referred to as a complement of $f_0$ in $[a, b]$, such that $\text{cl}(f_0 \cup f_1) = b$ and $f_0 \cap f_1 = a$ (note that a complement is not necessarily unique). For any pair of flats $b$ and $f \subseteq b$, we denote a complement of $f$ in $[\text{cl}(\emptyset), b]$ as $C(b, f)$, which hence satisfies $f \cap C(b, f) = \text{cl}(\emptyset)$ and $\text{cl}(f \cup C(b, f)) = b$.

A matroid may contain loops and parallel elements. A loop $l$ is an element of the ground set belonging to no independent set: $\{l\} \notin \mathcal{I}$; alternatively, $l$ belongs to the closure of the empty set. A collection of elements are said to be parallel if they are pairwise dependent: $\{e_i, e_j\} \notin \mathcal{I}$ for $i \neq j$; they hence all
belong to a set with rank 1. A matroid is said to be \textit{simple} if it does not contain any loops or parallel elements. For any matroid $\mathcal{M}$, the simple matroid obtained by removing all loops and keeping only one element in each set of parallel elements of $\mathcal{M}$ has the same lattice of flats as $\mathcal{M}$.

We now review some important classes of matroids.

- \textbf{Vector matroid}. $\mathcal{M}(A)$ has as ground set the rows of a matrix $A$ and independent sets are all sets of linearly independent rows. The closure of a set of rows $R$ consists of all the rows of $A$ in the linear subspace spanned by $R$.

- \textbf{Projective geometry}. If the rows of $A$ are all the non-zero vectors of $GF(q)^r$ with leading nonzero coefficient equal to 1, then the vector matroid $\mathcal{M}(A)$ is isomorphic to the projective geometry $PG(r-1,q)$. This matroid is simple, has rank $r$ and its flats are in one-to-one correspondence with the linear subspaces of $GF(q)^r$. Therefore, the number of flats of rank $k$ is given by the Gaussian binomial $\left[ \binom{r}{k} \right] = \frac{q^r - 1}{q^k - 1} \prod_{k=0}^{\infty} \left( 1 - q^{-k} \right) < q^{r-k}$ for all $0 \leq k \leq r$, where $K_q = \prod_{k=1}^{\infty} (1 - q^{-k}) < 1$ tends to 1 when $q$ tends to infinity \cite{11}.

- \textbf{Affine geometry}. Removing a hyperplane from the projective geometry $PG(r-1,q)$ yields the affine geometry $AG(r-1,q)$. This matroid is also simple with rank $r$ and its flats are the affine subspaces of $GF(q)^{r-1}$; there are $q^{r-k}\left[ \binom{r-1}{k-1} \right]$ flats of rank $k$ for all $0 \leq k \leq r$. Any affine subspace with rank $k$ can be represented by a linear subspace with dimension $k-1$ and a point belonging to a complementary linear subspace. By definition, $AG(r-1,q)$ is a submatroid of $PG(r-1,q)$, and can be viewed as a matroid on the points in $GF(q)^{r-1}$, where two points $a, b$ are affinely independent if and only if the vectors $(1, a), (1, b) \in GF(q)^r$ are linearly independent. The affine geometry can hence be viewed as the vector matroid $\mathcal{M}(B)$, where the first column of $B \in GF(q)^{r-1 \times r}$ is the all-one vector and the other part of the matrix is given by all the vectors of $GF(q)^{r-1}$.

- \textbf{Free matroid}. The free matroid on $r$ elements, classically denoted as $U_{r,r}$, has $[r] = \{0, 1, \ldots, r-1\}$ as a ground set, and any subset of $[r]$ is independent. Clearly, this matroid is simple, has rank $r$, and any subset of $[r]$ is a flat. The free matroid $U_{r,r}$ is isomorphic to the vector matroid $\mathcal{M}(I_r)$, where $I_r$ is the identity matrix of order $r$ over any field.

B. Error control for RLNC and SAF

We now review the existing models for error correction in RLNC and SAF given in \cite{1} and \cite{2}, respectively. For RLNC, several techniques have been proposed for error correction (see \cite{12}, \cite{13} for coherent error correction); however, we are interested here in the operator channel approach introduced in \cite{1} for noncoherent error control. Suppose a message, encoded into $k$ linearly independent packets
in $\mathbb{GF}(q)^n$, is transmitted through a network using RLNC. Since the linear combinations operated by
the intermediate nodes do not modify the subspace spanned by the packets, RLNC is viewed as the
transmission of a linear subspace of dimension $k$ of $\mathbb{GF}(q)^n$. The alterations of the message (packets
lost, injected, or in error) hence correspond to modifications of that subspace. The transmission of a
message using RLNC is hence modeled as an operator channel which modifies the input subspace sent
by the source into the output subspace received by the destination. Accordingly, codes on subspaces, and
more especially codes on a Grassmannian referred to as constant-dimension codes, have been proposed for
error correction in RLNC. Two metrics between subspaces have been proposed: the subspace metric and
the injection metric [4]. The maximum cardinality of a constant-dimension code, consisting of subspaces
of $\mathbb{GF}(q)^n$ with dimension $k$, with minimum injection distance $d$ (and equivalently, minimum subspace
distance $2d$) is between $q^{\min\{k(n-k-d+1),(n-k)(k-d+1)\}}$ and $K_q^{-1}q^{\min\{k(n-k-d+1),(n-k)(k-d+1)\}}$. These
bounds were tightened in [14]–[16].

A general construction of constant-dimension codes, referred to as liftings of rank metric codes, has
been proposed in [5]. Rank metric codes [17]–[19] are codes on matrices in $\mathbb{GF}(q)^{k\times \nu}$, where the rank
distance between two matrices is simply the rank of their difference. The number of matrices with
rank $r$ in $\mathbb{GF}(q)^{k\times \nu}$ is given by $\binom{k}{r}\prod_{i=0}^{r-1}(q^\nu - q^i)$ [18]. The maximum cardinality of a rank metric
code in $\mathbb{GF}(q)^{k\times \nu}$ with minimum rank distance $d$ is given by $q^{\min\{k(n-k-d+1),(n-k)(k-d+1)\}}$ and is achieved
by Gabidulin codes [18], an analogue of Reed-Solomon codes. For any $M \in \mathbb{GF}(q)^{k\times \nu}$, the linear
lifting $I_L(M)$ of $M$ is the row space of the matrix $(I_k|M)$, a subspace of $\mathbb{GF}(q)^{k+\nu}$ with dimension $k$ [5]. The injection distance between two liftings of matrices is equal to the rank distance between the
matrices, hence the lifting of a rank metric code has the same minimum injection distance as the original
code. In particular, liftings of Gabidulin codes are nearly optimal constant-dimension codes for which
low-complexity decoding algorithms were proposed [1], [5].

Similarly, an operator channel has been proposed for error correction in SAF in [2]. Suppose $k$ packets
in $\mathbb{GF}(q)^n$ are transmitted through a network with SAF. Also, assume the packets arrive at the destination
in a different order to which they were sent in. Then only the set of packets is preserved, and SAF is
modeled as the transmission of a subset of cardinality $k$ of $[q^n]$. Codes on subsets have hence been
proposed for error control in SAF with two distinct metrics: the Hamming metric and the modified
Hamming metric. Since subsets of $[q^n]$ are in bijection with vectors in $\mathbb{GF}(2)^{q^n}$, codes on subsets can
be viewed as binary codes; in particular, codes on subsets with the same cardinality can be viewed as
binary constant-weight codes. A construction of constant-weight codes with length $q^n$ and weight $q^l$
is the lifting of a nonrestricted Hamming metric code in $\mathbb{GF}(q^{n-l})^{q^l}$. The lifting $I_S(X)$ of any word

March 10, 2010 DRAFT
$X = (X_0, X_1, \ldots, X_{q^l-1}) \in [q^{n-l}][q^l]$ is given by the subset $\{x_0, x_1, \ldots, x_{q^l-1}\} \in \mathcal{P}([q^n], q^l)$, where $x_i = iq^{n-l} + X_i$ for $0 \leq i \leq q^l - 1$. This construction corresponds to adding the header $i$ (expanded in basis $q$) in front of each packet, which is its position in the original message. The lifting $I_S$ preserves the Hamming distance: $d_H(I_S(X), I_S(Y)) = 2d_H(X, Y)$, and liftings of nonrestricted Hamming metric codes can be used for error control with SAF.

III. TRANSMISSION MODEL

A. Model and discussion

In this section, we introduce a novel communication model for error-free data transmission through a network. We consider a source wishing to transmit a message $M$ in the alphabet $[A] = \{0, 1, \ldots, A - 1\}$ of size $A$ through a network toward a destination. Let $(E, I)$ be a simple matroid with set of flats $\mathcal{F}$, and assume that both the source and the destination know a common injective map $G$ from $[A]$ to $\mathcal{F}$.

The error-free data transmission follows three steps.

- Step I: at the source. The source encodes the original message $M$ into a flat $f = G(M) \in \mathcal{F}$. Then a stream of elements of $f$ containing a basis of $f$ is transmitted into the network.
- Step II: in the network. Each intermediate node combines the elements it has received by selecting and retransmitting elements of their closure.
- Step III: at the destination. The destination waits until it receives a basis of $f$, and then recovers the original message by determining $M = G^{-1}(f)$.

We now provide several remarks regarding the matroids and the flats used in our model.

1) We consider flats of a matroid, for the matroid structure ensures that the rank function is well-behaved. Indeed, a flat of rank $k$ can only be described by $k$ independent elements, no less and no more. Also, the independence augmentation axiom reviewed in Section II-A guarantees that any set of less than $k$ independent elements can be extended into a basis of $k$ elements of the flat.

2) A non-simple matroid contains loops and parallel elements. By definition, a loop belongs to every flat and hence does not carry any information about the transmitted flat. Also, two parallel elements belong to the same flats and are combined in the same way, hence they carry the same information. Therefore, loops and parallel elements are unnecessary to the destination, and our assumption of considering simple matroids only does not lead to any loss of generality.

3) Although flats of any rank may be sent, sending flats of the same rank is more suitable in practice for two reasons. First, this ensures that no transmitted flat is properly contained by another, thus
rendering the decoding non-ambiguous. Second, the destination always expects the same number of independent elements to start decoding, hence simplifying the decoding process. Henceforth, we consider that the source sends flats in the set \( \mathcal{F}_k \) of all flats of rank \( k \), and we denote \( N_k = |\mathcal{F}_k| \) for all \( k \). For any simple matroid, \( \mathcal{F}_0 = \{\emptyset\} \), \( N_0 = 1 \) and \( \mathcal{F}_1 = \mathcal{P}(E, 1) \), \( N_1 = |E| \).

