International Journal of Pure and Applied Mathematics
Volume 70 No. 3 2011, 307-316

# A NOTE ON MATROIDS, CODES AND INFORMATION THEORY

G.G. La Guardia[1 §], L. Grossi[2], R.C.A. Vieira[3], M.A.V. Pinto[4]
[1,2,3]Department of Mathematics and Statistics
State University of Ponta Grossa
84030-900, Ponta Grossa, PR, BRAZIL
[4]Department of Mechanics Engineering
Federal University of Paraná
CP 19.011, 81.531-990, Curitiba, PR, BRAZIL

**Abstract:** In this note we show that the height function of a lattice of flats of suitable classes of matroids satisfies the polymatroidal axioms. Moreover, we present a novel proof, by applying matroid theory, for the fact that the minimum distance of a graph-theoretic code $C$ is the smallest number of edges among the edge sets of cycles of $G$, where $G$ is the graph arising $C$.

**AMS Subject Classification:** 81Q99
**Key Words:** matroid theory, error-correcting codes, information theory

## 1. Introduction

In the seminal paper on matroid theory [20], Hassler Whitney drew attention to the problem of characterizing matroids that are representable over a given field. The connections between linear codes over fields and matroids represented over fields were presented in [10], where Greene shows how the weight enumerator of a linear code may be evaluated from Tutte's polynomial of an associated matroid. Other characterizations between matroids and error-correcting codes were presented in [2, 4, 3, 13, 14, 9, 6]. Concerning graph-theoretic codes there are some works available in the literature [12, 11, 1, 7, 8].

In this note we propose new connections among matroids, classical information theory and error-correcting codes.

This note is structured as follows. In Section 2, basic concepts on matroid

Received: November 24, 2010 

§Correspondence author

theory are revised. In Section 3 we present our contributions. More specifically: Subsection 3.1 presents a novel proof for a result concerning the minimum distance of graph-theoretic codes (see Theorem 14), Subsection 3.2 presents a novel relationship on matroids and classical information theory. Finally, in Section 4, the final discussion are drawn.

## 2. Review of Matroid Theory

In this section, we review basic concepts and results in matroid theory necessary for the development of this note. The following results can be found in [17, 19].

**Notation.** We consider that $q$ is a prime power, $F_q$ is a finite field with $q$ elements, $|\cdot|$ denotes the cardinality of a set, $V(k, F_q)$ denotes the $k$-vector space over $F_q$, $C(n, k)$ denotes a linear block code of length $n$ and dimension $k$, $M[A]$ denotes the vector matroid derived from the matrix $A$, $M(G)$ denotes the cycle matroid derived from the graph $G$.

**Definition 1.** (see [17]) A matroid $M$ is an ordered pair $(E, \mathcal{I})$ consisting of a finite set $E$ (ground set) and a collection $\mathcal{I}$ (independent sets) of subsets of $E$ satisfying the following three conditions:

(M1) $\emptyset \in \mathcal{I}$;

(M2) If $I \in \mathcal{I}$ and $I' \subset I$, then $I' \in \mathcal{I}$;

(M3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists an element $e \in I_1 - I_2$ such that $I_1 \cup e \in \mathcal{I}$, where $|\cdot|$ denotes the cardinality of a set.

A subset of $E$ that is not in $\mathcal{I}$ is called *dependent*. The minimal dependent sets are called circuits of $M$. The set of circuits of $M$ is denoted by $\mathcal{C}(M)$. A maximal independent set of a matroid $M$ is called *basis* or *base* of $M$ and denoted by $\mathcal{B}$. A multiset is a set that (can) contain repeated elements. Theorem 2 establishes relationships between matroid theory and error-correcting codes.

**Theorem 2.** (see [17]) *Let $E$ be the set of column labels of a matrix $A_{m\times n}$ over a field $F$, and let $\mathcal{I}$ be the set of subsets $X$ of $E$ for which the multiset of columns labeled by $X$ is linearly independent (LI) in $V(m, F)$. Then $(E, \mathcal{I})$ is a matroid.*

A matroid obtained from the matrix $A$, denoted by $M[A]$, is called *vector matroid* of $A$. Two matroids $M_1$ and $M_2$ are *isomorphic*, written $M_1 \cong M_2$, if

there exists a bijection $\psi$ from $E(M_1)$ to $E(M_2)$ such that, for all $X \subseteq E(M_1)$, $\psi(X)$ is independent in $M_2$ if and only if $X$ is independent in $M_1$. If a matroid is isomorphic to the vector matroid $M[D]$ of a matrix $D$ over a field $F$, then $M$ is said to be *representable over* $F$ or *$F$-representable*. $D$ is called a representation for $M$ over $F$.

**Theorem 3.** (see [17]) *Let $E$ be the set of edges of a graph $G$ and let $\mathcal{C}$ be the set of edge sets of cycles of $G$. Then $\mathcal{C}$ is the set of circuits of a matroid on $E$.*

A matroid obtained from a graph $G$ is called *cycle matroid* and denoted by $M(G)$. If a matroid $M$ is isomorphic to $M(G)$, then $M$ is called *graphic*.

**Theorem 4.** (see [17]) *If $G$ is a graph, then $M(G)$ is representable over every field.*

Let $M = (E, \mathcal{I})$ be a matroid and suppose that $X \subseteq E$. Let $\mathcal{I} \mid X = \{I \subseteq X : I \in \mathcal{I}\}$. Then the pair $(X, \mathcal{I} \mid X)$ is a matroid, denoted by $M \mid X$. We define the *rank* of $X$ to be the size of a base $B$ of $M \mid X$ (consequently, the size of all bases of $M \mid X$) and we call a set $B$ a basis of $X$. The rank function of $M$, denoted by $r_M$, is the function $r : 2^E \longrightarrow \mathbb{Z}^+$ such that, for each $X \subseteq E$, it associates the non-negative integer $r(X)$. The value $r(M)$ equals the size of a base of $M$. Let $r$ be the rank function of $M$. The *closure operator*, denoted by $cl$, is an application $cl : 2^E \longrightarrow 2^E$, for all $X \subseteq E$, defined by $cl(X) = \{x \in E : r(X \cup x) = r(X)\}$.

A partially ordered set (poset) is a (possibly infinite) set $P$ together with a binary relation $\leq$ such that, for all $x, y, z \in P$, one has: (i) $x \leq x$; (ii) if $x \leq y$ and $y \leq x$ hold then $x = y$; (iii) if $x \leq y$ and $y \leq z$ hold then $x \leq z$. If $x < y$ but there exists no element $z$ of $P$ such that $x < z < y$, then we say that $y$ *cover* $x$ in $P$. Let $P$ a finite poset. A *chain* in $P$ from $x_0$ to $x_n$ is a subset $\{x_0, x_1, \ldots, x_n\}$ of $P$ such that $x_0 < x_1 < \ldots < x_n$. The *length* of such a chain