4) Not all flats of the same rank necessarily have the same cardinality and the same number of bases, which results in different combination powers, and hence different protections to packet losses. However, as shown below, SAF and RLNC use matroids for which all flats of the same rank have equal cardinalities. Matroids satisfying this property are referred to as perfect matroid designs \cite{20}, \cite[3.4]{6}. Due to their highly specific structure, very few classes of perfect matroid designs are known so far. When considering a perfect matroid design, we shall denote the cardinality of any flat of rank \( k \) as \( C_k \) henceforth, where \( C_0 = 0 \) and \( C_1 = 1 \) for any simple perfect matroid design.

We also comment on the validity of our model and on some practical issues regarding its realization. Our model is general and does not take advantage of any knowledge of the network topology. It is hence noncoherent, and is robust to network topology variations, such as node or link appearance/disappearance. Accordingly, the intermediate nodes are assumed to operate blindly on the elements they receive, regardless of the source, the destination, or the actual transmitted data. We also remark that our model can be generalized to the case of multiple destinations or multiple sources as well.

In terms of practical implementation, all intermediate nodes should have an efficient algorithm to combine elements. This algorithm, however, does not guarantee to yield a new basis of the flat. This operation can be viewed as a form of random sampling on the elements of a flat. Also, the destination needs an efficient algorithm to retrieve the original message from any basis of the flat. This can be performed by determining a basis \( B(f) \) for any flat \( f \), referred to as the canonical basis, which is directly related to the message. The decoding problem is thus reduced to obtaining the canonical basis given another basis of the same flat.

**B. Matroids for SAF and RLNC**

We now determine the matroids associated to SAF and RLNC. We assume that encoded messages of \( k \) packets of length \( n \) over \( \text{GF}(q) \) are transmitted.

First, for SAF, the only combination possible is the selection of an element, hence the flats are the subsets of cardinality \( k \) of \( [q]^n \). The associated matroid is the free matroid \( U_{q^n,q^n} \) and the rank of the transmitted flat is \( k \). Therefore, we have \( E = [q^n] \), \( \mathcal{F}_k = \mathcal{P}(E, k) \) for all \( 0 \leq k \leq q^n \), and hence \( N_k = \binom{q^n}{k} \) and \( C_k = k \). We remark that each flat has only one basis, which is necessarily the canonical
basis. In order to use notations reflecting the protocol and the alphabet and length of packets, we denote $U_{q^n,q^n}$ as $S(q,n)$ or simply $S$ when there is no ambiguity.

Second, our model differs slightly from the purely random linear combinations typically proposed for RLNC. Indeed, a linear combination may yield the all-zero vector or collinear vectors: these are respectively loops and parallel elements. However, according to Remark 2), our model considers the simple matroid associated to RLNC. Therefore, the corresponding matroid is the projective geometry $PG(n-1,q)$, and hence $N_k = \binom{n}{k}$ and $C_k = \binom{k}{1}$. The ground set $E$ is the set of one-dimensional subspaces of GF($q$)$^n$, and $F_k$ is a Grassmannian for $0 \leq k \leq n$. We remark that a canonical basis $B(f)$ is given by the unique matrix in row-reduced echelon form whose rows span the flat $f$. Clearly, the combinations operated by the intermediate nodes are linear combinations which ensure the output vector is non-zero and has leading non-zero coefficient equal to 1. Also, determining the canonical basis is achieved via Gaussian elimination. We denote $PG(n-1,q)$ as $L(q,n)$ or simply $L$ when there is no ambiguity henceforth.

IV. PARAMETERS FOR ERROR-FREE NETWORKS

In this section, we define, determine, and compare some performance parameters of different matroids, hence leading to a performance comparison of different network protocols. Without loss of generality, we assume that any element of the flat is carried by one packet. Since our model is noncoherent as noted in Section III-A we assume that the intermediate nodes choose a random combination independently and according to a uniform distribution in order to guarantee the highest combination power. Accordingly, we suppose that the destination receives elements chosen independently and uniformly amongst all elements of the flat. Although this assumption seems unlikely in practice, we believe it provides a good intuition on how the protocols behave. This simple assumption also allows for the thorough performance study below. The parameters we introduce illustrate the impact of the combination power of different protocols in terms of data rate, delay, and partial decoding.

Steps I and III of the model introduced in Section III-A can be regarded as an extension of fountain coding to the case of matroids with a certain probability distribution. In this model, the distribution is effectively produced by the combinations operated in Step II by the intermediate nodes. However, efficient probability distributions are usually considered in fountain coding, as they offer more desirable properties such as low decoding complexity. The performance analysis developed below for the uniform distribution can be adapted to those distributions as well.

We comment on the term “error-free” used in the title of this section. Although the destination does
not necessarily recover the whole transmitted flat immediately, it keeps receiving elements of the flat and hence it will necessarily be able to reconstruct the whole flat. The term error-free indicates that no other flat of the same rank can be reconstructed by the destination, and hence only the message sent by the source can be decoded.

A. Matroid rate

The data rate of the communication is given by the ratio between the amount of information decoded over the amount of data needed to transmit a flat: \( \frac{\log_q A}{nk} = R_{\text{code}}(A, \mathcal{M})R(\mathcal{M}, k) \), where \( R_{\text{code}}(A, \mathcal{M}) = \frac{\log_q A}{\log_q N_k} \) can be viewed as the rate of the code formed by all the possible transmitted flats and the \textit{matroid rate} is defined as

\[
R(\mathcal{M}, k) = \frac{\log_q N_k}{nk}. \tag{2}
\]

We remark that \( R_{\text{code}}(A, \mathcal{M}) \) only depends on the encoding of the message into a flat, and does not depend on the actual matroid (we only require \( N_k \geq A \)). Therefore, we only focus on the matroid rate henceforth, which indicates how efficiently a flat of rank \( k \) is embedded into a message of \( k \) packets.

We can further decompose the matroid rate into \( R(\mathcal{M}, k) = \frac{\log_q N_k}{k \log_q |E|} \cdot \frac{\log_q |E|}{n} \), where the first ratio is an intrinsic property of the matroid, while the second ratio indicates how efficiently a matroid element is embedded into a packet. Note that the rate is entirely determined by the lattice of flats of \( \mathcal{M} \), and does not depend on the cardinalities of flats. Proposition 1 below determines the matroid rates of SAF and RLNC.

\textit{Proposition 1 (Matroid rate of SAF and RLNC):} The matroid rates of SAF and RLNC are respectively given by

\[
R(S, k) = \frac{\log_q \left(\begin{array}{c} q^n \\ k \end{array}\right)}{nk} \geq 1 - \frac{\log_q k}{n}, \tag{3}
\]

\[
R(L, k) = \frac{\log_q \left[\begin{array}{c} n \\ k \end{array}\right]}{nk} < 1 - \frac{k + \log_q K_q}{n}. \tag{4}
\]

\textit{Proof:} For SAF, the rate is determined by (2), \( k = m \), and \( N_k = \left(\begin{array}{c} q^n \\ k \end{array}\right) \). Since \( \left(\begin{array}{c} q^n \\ k \end{array}\right) \geq \left(\begin{array}{c} q^n \\ \frac{q^n}{k} \end{array}\right)^k \), we obtain the lower bound in (3). For RLNC, the rate is determined by (2), \( k = m \), and \( N_k = \left[\begin{array}{c} n \\ k \end{array}\right] \). Since \( \left[\begin{array}{c} n \\ k \end{array}\right] < K_q^{-1} q^{k(n-k)} \), we obtain the lower bound in (4).

Proposition 1 indicates that the rate of RLNC decreases linearly with the number of packets, while the rate of SAF only decreases with the logarithm of the number of packets. Therefore, RLNC is only suitable for a small number of packets, while SAF is more suitable for a large number of packets. This confirms the assumption in [2] of studying SAF for large numbers of packets.
B. Average delay and throughput

According to the assumptions made in the introduction of Section IV, the packets arrive at the destination at random. Therefore, the number of packets to be received in order to obtain \( k \) independent packets, referred to as the delay of a transmission, is a random variable. Clearly, the minimum delay is exactly \( k \), while the maximum delay is unbounded. We hence define the average delay of a transmission as the expected number of packets received in order to obtain \( k \) independent packets. Clearly, \( D(\mathcal{M}, k) \geq k \) for any matroid \( \mathcal{M} \). The value of \( D(\mathcal{M}, k) \) is determined in Proposition 2 below for perfect matroid designs as a function of the cardinalities of the flats of \( \mathcal{M} \) by generalizing the approach typically used to solve the coupon collector problem [21].

Proposition 2 (Average delay): For a perfect matroid design where all flats of rank \( k \) have cardinality \( C_k \) for all \( k \), the average number of packets required to obtain \( k \) independent packets is given by

\[
D(\mathcal{M}, k) = \sum_{i=1}^{k} \frac{C_k}{C_k - C_{i-1}}.
\]

Proof: Let \( X_i \) be the number of packets needed to receive the \( i \)th independent packet, given that \( i-1 \) independent packets have already been received. Then \( X_i \) is a random variable whose distribution is geometric with success parameter \( p_i = \frac{C_k-C_{i-1}}{C_k} \). The mean value of \( X_i \) is \( E(X_i) = p_i^{-1} \). If \( X \) is the number of packets needed to receive in order to obtain \( k \) linearly independent packets, then

\[
E(X) = \sum_{i=1}^{k} E(X_i) = \sum_{i=1}^{k} p_i^{-1}.
\]

We now determine the value of the average delay for SAF and RLNC.

Corollary 1 (Average delay of SAF and RLNC): First, the average delay of SAF is given by the coupon collector problem: \( D(S, k) = k \sum_{i=1}^{k} i^{-1} > k(\log k + \gamma) \), where \( \gamma \) is Euler’s constant. Second, for RLNC, we have \( D(L, k) = k + \sum_{j=1}^{k-1} \frac{1-q^{j-k}}{q^{j-1}} < k + \alpha_q \), where \( \alpha_q = \sum_{j=1}^{\infty} \frac{1}{q^{j-1}} \).

The constant \( \alpha_q \) is related to the \( q \)-analogue of Riemann’s zeta function [22] by \( \alpha_q = \frac{q}{q-1} \zeta_q^{-1} \), and satisfies \( \alpha_q < \frac{q}{(q-1)^2} \). Therefore, in RLNC, the expected number of packets needed to obtain in order to decode the subspace completely is between the dimension of the subspace and the dimension plus a constant which tends to 0 as \( q \) tends to infinity.

We now define the throughput of a matroid as the ratio between the amount of transmitted information over the amount of data received on average by the destination. In other words, it measures the proportion of useful information received by the destination. By definition, the throughput is given by

\[
T(\mathcal{M}, k) = \frac{\log_q N_k}{nD(\mathcal{M}, k)} = kR(\mathcal{M}, k)D(\mathcal{M}, k),
\]

(5)
By (5), this quantity is proportional to the ratio between the matroid rate and the average delay. Combining the results in Proposition 1 and Corollary 1, the throughputs of SAF and RLNC are respectively around

\[ T(S, k) \sim \frac{1}{\log k} - \frac{1}{n \log q}, \]  

(6)

\[ T(L, k) \sim 1 - \frac{k}{n}. \]  

(7)

The \( \sim \) sign refers to an approximation which holds for large values of one or several parameters. By (6) and (7), the throughput of RLNC is higher for small values of \( k \), but decreases linearly with \( k \). On the other hand, the throughput of SAF only decreases with the logarithm of \( k \), hence this protocol is more appropriate for messages with a large number of packets.

The relation between the throughput and the rate and average delay in (5) provides an indication on the desirable properties of a matroid for network communications. By (5), a matroid should maintain a low average delay, while trying to maximize its data rate. By Proposition 2, minimizing the average delay is equivalent to minimizing the ratio \( \frac{C_l}{C_k} \); therefore, the cardinality of flats must increase rapidly with their rank. Also, by definition the matroid rate directly depends the number of flats \( N_k \). A matroid should hence have a large number of flats, whose cardinalities increase rapidly with their ranks.

C. Number of received independent packets

We now investigate the delay in higher detail by considering the random variable \( X_I(M, k; r) \) given by the number of informative packets received by the destination once \( r \) packets have been received. Therefore, \( \Pr\{X_I(M, k; r) = l\} \) is equal to the probability \( P_I(M, k; r, l) \) to obtain \( l \) independent packets once \( r \) packets have been received. An important special case is given by the probability \( P_I(M, k; k, k) \) to receive all the necessary independent packets to reconstruct the flat with minimum delay. Proposition 3 below determines a recursive way of computing \( P_I(M, k; r, l) \).

**Proposition 3 (Probability of independence):** We have \( P_I(M, k; r, 0) = 0 \) and for \( r \geq 0 \),

\[ P_I(M, k; r + 1, l + 1) = \left( 1 - \frac{C_l}{C_k} \right) P_I(M, k; r, l) + \frac{C_{l+1}}{C_k} P_I(M, k; r, l + 1). \]  

(8)

In particular,

\[ P_I(M, k; k, k) = \prod_{i=1}^{k-1} \left( 1 - \frac{C_i}{C_k} \right). \]  

(9)

**Proof:** In order to obtain \( l + 1 \) independent packets after receiving \( r + 1 \) packets, one must have received either \( l \) or \( l + 1 \) independent packets in the first \( r \) received packets. Hence \( P_I(M, k; r + 1, l + 1) = p_0 P_I(M, k; r, l) + p_1 P_I(M, k; r, l + 1) \), where \( p_0 \) is the probability to receive a packet outside of a flat.
of rank \( l \) and \( p_1 \) is the probability to receive a packet inside of a flat of rank \( l+1 \). It is easily shown that 
\[ p_0 = \frac{C_{l-1}}{C_l} \] and 
\[ p_1 = \frac{C_{l+1}}{C_l} , \] and hence we obtain (8). Applying (8) successively for \( l = r \) yields (9).

We derive closed-form formulas of the probability of independence for SAF and RLNC in Corollary 2 below.

**Corollary 2 (Probability of independence for SAF and RLNC):** For SAF, we have for all \( l \)
\[ P_I(S, k; r, l) = \frac{k!}{k^r(l-k)!} r \left\{ \binom{r}{l} \right\} = \frac{(k)}{k^r} \sum_{j=0}^{l} (-1)^{l-j} \binom{l}{j} j^r , \] (10)
where \( \left\{ \binom{r}{l} \right\} \) is a Stirling number of the second kind [23]. In particular,
\[ P_I(S, k; k, k) = \frac{k!}{k^k} < \sqrt{2\pi k e^{-k+\frac{1}{12k}}} \] (11)
is the probability that all \( k \) distinct packets are received with minimum delay.

For RLNC, we have
\[ P_I(L, k; r, l) = \frac{\binom{k}{l}}{(q^k-1)^r \sum_{s=0}^{r-l} (-1)^s (r)} \sum_{i=0}^{l-1} (q^{r-s} - q^i) \] (12)
and in particular 
\[ P_I(L, k; k, k) = \prod_{i=1}^{k-1} (1 - \frac{q^{r-1}}{q^i-1}) > K_q. \]

**Proof:** For SAF, \( P_I(S, k; r, l) = \frac{S(r, l)}{k^r} \), where \( S(r, l) \) is the number of words of length \( r \) with \( l \) distinct symbols can be put in correspondence with the partition of \( [r] \) into \( l \) cells, where each cell contains the positions of a given symbol in the word. By definition of the Stirling numbers, there are \( \left\{ \binom{r}{l} \right\} \) such partitions. Also, once the partition is fixed, there are \( k(k-1) \cdots (k-l+1) \) choices for the symbols. Combining, we obtain (10). For \( r = l = k \), we obtain 
\[ P_I(S, k; k, k) = \frac{k!}{k^k} , \] which combined with \( k! \leq \sqrt{2\pi k e^{-k+\frac{1}{12k}}} \) [24] leads to (11).

For RLNC, we have 
\[ P_I(L, k; r, l) = \frac{R_I(r, l)}{k^r} \], where \( R_I(r, l) \) is the number of matrices in \( GF(q)^{k \times r} \) with rank \( l \) such that all the columns are nonzero and the leading nonzero coefficient is equal to 1. The number of matrices with rank \( l \) and \( s \) nonzero columns is hence given by 
\[ \binom{r}{l} (q-1)^s R_I(s, l) \]. Also, the number of matrices in \( GF(q)^{k \times r} \) with rank \( l \) is given by 
\[ \binom{k}{l} \prod_{i=0}^{l-1} (q^r - q^i) \]. Summing all matrices with rank \( l \) and \( s \) nonzero columns for \( l \leq s \leq r \), we obtain
\[ \sum_{s=l}^{r} \binom{r}{s} (q-1)^s R_I(s, l) = \binom{k}{l} \prod_{i=0}^{l-1} (q^r - q^i) \].
By applying the reverse binomial transform [25], we obtain (12).

We now investigate the moments of the probability distribution \( P_I(M, k; r, l) \), in particular the expectation \( E_I(M, k; r) \) and the variance \( V_I(M, k; r) \). We clearly have 
\[ E_I(M, k; r) \leq \min\{k, r\}, E_I(M, k; r) \leq \]
$E_I(\mathcal{M}, k; r + 1) \leq E_I(\mathcal{M}, k; r) + 1$, and $\lim_{r \to \infty} E_I(\mathcal{M}, k; r) = k$ and $\lim_{r \to \infty} V_I(\mathcal{M}, k; r) = 0$. Proposition 4 below determines the expectation and the variance for SAF.

**Proposition 4 (Average number of independent elements in SAF):** For all $k$ and $r$,

$$E_I(S, k; r) = k \left[1 - \left(1 - \frac{1}{k}\right)^r\right] \sim k(1 - e^{-\frac{r}{k}}). \quad (13)$$

Also, the variance is given by

$$V_I(S, k; r) = k \left[\left(1 - \frac{1}{k}\right)^r - \left(1 - \frac{2}{k}\right)^r\right] + k^2 \left[\left(1 - \frac{2}{k}\right)^r - \left(1 - \frac{1}{k}\right)^{2r}\right] \sim ke^{-\frac{r}{k}}(1 - e^{-\frac{r}{k}}). \quad (14)$$

**Proof:** Let $N_I(r, l)$ denote the number of words of length $r$ with $l$ distinct symbols, then $P_I(S, k; r, l) = k^{-r}N_I(r, l)$. Consider the bipartite graph on $[k]^r$ and $\mathcal{P}([k], a)$ ($1 \leq a \leq k$), where two vertices are adjacent if and only if there exist $a$ symbols of the word in $[k]^r$ equal to the $a$ elements in $[k]$. Let us count the number of edges in this graph in two different ways. First, there are $\binom{k}{a}$ edges adjacent to a word in $[k]^r$ with $l$ different coefficients, hence there are $\sum_{l=a}^{k} \binom{k}{a} N_I(r, l)$ edges in the graph. Second, by the inclusion-exclusion principle, we obtain that each subset of $[k]$ with cardinality $a$ appears in exactly $\sum_{i=0}^{a} (-1)^{i} \binom{a}{i} (k - i)^r$ words in $[k]^r$. Therefore,

$$\sum_{l=a}^{k} \binom{k}{a} N_I(r, l) = \binom{k}{a} \sum_{i=0}^{a} (-1)^{i} \binom{a}{i} (k - i)^r,$$

which yields (13) for $a = 1$. Using this identity for $a = 2$ and combining, we also obtain (14). \[\square\]

In particular, for $r = k$, (13) indicates that only around $1 - e^{-1} \approx 0.632$ of the first $k$ received packets are independent on average.

For RLNC, (12) indicates that $P_I(L, k; r, r) > K_q$ for all $r \leq k$. Therefore, $E_I(L, k; r) > K_q \min\{r, k\}$ for all $r$, and the average number of independent packets tends to the optimal with the field size. Accordingly, the variance $V_I(L, k; r)$ tends to 0 with the field size.

The expected number of independent elements for RLNC and SAF determined above is illustrated in Figure 1 for $k = 10$ and $1 \leq r \leq 30$. For SAF, the exponential pattern determined in Proposition 4 is clearly displayed. As proved above, RLNC is close to optimality, even for small values of $q$. In this case, the average delay is given by $D(S(q, n), 10) \approx 29.3$ for any $q$ and $n$ such that $q^n \geq 10$ while $D(L(2, n), 10) \approx 11.6$ and $D(L(4, n), 10) \approx 10.4$ for any $n \geq 10$.

**D. Partial decoding**

The model introduced in Section III and the parameters determined so far assume the destination waits to receive $k$ independent packets in order to begin the decoding procedure. However, the destination
may choose to operate partial decoding on a fraction of \( k \) independent packets. The problem of partial decoding is hence as follows: Suppose that less than \( k \) independent packets have been received, how many packets do we expect to decode? We remark that this problem is intrinsic to the matroid, and does not depend on the assumptions on the model made in the introduction of Section [IV].

Let \( P_D(\mathcal{M}, k; l, d) \) be the probability to decode \( d \) elements after receiving \( l \) independent elements. Provided a canonical basis exists for all flats, decoding \( d \) elements is equivalent to receiving a flat containing \( d \) members of the canonical basis \( B(f) \) of the transmitted flat \( f \in \mathcal{F} \). We determine \( P_D(\mathcal{M}, k; l, d) \) under certain assumptions on the matroid, which are satisfied by \( \mathcal{L} \) and \( \mathcal{S} \).

**Proposition 5 (Probability of partial decoding):** Suppose the transmitted flat of rank \( k \) contains \( G(l, k) \) flats of rank \( l \) for all \( 0 \leq l \leq k \). Furthermore, assume that for all \( a \leq l \leq k \), any flat with rank \( a \) is contained into \( F(a, l) \) flats of rank \( l \), all of them being contained in the transmitted flat. We then have

\[
P_D(\mathcal{M}, k; l, d) = \frac{\binom{k}{d}}{G(l, k)} \sum_{a=d}^{l} (-1)^{a+d} \left( \frac{k-d}{a-d} \right) F(a, l).
\] (15)

**Proof:** The probability \( P_D(\mathcal{M}, k; l, d) \) is given by \( P_D(\mathcal{M}, k; l, d) = \frac{N_D(l,d)}{G(l,k)} \), where \( N_D(l,d) \) is the number of flats of rank \( l \) with \( d \) decodable elements. We now determine the value of \( N_D(l,d) \).

First, the set of flats of rank \( l \) with \( l \) decodable elements is given by \( \{ \text{cl}(X) : |X| = l, X \subseteq B(f) \} \), and hence \( N_D(l,l) = \binom{k}{l} \). Now consider the bipartite graph on the set of subflats of \( f \) of rank \( l \) and the set of flats of rank \( a \) with \( a \) decodable elements \( (a \leq d \leq l) \), where two vertices \( f_l \in \mathcal{F}_l, f_a \in \mathcal{F}_a \)
are adjacent if and only if \( f_a \subseteq f_l \). We now count the edges in this graph in two ways. Since there are \( F(a,l) \) edges adjacent to any flat of rank \( a \), the number of edges is given by \( \binom{k}{a} F(a,l) \). Also, there are \( \binom{d}{a} \) edges adjacent to any flat of rank \( l \) with \( d \) decodable elements, hence there are \( \sum_{d=a}^{l} \binom{d}{a} N_D(l,d) \) edges. Combining, we obtain

\[
\sum_{d=a}^{l} \binom{d}{a} N_D(l,d) = \binom{k}{a} F(a,l). \tag{16}
\]

Denoting \( n = (N_D(l,a), N_D(l,a+1), \ldots, N_D(l,l)), v = (\binom{k}{a} F(a,l), \binom{k+1}{a+l} F(a+1,l), \ldots, \binom{k}{l} F(l,l)), \) (16) becomes \( nL = v \), where \( L = (l_{d,a}) \) is a Pascal matrix: \( l_{d,a} = \binom{d}{a} \) \([26]\). Since \( L^{-1} = (m_{a,d}) \) has \( m_{a,d} = (-1)^{d+a} \binom{a}{a} \), we obtain (15).

We remark that (16) provides the binomial moments of the \( P_D(M,k;l,d) \) distribution. In particular, the expectation \( E_D(M,k;l) \) and the variance \( V_D(M,k;l) \) are respectively given by

\[
E_D(M,k;l) = \frac{k F(1,l)}{G(l,k)}, \tag{17}
\]

\[
V_D(M,k;l) = \frac{k(k-1)F(2,l) + F(1,l)}{G(l,k)} - \frac{k^2 F(1,l)^2}{G(l,k)^2}. \tag{18}
\]

**Corollary 3 (Probability of partial decoding for SAF and RLNC):** For SAF, \( P_D(S,k;l,d) = \delta_{l-d} \) for all \( l,d \), and hence \( E_D(S,k;l) = l \) and \( V_D(S,k;l) = 0 \) for all \( l \). For RLNC, we have \( E_D(L,k;l) = k^{\frac{d-1}{q-1}} < kq^{l-k} \) for all \( l \).

**Proof:** For SAF, all elements are decodable and \( P_D(S,k;l,d) = \delta_{l-d} \) for all \( l,d \). This can also be demonstrated via Proposition 5, where \( F(a,l) = \binom{k-a}{l-a} \) and \( G(l,k) = \binom{k}{l} \). For RLNC, we have \( F(a,l) = \binom{k-a}{l-a} \) and \( G(l,k) = \binom{k}{l} \) by \([27]\) Lemma 2, and (17) leads to \( E_D(S,k;l) = k^{\frac{k-1}{q}} \).

Figure 2 displays \( E_D(S,k;l) \) and \( E_D(L,k;l) \) with \( q = 2 \) and \( q = 4 \) for \( k = 10 \). The exponential growth of the average number of decodable elements for RLNC is clearly illustrated. We remark that \( E_D(L,k;k-1) \sim kq^{-1} \) by Corollary 3; hence for \( q = 2^8 \) only 0.39\% of the packets can be decoded before receiving all the packets. Therefore, for practical values of the field size, RLNC hardly offers any opportunity of partial decoding.

Finally, let \( P_T(M,k;r,d) \) be the probability to decode \( d \) packets given that \( r \) packets (not necessarily independent) have been received. Clearly, we have

\[
P_T(M,k;r,d) = \sum_{l=0}^{r} P_I(M,k;r,l) P_D(M,k;l,d). \tag{19}
\]

By (19), we can regroup the results on \( P_I(M,k;r,l) \) and \( P_D(M,k;l,d) \) above and thus determine the probability \( P_T(M,k;r,d) \). For SAF, by Corollary 3 the expected number of decodable packets is given by \( E_T(S,k;r) = E_I(S,k;r) \sim k(1 - e^{-\frac{r}{n}}) \). For RLNC, we have \( E_T(L,k;r) \leq E_D(L,k;r) < kq^{r-k} \).
In particular, $E_T(\mathcal{L}, k; k - 1) < kq^{-1}$, hence only $q^{-1}$ of the packets can be partially decoded before receiving $k$ packets. RLNC then follows a zero-one behavior: before receiving $k$ packets, no decoding is possible; once $k$ packets are received, they are independent with high probability and the whole message can be decoded. This behavior is partly illustrated in Figure 3, where the values of $E_T(S, k; l)$ and $E_T(\mathcal{L}, k; l)$ for $q = 2$ and $q = 4$ are displayed for $k = 10$. The zero-one pattern of RLNC is not clearly depicted, as the values of $q$ are extremely small; for more practical values such as $q = 2^8$, the zero-one pattern would be very clear.

V. OPERATOR CHANNEL AND MATROID CODES

A. Operator channel and metrics for error correction

In Section III, we modeled data communication through a network as the transmission of a flat of a matroid. However, the model in Section III did not take into account the possible alterations undergone by the message during its transmission through the network. These alterations due to the network—packet losses, injections, errors, etc.—modify not only the packets but also the flat being transmitted. A flat $f \in \mathcal{F}_k$ can be modified in two ways: an erasure turns $f$ into a proper subflat of rank $k - 1$, while a disclosure turns $f$ into a proper superflat of rank $k + 1$. An erasure (a disclosure, respectively) is hence equivalent to moving one step down (up, respectively) the lattice of flats. Any flat $f$ can be turned into any other flat $g$ via a sequence of disclosures and erasures.
Proposition 6 below proves that the shortest way to modify one flat into another is to perform all the disclosures first, and then all the erasures. This can be intuitively explained as follows. By performing the disclosures first, the network works in larger flats with a much higher combination power. This large number of combinations allows to produce bases with ‘distant’ elements to the original flat, and hence drift away from the original flat without taking steps on the lattice. It then suffices to go back down by erasing some elements. On the other hand, performing the erasures first implies to work in smaller flats with less combination power, which hinders the message from drifting away from the original flat.

Proposition 6: For any pair of flats $f, g$ of a matroid, the union-path $U(f, g)$, defined as starting from $f$, going up the lattice of flats to $\text{cl}(f \cup g)$, and then going back down to $g$, is a shortest path between $f$ and $g$. Therefore, the shortest path distance $s(f, g)$ between $f$ and $g$ is given by $s(f, g) = 2\text{rk}(f \cup g) - \text{rk}(f) - \text{rk}(g)$.

Proof: Without loss of generality, suppose $\text{rk}(f) \geq \text{rk}(g)$. We shall prove the claim by induction on $s(f, g)$. First, the cases $s(f, g) = 0$ and $s(f, g) = 1$ are trivial. Also, if $s(f, g) = 2$, then either $g \subset f$ and the union-path is the only path of length 2 or $g \nsubseteq f$ and the only path of length 2 distinct from the union-path is the intersection-path $\{f, f \cap g, g\}$. The intersection-path has length $\text{rk}(f) + \text{rk}(g) - 2\text{rk}(f \cap g)$; however, $2\text{rk}(f \cup g) - \text{rk}(f) - \text{rk}(g) \leq \text{rk}(f) + \text{rk}(g) - 2\text{rk}(f \cap g)$ by (1), and hence the union-path is no longer than the intersection-path. Therefore, the union-path is among the shortest paths for $s(f, g) = 2$.

Now suppose the claim is true for all pairs of flats with a shortest path of length no more than $d$, ...
and consider \( f \) and \( g \) such that \( s(f, g) = d + 1 \). Let \( \{f, p_1, \ldots, p_d, g\} \) be a shortest path between \( f \) and \( g \). Since \( s(f, p_d) = d \), \( U(f, p_d) \) is a shortest path between \( f \) and \( p_d \), and without loss of generality we assume \( \{f, p_1, \ldots, p_{d-1}, p\} = U(f, p_d) \). Also, by definition of the lattice, either \( g \subseteq p_d \) or \( p_d \subseteq g \). We consider both cases successively.

- **Case I:** \( g \subseteq p_d \). We first prove that \( \text{cl}(f \cup g) = \text{cl}(f \cup p_d) \). Since \( g \subseteq p_d \), we have \( \text{cl}(f \cup g) \subseteq \text{cl}(f \cup p_d) \). Also, the length of \( U(f, p_d) \) indicates that \( 2\text{rk}(f \cup p_d) = \text{rk}(f) + \text{rk}(g) + 1 + d \); similarly, the length of \( U(f, g) \) yields \( 2\text{rk}(f \cup g) = \text{rk}(f) + \text{rk}(g) + d + 1 = 2\text{rk}(f \cup p_d) \), and we obtain \( \text{cl}(f \cup p_d) = \text{cl}(f \cup g) \). Therefore, the union-path between \( f \) and \( g \) satisfies \( U(f, g) = U(f, p_d) \cup \{g\} \) and hence has length \( d + 1 \) and is a shortest path.

- **Case II:** \( p_d \subseteq g \). We have \( \text{rk}(f) \geq \text{rk}(g) = \text{rk}(p_d) + 1 \), and hence \( \text{rk}(p_d) = \text{rk}(g) \). Since \( s(p_{d-1}, g) = 2 \), \( U(p_{d-1}, g) = \{p_{d-1}, \text{cl}(p_{d-1} \cup g), g\} \) is a shortest path between \( p_{d-1} \) and \( g \). Therefore, the path \( U(f, \text{cl}(p_{d-1} \cup g)) \cup \{g\} \) is a shortest path between \( f \) and \( g \) which satisfies the hypotheses of Case I. Thus, the union-path \( U(f, g) \) is a shortest path between \( f \) and \( g \).

By Proposition 6 the easiest way to modify messages transmitted through a network is by injecting more packets first, and then erasing other packets. Therefore, we model data transmission through a faulty network as an operator channel, where the source transmits a flat \( f \in \mathcal{F} \) and the destination obtains another flat \( g \in \mathcal{F} \), which can be expressed as

\[
g = C(f \cup \delta, \epsilon),
\]

where \( \delta = C(f \cup g, f) \) is a flat representing the disclosures that have been performed, \( \epsilon = C(f \cup g, g) \) is a flat representing all the erasures, and \( C \) denotes the complement, defined in Section II-A. We remark that although \( \delta \) and \( \epsilon \) are not unique, their ranks are uniquely determined by \( f \) and \( g \) and given by \( \text{rk}(\delta) = \text{rk}(f \cup g) - \text{rk}(f) \) and \( \text{rk}(\epsilon) = \text{rk}(f \cup g) - \text{rk}(g) \), respectively. They hence represent the minimal number of disclosures and erasures for the network to transform the input flat \( f \) into the output flat \( g \). Accordingly, we define the lattice distance between \( f \) and \( g \) as

\[
d_L(f, g) = \text{rk}(\delta) + \text{rk}(\epsilon)
\]

\[
= 2\text{rk}(f \cup g) - \text{rk}(f) - \text{rk}(g)
\]

\[
\leq \text{rk}(f \cup g) - \text{rk}(f \cap g)
\]

\[
\leq \text{rk}(f) + \text{rk}(g) - 2\text{rk}(f \cap g),
\]

where (22) and (23) follow the submodular inequality (1).
For SAF, the lattice distance between two subsets is their Hamming distance; for RLNC, the lattice distance between two linear subspaces is their subspace distance. We remark that for both RLNC and SAF, we have equality in (22) and (23) for all flats. This however does not hold for all matroids; those which satisfy this property can all be expressed as direct sums of free matroids and projective geometries [3, Proposition 6.9.1]. Furthermore, the right hand sides of (22) and (23) are not necessarily metrics.

As an illustration of inequalities (22) and (23), we now provide an example where these inequalities are strict. Consider the following matroid, where \( E = [5], I = \mathcal{P}(E) - \mathcal{P}(E, 5), \) and \( F = \mathcal{P}(E) - \mathcal{P}(E, 4). \) Then the flats \( f = \{0, 1, 2\} \) and \( g = \{0, 3, 4\} \) satisfy \( \text{rk}(f) = \text{rk}(g) = 3, \text{rk}(f \cup g) = 4, \) and \( \text{rk}(f \cap g) = 1, \) and hence \( d_L(f, g) = 2, \) while \( \text{rk}(f \cup g) - \text{rk}(f \cap g) = 3 \) and \( \text{rk}(f) + \text{rk}(g) - 2\text{rk}(f \cup g) = 4. \) Also, by considering the flats \( f, g, \) and \( E, \) it can be shown that the right hand sides of (22) and (23) violate the triangular inequality. This example also illustrates how the lattice distance expresses the minimum number of operations required to change one flat into the other. In our example, changing \( f \) into \( g \) takes only two operations: first disclose the element 3 to obtain \( \text{cl}(f \cup \{3\}) = E, \) which after combinations has a basis given by \( \{0, 2, 3, 4\}; \) then erase the element 2 to obtain \( \{0, 3, 4\} = g. \)

The modified lattice distance

\[
d_M(f, g) = \max\{\text{rk}(\delta), \text{rk}(\epsilon)\}
= \text{rk}(f \cup g) - \min\{\text{rk}(f), \text{rk}(g)\}
\leq \max\{\text{rk}(f), \text{rk}(g)\} - \text{rk}(f \cap g)
\]

represents the maximum between the number of erasures and the number of disclosures needed to modify the input flat \( f \) into the output flat \( g. \) For SAF, it coincides with the modified Hamming metric [2], while for RLNC the modified lattice distance between two subspaces is given by their injection distance [4]. Similarly to the lattice distance, equality holds in (25) for SAF and RLNC; however, inequality is strict in the example above. Furthermore, an example where the right hand side of (25) violates the triangular inequality can be found.

We remark that the lattice distance and the modified lattice distance only depend on the lattice of flats of the matroid. However, for any non-simple matroid, there exists a simple matroid with the same lattice of flats. Therefore, our assumption in Section III of considering simple matroids only does not lead to any loss in generality.

Corollary 4 ensures that the distances defined above are metrics. Therefore, error correction for random network communications can be viewed as a coding theory problem, where the codewords are flats of a
Corollary 4: For any simple matroid with rank \( r \), the lattice distance and the modified lattice distance associated to that matroid are metrics which take integer values between 0 and \( r \).

Proof: The lattice distance is a metric according to Proposition 6. For the modified lattice distance, by (21) and (24) we have
\[
d_M(f, g) = \frac{1}{2} d_L(f, g) + \frac{1}{2} |\mathrm{rk}(f) - \mathrm{rk}(g)|
\]
for all flats \( f, g \in \mathcal{F} \), and hence we easily obtain that \( d_M \) is also a metric. It is clear that these metrics only have integer values between 0 and \( r \).

We remark that it was already proven that the lattice distance is a metric in [28, Theorem 2.4], using a completely different approach.

B. Matroid codes and liftings

For any simple matroid \( \mathcal{M} \), we define a matroid code as a nonempty set of flats of a matroid, or equivalently as a subset of the set of flats \( \mathcal{F} \). The minimum lattice (modified lattice, respectively) distance of a matroid code is given by the minimum distance between two pairs of distinct codewords. All the other classical parameters of a code, such as the error correction capability, the covering radius, the diameter, etc. can be similarly defined. Following Remark 3) of Section III, we also define a constant-rank matroid code as a set of flats of the same rank. By (21) and (24), the minimum lattice distance of a constant-rank matroid code is twice its minimum modified lattice distance.

The definitions above can be extended to codes on \( n \)-tuples of flats, where the lattice distance between two \( n \)-tuples \( f = (f_0, f_1, \ldots, f_{n-1}) \) and \( g = (g_0, g_1, \ldots, g_{n-1}) \) in \( \mathcal{F}^n \) can be defined as the sum of distances between their coordinates:
\[
d_L(f, g) = \sum_{i=0}^{n-1} d_L(f_i, g_i)
\]
and the modified lattice distance can be similarly defined. Codes on \( n \)-tuples allow for error control on the level of the stream of messages. They hence offer a higher data rate for the same error correction capability and as such have been proposed for RLNC [29] and SAF [30]. However, for the sake of clarity and conciseness we shall not consider such codes in this paper.

We now derive bounds on matroid codes and constant-rank matroid codes which generalize the bounds derived for constant-dimension codes and constant-weight codes. We denote the maximum cardinality of a matroid code on the flats of a simple matroid \( \mathcal{M} \) with minimum lattice (modified lattice, respectively) distance \( d \) as \( A_L(\mathcal{M}, d) \) (\( A_M(\mathcal{M}, d) \), respectively). We also denote the maximum cardinality of a constant-rank matroid code on the flats of rank \( k \) of \( \mathcal{M} \) with minimum modified lattice distance \( d \) (and hence minimum lattice distance \( 2d \)) as \( A_M(\mathcal{M}, k, d) \).
Denoting the rank of $\mathcal{M}$ as $r$, we first remark that $A_L(\mathcal{M}, k, 1) = N_k$ for all $0 \leq k \leq r$ and $A_L(\mathcal{M}, 1) = A_M(\mathcal{M}, 1) = \sum_{k=0}^{r} N_k$. Also, it is easily shown that for all $f, g \in \mathcal{F}$

$$|\text{rk}(f) - \text{rk}(g)| \leq d_L(f, g) \leq \min \{ \text{rk}(f) + \text{rk}(g), 2r - \text{rk}(f) - \text{rk}(g) \},$$

(26)

$$|\text{rk}(f) - \text{rk}(g)| \leq d_M(f, g) \leq \min \{ \max \{\text{rk}(f), \text{rk}(g)\}, r - \min \{\text{rk}(f), \text{rk}(g)\} \}.$$  

(27)

In particular, if $\text{rk}(f) = \text{rk}(g) = k$, we have $d_M(f, g) \leq \min \{k, r - k\}$. We hence shall use the following convention: $A_M(\mathcal{M}, k, d) = 1$ for all $d > \min \{k, r - k\}$.

Proposition 7 gives some elementary relations between the quantities defined above.

**Proposition 7 (Bounds on the maximum cardinality of matroid codes):** For $d > \frac{r}{2}$, $A_M(\mathcal{M}, d) = 2$. For $d \leq \frac{r}{2}$, we have

$$\max_{0 \leq k \leq n} A_M(\mathcal{M}, k, d) \leq A_L(\mathcal{M}, 2d) \leq A_M(\mathcal{M}, d) \leq 2 + \sum_{k=d}^{r-d} A_M(\mathcal{M}, k, d).$$

(28)

**Proof:** For all $f, g \in \mathcal{F}$, we have $d_L(f, g) \leq 2d_M(f, g)$ by (21) and (24). Hence a matroid code with minimum lattice distance $2d$ has minimum modified lattice distance at least $d$, and $A_L(\mathcal{M}, 2d) \leq A_M(\mathcal{M}, d)$. Also, any constant-rank matroid code of rank $k$ and minimum modified lattice distance $d$ is a matroid code with minimum lattice distance $2d$, which easily leads to the lower bound in (28).

We now prove the upper bound. We remark that the code $\{\emptyset, E\}$ has minimum modified lattice distance $r$, and hence $A_M(\mathcal{M}, d) \geq 2$ for all $d$. Also, let $C$ be a code on the flats of $\mathcal{M}$ with minimum modified lattice distance $d$ and let $f, g \in C$. We have $\max \{\text{rk}(f), \text{rk}(g)\} \geq d$ by (27), therefore there is at most one codeword in $C$ with rank less than $d$. Similarly, $\min \{\text{rk}(f), \text{rk}(g)\} \leq r - d$, and there is at most one codeword with rank greater than $r - d$. Thus $A_M(\mathcal{M}, d) = 2$ for $d > \frac{r}{2}$ and $A_M(\mathcal{M}, d)$ is no more than two plus the cardinality of a code whose codewords have rank between $d$ and $r - d$ for $d \leq \frac{r}{2}$. It is clear that the cardinality of such a code is upper bounded by $\sum_{k=d}^{r-d} A_M(\mathcal{M}, k, d)$, and hence we obtain the upper bound in (28).

Expressing the rightmost inequality in (28) as a lower bound on $A_M(\mathcal{M}, k, d)$, Corollary 5 indicates that constant-rank matroid codes are nearly optimal matroid codes for both the lattice metric and the modified lattice metric. Therefore, we only consider constant-rank matroid codes henceforth.

**Corollary 5:** For $d \leq \frac{r}{2}$, we have $\max_{0 \leq k \leq r} A_M(\mathcal{M}, k, d) \geq \frac{A_M(\mathcal{M}, d) - 2}{r - 2d + 1} \geq \frac{A_L(\mathcal{M}, 2d) - 2}{r - 2d + 1}$.

Johnson bounds have first been derived for constant-weight codes [31] and have been adapted to constant-dimension codes in [14], [16]. Proposition 8 below generalizes these bounds to the case of constant-rank matroid codes. We introduce two ways to restrict to a submatroid of inferior rank. First, for any $e \in E$, we denote the simple matroid with lattice of flats given by the interval $[e, E]$ as $\mathcal{M} + e$.
and for any non-empty flat $f \in \mathcal{F}(\mathcal{M})$, we denote the flat $\text{cl}(f \cup e)$ as $f + e \in \mathcal{F}(\mathcal{M} + e)$. Note that the matroid $\mathcal{M} + e$ has rank $r - 1$ and for all $f$, $\text{rk}_{\mathcal{M} + e}(f + e) = \text{rk}_{\mathcal{M}}(f \cup e) - 1$. Second, for any hyperplane $h \in \mathcal{F}_{r-1}$, we denote the simple matroid whose lattice of flats is given by the interval $[\emptyset, h]$ as $\mathcal{M}|h$. For any flat $f$, the flat $f \cap h$ is in $\mathcal{M}|h$ and $\text{rk}_{\mathcal{M}}(f \cap h) = \text{rk}_{\mathcal{M}|h}(f \cap h)$.

**Proposition 8 (Johnson bound for constant-rank matroid codes):** For all $\mathcal{M}$ and $0 \leq k \leq r$, denote the minimum cardinality of a flat of rank $k$ and the minimum number of hyperplanes containing a given flat of rank $k$ as $c_k$ and $h_k$, respectively. Then there exist $e \in E$ and $h \in \mathcal{F}_{r-1}$ such that

$$A_{\mathcal{M}}(\mathcal{M}, k, d) \leq \frac{N_1}{c_k} A_{\mathcal{M}}(\mathcal{M} + e, k - 1, d),$$

$$A_{\mathcal{M}}(\mathcal{M}, k, d) \leq \frac{N_{r-1}}{h_k} A_{\mathcal{M}}(\mathcal{M}|h, k, d).$$

**Proof:** We only prove (29), the proof of (30) being similar. For all $f \in \mathcal{F}$ and $e \in E$, let $\chi(e, f) = 1$ if $e \in f$ and $\chi(e, f) = 0$ otherwise. Let $\mathcal{C}$ be a code on the flats of $\mathcal{M}$ with constant-rank $k$, minimum distance $d$, and cardinality $A_{\mathcal{M}}(\mathcal{M}, k, d)$. Then for all $e \in E$, $\mathcal{C}(e) = \{ f + e : f \in \mathcal{C}, e \in f \}$ is a code on the flats of $\mathcal{M} + e$ with constant-rank $k - 1$ and cardinality $\sum_{f \in \mathcal{C}} \chi(e, f)$. Furthermore, if $f$ and $g$ are two codewords of $\mathcal{C}$ containing $e$, then $d_{\mathcal{M}}(f + e, g + e) = d_{\mathcal{M}}(f, g)$. Therefore, $\mathcal{C}(e)$ has minimum distance $d$ and hence $\sum_{f \in \mathcal{C}} \chi(e, f) \leq A_{\mathcal{M}}(\mathcal{M} + e, k - 1, d)$. Conversely, we have $\sum_{e \in E} \chi(e, f) = |f| \geq c_k$ for all $f \in \mathcal{C}$. Combining, we obtain that there exists an element $e' \in E$ for which $|E|A_{\mathcal{M}}(\mathcal{M} + e', k - 1, d) \geq \sum_{e \in E} \sum_{f \in \mathcal{C}} \chi(e, f) \geq c_k A_{\mathcal{M}}(\mathcal{M}, k, d)$.

**Proposition 9** below is a generalization of the Singleton bound for constant-dimension codes derived in [1].

**Proposition 9 (Singleton bound for constant-rank matroid codes):** For all $\mathcal{M}$, $0 \leq k \leq r$, and any element $e \in E$, we have $A_{\mathcal{M}}(\mathcal{M}, k, d) \leq A_{\mathcal{M}}(\mathcal{M} + e, k, d - 1)$.

**Proof:** Let $\mathcal{C}$ be a code on $\mathcal{F}_k(\mathcal{M})$ with minimum distance $d$ and cardinality $A_{\mathcal{M}}(\mathcal{M}, k, d)$. For any $f \in \mathcal{C}$, we define the puncturing $H_e(f)$ as the following flat in $\mathcal{F}_k(\mathcal{M} + e)$: $H_e(f) = f + e$ if $\text{rk}_{\mathcal{M} + e}(f + e) = k$ and $H_e(f)$ is a random superflat of $f + e$ if the latter has rank $k - 1$. Then by the lengths of the shortest paths on the lattice of flats of $\mathcal{M}$, $d_L(H_e(f), H_e(g)) \geq d_L(f, g) - 2$ and hence $d_{\mathcal{M}}(H_e(f), H_e(g)) \geq d_{\mathcal{M}}(f, g) - 1$. Therefore, the code $\{H_e(f) : f \in \mathcal{C}\}$ is a code on the flats of $\mathcal{M} + e$ with constant-rank $k$ and minimum distance at least $d - 1$ and its cardinality satisfies $A_{\mathcal{M}}(\mathcal{M}, k, d) \leq A_{\mathcal{M}}(\mathcal{M} + e, k, d - 1)$.

We remark that the Singleton bound in Proposition 9 is defined in terms of $\mathcal{M} + e$ and does not have a counterpart in terms of $\mathcal{M}|h$. This is because $\text{rk}(f \cap h) \geq \text{rk}(f) - 1$ does not necessarily hold for all flats $f$ and hyperplanes $h$. For instance, following the example given in Section V-A, we have
\( \text{rk}(f) = 3 \), while \( \text{rk}(f \cap g) = 1 \). Therefore, any puncturing based on the intersection with a hyperplane and guaranteeing a constant rank would alter the distance properties of the code.

Applying the Singleton bound in Proposition 9 successively yields the following compact form of the Singleton bound.

**Corollary 6:** For all \( M \) and \( 0 \leq k \leq r \), we have \( A_M(M, k, d) \leq \min_{g \in \mathcal{F}_{d-1}} |\{ f \in \mathcal{F}_{k+d-1} : g \subseteq f \}|. \)

We finish this section by deriving the analogues of the Gilbert and Hamming bounds for constant-rank matroid codes. For all \( k, l, \) and \( t \), we denote the average (minimum, respectively) over all flats \( f \in \mathcal{F}_k \) of the number of flats of rank \( l \) at lattice distance no more than \( t \) from \( f \) as \( V_L^{\text{avg}}(k, l, t) \) (\( V_L^{\text{min}}(k, l, t) \), respectively).

**Proposition 10 (Gilbert and Hamming bounds for constant-rank matroid codes):** For all \( k \) and \( d \), we have

\[
\frac{N_k}{V_L^{\text{avg}}(k, k, 2(d-1))} \leq A_M(M, k, d) \leq \min_{0 \leq l \leq r} \left\{ \frac{N_l}{V_L^{\text{min}}(k, l, d-1)} \right\}. \tag{31}
\]

**Proof:** The lower bound is a direct application of the generalization of the Gilbert bound in [32], while the upper bound is obtained by a sphere-packing argument on \( \mathcal{F}_l \).

### C. Liftings

Perhaps the most interesting property of subspace codes is their construction by lifting a rank metric code, thus reducing the design of good subspaces codes as a problem on matrices. In this section, we generalize this definition to all matroids and we evaluate the performance of different types of liftings.

We define a lifting as a triple \((\nu, d, I)\), where \( \nu \) is an integer, \( d \) is a metric on \([q^{k\nu}]\), and \( I \) is an isometry from \((q^{k\nu}, d)\) to \((\mathcal{F}_k, d_M)\). Clearly, we have \( q^{k\nu} \leq N_k \); accordingly, Proposition 11 below shows that a lifting with \( \nu = \lfloor \log_q N_k \rfloor \) always exists.

**Proposition 11:** For any matroid \( M \) with \( N_k \) flats of rank \( k \) and any \( q \geq 2 \), there exists a lifting with \( \nu = \lfloor \log_q N_k \rfloor \).

**Proof:** Order all the flats of rank \( k \) as \( f_m, 0 \leq m \leq |\mathcal{F}_k| - 1 \) and define \( I \) from \([q^{k\nu}]\) to \( \mathcal{F}_k \) as \( I(m) = f_m \) and \( d(m, n) = d_L(I(m), I(n)) \) for all \( m, n \in [q^{k\nu}] \). By construction, the triple \((\nu, d, I)\) forms a lifting.

According to Proposition 11, we say the lifting is optimal if \( \nu = \lfloor \log_q N_k \rfloor \). We remark that the lifting presented in the proof of Proposition 11 is only interesting theoretically but not practically, as it does not use any other structure than the one supported by the set of flats, and instead selects a subset of flats and applies the lattice distance to it. We hence introduce the concept of systematic liftings, which utilize...
and take advantage of a different structure. A lifting is said to be systematic if for all \( m \in [q^k]\), there exists a basis of \( I(m) \) which contains the expansion of \( m \) in basis \( q \). Proposition 12 below evaluates the optimality of the systematic liftings proposed for SAF and RLNC and reviewed in Section II-B.

**Proposition 12:** The linear lifting \( I_L \) for RLNC is systematic and optimal for all \( q \geq 2 \) and \( k \geq 1 \). The systematic lifting \( I_S \) for SAF is optimal for \( q > 2 \) but not necessarily optimal for \( q = 2 \).

**Proof:** Since both liftings are clearly systematic, we only study their optimality. For RLNC, we have \( \binom{n}{k} < K_q^{-1}q^{k(n-k)} \), where \( K_q^{-1} < 2^2 \) and \( K_q^{-1} < q \) for \( q > 2 \). Therefore, the lifting \( I_L \) is optimal for \( q > 2 \) or \( k \geq 2 \). For \( q = 2, k = 1 \), we have \( \binom{n}{1} = 2^n - 1 < 2^{(n-1)+1} \), and hence \( I_L \) is still optimal. For SAF, we have \( \binom{q^n}{k} < e^k \left( \frac{q^n}{k} \right)^k \), and hence the lifting \( I_S \) is optimal for \( q > e \). However, if \( q = 2, n = 6, k = 2^3 \), then \( \log_q \left( \frac{q^n}{k} \right) > 4 \), while \( \nu = n - \log_q k = 3 \) for \( I_L \), which is not optimal.

We remark that the example given in the proof of Proposition 12 is far from being a singularity. Indeed, for all \( k \geq 6 \) there exists an integer \( n_k \) such that \( \binom{n_k}{k} \geq \left( \frac{2n_k}{k} \right)^k \), and hence the lifting \( I_S \) is not optimal. Furthermore, \( n_k \) is on the order of \( 2k \) for large values of \( k \).

**VI. RANDOM AFFINE NETWORK CODING**

A. Model and parameters

As seen in Section III-B the simple matroid associated to RLNC is the projective geometry with rank \( n \), whose alphabet only has \( \binom{n}{1} \sim q^{n-1} \) elements. This implies a loss in terms of data rate, as the elements are not perfectly embedded into packets of length \( n \). Similarly, any linear subspace has \( \binom{k}{1} \sim q^{k-1} \) elements, which compared to the \( q^k \) possible linear combinations, leads to a decrease in combination power. These issues are immediate consequences of the existence of a loop (the all-zero vector) and parallel elements (collinear vectors), which in turn follows the paradigm of linear network coding of viewing packets as vectors.

In this section, we introduce a novel network coding protocol, referred to as random affine network coding (RANC), where packets are viewed as points in an affine space and where intermediate nodes combine packets by affine combinations. An affine combination of points \( \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1} \in \text{GF}(q)^n \) is any sum of the form \( \sum_{i=0}^{k-1} a_i \mathbf{v}_i \), where the scalars \( a_i \in \text{GF}(q)^n \) satisfy \( \sum_{i=0}^{k-1} a_i = 1 \). In other words, an affine combination corresponds to determining the centroid of the points \( \mathbf{v}_i \) with masses \( a_i \).

A collection of points are said to be affinely independent if \( \sum_{i=0}^{k-1} b_i \mathbf{v}_i \neq 0 \) for all \( b_i \)s not all zero and satisfying \( \sum_{i=0}^{k-1} b_i = 0 \). The matroid associated to RANC is hence given by the affine geometry \( AG(n, q) \), which we will denote as \( A(q, n) \) or simply \( A \) if there is no ambiguity about the parameter values. The closure of a set of points is all the possible affine combinations of these points, referred to as the affine hull,
which forms an affine subspace. By definition, the rank of a set of points is given by the number of affinely independent points, and is equal to the rank of their affine hull. For any $v_0, v_1, \ldots, v_{k-1} \in \mathbb{GF}(q)^n$, we then have $\text{rk}(v_0, v_1, \ldots, v_{k-1}) = \text{rank}(1|V)$, where $V = (v_0^T, v_1^T, \ldots, v_{k-1}^T)^T$ and rank denotes the number of linearly independent rows of a matrix.

Unlike RLNC, the matroid associated to RANC has rank $n + 1$. The set $\mathcal{F}_k$ of flats of rank $k$ being the set of affine subspaces of rank $k$, we have $N_k = q^{n-k+1}\binom{n}{k-1}$ and $C_k = q^{k-1}$ for $1 \leq k \leq n + 1$ [3, Section 6.2]. By construction, $\mathcal{A}(q, n) = AG(n, q)$ is a submatroid of $\mathcal{L}(q, n+1) = PG(n, q)$. However, we shall demonstrate below that $\mathcal{A}(q, n)$ behaves closely to $\mathcal{L}(q, n+1)$, hence virtually allowing to work on packets of length $n + 1$ instead of $n$.

The affine geometry is a perfect matroid design, hence the results derived in Section IV about rate, delay, and partial decoding can be applied. The performance parameters defined in Sections IV-A and IV-B are given for $\mathcal{A}$ by

$$R(\mathcal{A}, k) = \frac{n - k + 1 + \log q^n}{nk} \sim 1 - \frac{k - 1}{n}, \quad (32)$$

$$D(\mathcal{A}, k) = k + \sum_{j=1}^{k-1} \frac{1}{q^j - 1} < k + \alpha_q, \quad (33)$$

$$T(\mathcal{A}, k) \sim 1 - \frac{k - 1}{n}. \quad (34)$$

Let us compare these results to the ones derived in Section IV for RLNC. First, the affine geometry allows a gain in terms of rate of about one symbol per packet, due to the increase in the number of flats from around $q^{k(n-k)}$ to around $q^{k(n-k+1)}$. This gain of one symbol per packet follows the fact that RLNC only considers around $q^{-1}$ of all possible packets of length $n$, while RANC considers all possible packets. Second, the delay of RANC is very close to that of RLNC. Indeed, by Proposition 2 the average delay is determined by the cardinality of flats, which only changed from $\frac{q^{k-1}}{q-1}$ for RLNC to $q^{k-1}$ for RANC. Third, the increase in rate and the constant delay lead to a gain in throughput of one symbol per packet in (34).

We now determine the probability to receive $l$ affinely independent packets once $r$ packets have been received.

**Proposition 13 (Probability of independence for RANC):** For RANC, we have $P_l(\mathcal{A}, k; r, 0) = \delta_r$ and for all $1 \leq l \leq r$ and $k$,

$$P_l(\mathcal{A}, k; r, l) = q^{-(k-1)(r-1)} \binom{k-1}{l-1} \prod_{i=0}^{l-2} (q^{r-1} - q^i), \quad (35)$$

and in particular $P_l(\mathcal{A}, k; k, k) = \prod_{j=1}^{k-1} (1 - q^{-j}) > K_q$. 

March 10, 2010 DRAFT
As we shall see later, the upper bound on $P_I(A,k;r,l)$ is the number of collections of points $v_0, v_1, \ldots, v_{r-1} \in \text{GF}(q)^n$ in a flat of rank $k$ with exactly $l$ affinely independent points. Let $W = (v_0^T - v_{r-1}^T, v_1^T - v_{r-1}^T, \ldots, v_{r-2}^T - v_{r-1}^T)^T \in \text{GF}(q)^{(r-1) \times n}$. Then $\text{rk}(v_0, v_1, \ldots, v_{r-1}) = \text{rank}(V) = 1 + \text{rank}(W)$. Therefore, $W$ is a matrix with rank $l - 1$ whose columns belong to a linear subspace of dimension $k - 1$. There are $q^{k-1}$ choices for $v_{r-1}$ and $\prod_{i=0}^{l-2}(q^{r-1} - q^i)$ choices for $W$, and hence $A(r,l) = q^{k-1} \prod_{i=0}^{l-2}(q^{r-1} - q^i)$ which leads to (35). In particular, for $r = l = k$, (35) yields $P_I(A,k;k,k) = \prod_{j=1}^{k-1}(1 - q^{-j})$.

Therefore, the average number of independent elements given $r$ elements have been received satisfies $E_I(A,k;r) > K_q \min\{r,k\}$, which tends to the optimal when the field size $q$ increases. Hence RANC behaves similarly to RLNC in terms of receiving independent messages. This confirms our result in (33) where we showed that RANC and RLNC have very close average delays.

Finally, by applying Proposition 5 to the affine geometry and using $F(a,l) = \prod_{j=1}^{k-1}(1 - q^{-j})$, we easily obtain (36). Therefore, RANC is also very similar to RLNC in terms of partial decoding and follows the same zero-one pattern.

### B. Matroid codes for the affine geometry

We are now interested in matroid codes on affine subspaces, and more particularly to constant-rank matroid codes, according to Corollary 5. We first remark that the affine geometry does not have a dual relationship similar to those existing for SAF or RLNC. Hence, (21) does not necessarily hold with equality in the affine geometry. For example, two parallel hyperplanes in $A(q,n)$ are at lattice distance 2, while (21) yields $n + 1$.

By definition, we have $A_M(A,k,1) = A_k = q^{n-k+1} \sum_{k-1}^{n} \geq q^{k(n-k+1)}$ for all $0 \leq k \leq n + 1$. Since the affine geometry $A(q,n)$ is a matroid of the projective geometry $L(q,n+1)$, we easily obtain

$$A_M(A(q,n),k,d) \leq A_M(L(q,n+1),k,d) < K_q^{-1} q^{\min\{(n-k+1)(k-d+1),k(n-k-d+2)\}}.$$ (36)

As we shall see later, the upper bound on $A_M(A(q,n),k,d)$ in (36) is tight up to a scalar. However, we refine this bound below by applying the Johnson bounds derived in Proposition 8 to codes on affine subspaces.

**Proposition 14 (Bounds on constant-rank matroid codes on affine subspaces):** For all $2 \leq k \leq n - 1$
and $2 \leq d \leq \min\{k, n - k + 1\}$, we have
\[
A_M(A(q, n), k, d) \leq q^{n-k+1} A_M(L(q, n), k - 1, d),
\]
(37)
\[
A_M(A(q, n), k, d) \leq \left[ q \frac{q^n - 1}{q^{n-k+1} - 1} A_M(A(q, n - 1), k, d) \right]
\leq \left[ q \frac{q^n - 1}{q^{n-k+1} - 1} \left[ q \frac{q^{n-1} - 1}{q^{n-k} - 1} \cdots \left[ q \frac{q^{k+d-1} - 1}{q^d - 1} \cdots \right] \right] \right].
\]
(38)
(39)

**Proof:** For any $e \in \text{GF}(q)^n$ and $h \in F_n(A(q, n))$, $A(q, n) + e$ and $A(q, n)|h$ are isomorphic to $L(q, n - 1)$ and $A(q, n)$, respectively [3, Proposition 6.2.5]. Also, every flat with rank $k$ of $A(q, n)$ contains $q^{k-1}$ elements and is contained into $\left[\begin{array}{c} n-k+1 \end{array}\right]$ hyperplanes. Applying Proposition 9 and (29) and (30) in Proposition 8 to $A(q, n)$ hence leads to (37) and (38), respectively. Finally, applying (38) recursively yields (39).

We remark that the first Johnson bound in (37) is good for $2k \leq n + 1$, while the second Johnson bound in (38) is good for $2k \geq n + 1$. Also, the bounds obtained by applying the Singleton bound in Proposition 9 and the Hamming bound in Proposition 10 are looser than (37), and are hence omitted.

We now design an optimal systematic lifting for the affine geometry. Let $\nu = n - k + 1$, $d_R$ be the rank distance on matrices in $\text{GF}(q)^{k \times \nu}$ and $I_A$ be the mapping from $\text{GF}(q)^{k \times \nu}$ to $F_k$ defined as follows: for any $M \in \text{GF}(q)^{k \times \nu}$, $I_A(M)$ is the closure of the rows of $(I_k^T|M)$, where $I_k = (0|I_{k-1})^T \in \text{GF}(q)^{k \times (k-1)}$.

**Proposition 15 (Affine lifting):** The triple $(\nu, d_R, I_A)$ is an optimal systematic lifting from $\text{GF}(q)^{k \times \nu}$ to the set of flats with rank $k$ of $A(q, n)$.

**Proof:** First, $\text{rk}(I_A(M)) = \text{rank}(1|I_k^T|M) = k$ for all $M \in \text{GF}(q)^{k \times \nu}$, hence $I_A$ maps $\text{GF}(q)^{k \times \nu}$ to $F_k$. We now prove that $I_A$ is an isometry by considering two matrices $M, N \in \text{GF}(q)^{k \times \nu}$. We have
\[
\text{rk}(I_A(M) \cup I_A(N)) = \text{rank} \left( \begin{array}{c|c} 1 & I_k^T \\ \hline 1 & I_k \\ \end{array} \right) \begin{array}{c|c} M \\ \hline N \\ \end{array} = \text{rank} \left( \begin{array}{c|c} 1 & I_k^T \\ \hline 0 & 0 \\ \end{array} \right) \begin{array}{c|c} M \\ \hline N \\ \end{array} = k + \text{rank}(M - N)
\]
since the matrix $(1|I_k^T)$ has rank $k$. Therefore, $d_L(I_A(M), I_A(N)) = d_R(M, N)$ and $(\nu, d_R, I_A)$ is a lifting. By construction, this lifting is both optimal and systematic.

We remark that affine liftings of rank metric codes have a clear canonical basis, given by the matrix $(I_k^T|M)$. This basis can be easily determined from any other basis of a flat via Gaussian elimination of the pairwise differences of the received points.

By lifting an optimal rank metric code, we easily obtain a construction of nearly optimal constant-rank matroid codes on the affine geometry.

**Corollary 7:** For all $0 \leq k \leq n + 1$, we have $A_M(A, k, d) \geq q^{\min\{\binom{n-k+1}{k-d+1}, k(n-k-d+2)\}}$. 

March 10, 2010
Combining (36), Corollary 7, and the bounds on the maximum cardinality of constant-dimension codes reviewed in Section II, we obtain

\[ K_q A_M(\mathcal{L}(q, n + 1), k, d) < A_M(\mathcal{A}(q, n), k, d) \leq A_M(\mathcal{L}(q, n + 1), k, d). \]

Therefore, RANC utilizes codes with a similar cardinality to subspace codes for packets longer by one symbol. This gain is clearly illustrated by the definition of affine lifting, which removes the first column from the identity matrix used in the linear lifting. The gain in data rate in (33) derived for the error-free case is hence preserved when error control is implemented. Furthermore, we prove in Section VI-C below that this gain comes with no significant cost in terms of decoding complexity.

C. Decoding of liftings of Gabidulin codes

By construction, the lifting introduced above for RANC is closely related to the lifting introduced in [?1?] for RLNC. In this section, we utilize this relation to design a low-complexity decoding of affine liftings of Gabidulin codes. More generally, we prove that decoding the affine lifting of a rank metric code can be performed using a subspace distance decoder for the linear lifting of the same code.

In order to clarify notations, we shall use the subscripts \( \mathcal{A} \) and \( \mathcal{L} \) to refer to objects (ranks and lattice distances) defined for RANC and RLNC, respectively. We introduce the nonsingular matrix \( X_{n+1} = (v_k^T | I_{n+1}') \in \text{GF}(q)^{(n+1) \times (n+1)} \), where \( v_k = (1, -1, -1, \ldots, -1, 0, \ldots, 0) \) has \( k \) nonzero coefficients. For any affine subspace \( M \in \mathcal{F}(\mathcal{A}(q, n)) \) of rank \( k \) given by the closure of the rows of the matrix \( M \in \text{GF}(q)^{k \times n} \), we denote the linear subspace of \( \text{GF}(q)^{n+1} \) with dimension \( k \) generated by \( (1|M)X_{n+1} \) as \( r(M) \in \mathcal{F}(\mathcal{L}(q, n + 1)) \). Multiplying on the right by \( X_{n+1} \) can hence be viewed as mapping the affine subspaces of \( \text{GF}(q)^n \) into linear subspaces of \( \text{GF}(q)^{n+1} \). Proposition 16 below shows that this mapping preserves the lattice distance, and that the image of the affine lifting of a matrix is the linear lifting of the same matrix.

**Proposition 16:** For any affine subspace \( M \in \mathcal{F}(\mathcal{A}(q, n)) \) and any affine lifting \( I_\mathcal{A}(G) \in \mathcal{F}(\mathcal{A}(q, n)) \), we have \( d_{\mathcal{L}, \mathcal{A}}(M, I_\mathcal{A}(G)) = d_{\mathcal{L}, \mathcal{L}}(r(M), I_\mathcal{L}(G)) \).

**Proof:** Since \( X_{n+1} \) is nonsingular, we have \( \text{rk}_\mathcal{A}(M) = \text{rk} \{(1|M)X_{n+1}\} = \text{rk}_\mathcal{L}(r(M)) \). Also, it
is easily shown that \((1|I_k|C)X_{n+1} = (I_k|C)\), and hence

\[
d_{L,\mathcal{A}}(M, I_A(C)) = 2\text{rank} \left( \begin{array}{ccc} 1 & M & X_{n+1} \\ 1 & I_k & C \end{array} \right) - \text{rank}(1|M) - \text{rank}(1|I_k|C) \tag{40} \]

\[
= 2\text{rank} \left( (1|M)X_{n+1} \right) - \text{rank}(1|M)X_{n+1} \} - \text{rank}(I_k|C) \tag{41} \]

\[
= d_{L,\mathcal{L}}(r(M), I_{\mathcal{L}}(C)), \tag{42} \]

where (40) and (42) follow the definition of the lattice distance in (21), while (41) is obtained by multiplying by \(X_{n+1}\) on the right.

By Proposition 17, decoding \(M\) using the affine lifting of a Gabidulin code is equivalent to decoding \(r(M)\) using the linear lifting of the same code. We remark that transforming the matrix \(M\) into \((1|M)X_{n+1}\) can be simply performed by adding a column in front of \(M\), whose value is given by \(1 - \sum_{i=0}^{k-1} m_i\), where \(m_i\) denotes the \(i\)-th column of \(M\) for all \(0 \leq i \leq n - 1\). Therefore, the decoding algorithm for the affine lifting of a Gabidulin code follows two steps:

- **Step 1.** Obtain a matrix \(M\), and add the column \(1 - \sum_{i=0}^{k-1} m_i\) in front of it.
- **Step 2.** Apply the bounded subspace distance decoding algorithm in [1] for the row space of the extended matrix.

It is clear that the decoding complexity of this algorithm is on the same order as that of the algorithm in [1] for the same Gabidulin code, which is \(O(n^2)\) operations over \(GF(q)^{n-k+1}\). In order to summarize our results, the proposed implementation scheme for affine network coding is illustrated in Figure 4 for \(2k \leq n + 1\).

\[\text{VII. CONCLUSION}\]

In this paper, we introduced a novel model for the performance study of and noncoherent error control for data transmissions through a network. This model, based on flats of matroids, encompasses traditional techniques, such as linear network coding and routing, and offers a wealth of alternatives to these protocols. We evaluated the performance of these two protocols both in the error-free case and in the case where packets are lost, injected, or in error. We then designed a new network coding protocol based on the affine geometry which outperforms linear network coding in terms of data rate for the coded and non-coded cases. We identify a class of nearly optimal codes, for which we provide a low-complexity decoding algorithm. The results are summarized in Table I.
This topic opens many directions for future research, four of which are detailed below. First, the model we proposed is based on simple assumptions, which may not accurately reflect the reality of the network. Hence, we need to investigate how the specificity of the given network can be incorporated into our model. Second, many different types of matroids have been proposed, from the most elementary to the most sophisticated. Determining which matroids are desirable for a given situation is an important research direction, as it also determines the according protocol. Third, once the matroid is fixed, some tools are required to evaluate its performance and to compare it with other matroids. Although we introduced some parameters, such as the data rate and the average delay, new parameters may reflect some situations more accurately. Fourth, random affine network coding deserves to be investigated in further detail. In particular, the implementation of the low-complexity decoding procedure for liftings of Gabidulin codes introduced in this paper has a significant impact on the feasibility of affine network coding.

REFERENCES

<table>
<thead>
<tr>
<th>Matroid Parameters</th>
<th>Protocol</th>
<th>SAF</th>
<th>RLNC</th>
<th>RANC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matroid</td>
<td>$U_{q^n,q^n}$</td>
<td></td>
<td>$PG(n-1,q)$</td>
<td>$AG(n,q)$</td>
</tr>
<tr>
<td>Rank of the matroid</td>
<td>$q^n$</td>
<td></td>
<td>$n$</td>
<td>$n+1$</td>
</tr>
<tr>
<td>Combination</td>
<td>Selection</td>
<td></td>
<td>Linear combination</td>
<td>Affine combination</td>
</tr>
<tr>
<td>Flats</td>
<td>Subsets</td>
<td></td>
<td>Linear subspaces</td>
<td>Affine subspaces</td>
</tr>
<tr>
<td>Number of flats of rank $k$</td>
<td>$\binom{q^n}{k}$</td>
<td></td>
<td>$\binom{n}{k}$</td>
<td>$q^{n-k+1}\binom{n}{k-1}$</td>
</tr>
<tr>
<td>Cardinality of flats of rank $k$</td>
<td>$k$</td>
<td></td>
<td>$\frac{q^n-1}{q-1}$</td>
<td>$q^{k-1}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance Parameters</th>
<th>Rate</th>
<th>Average delay</th>
<th>Throughput</th>
<th>Independent elements</th>
<th>Partially decodable elements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\sim 1 - \frac{k \log q}{n}$</td>
<td>$\sim k \log k$</td>
<td>$\sim \frac{1}{\log k} - \frac{1}{n \log q}$</td>
<td>$\sim k(1 - e^{-\frac{k}{n}})$</td>
<td>$l \sim kq^{l-k}$</td>
</tr>
<tr>
<td></td>
<td>$\sim 1 - \frac{k}{n}$</td>
<td>$\sim k$</td>
<td>$\sim 1 - \frac{k}{n}$</td>
<td>$\sim \min{r,k}$</td>
<td>$\sim \min{r,k}$</td>
</tr>
<tr>
<td></td>
<td>$\sim k$</td>
<td>$\sim 1 - \frac{k}{n}$</td>
<td>$\sim 1 - \frac{k}{n}$</td>
<td>$\sim \min{r,k}$</td>
<td>$\sim \min{r,k}$</td>
</tr>
<tr>
<td></td>
<td>$\sim kq^{l-k}$</td>
<td>$\sim kq^{l-k}$</td>
<td>$\sim kq^{l-k}$</td>
<td>$\sim kq^{l-k}$</td>
<td>$\sim kq^{l-k}$</td>
</tr>
</tbody>
</table>

**TABLE I**

**Summary of parameters for SAF, RLNC, and RANC.**


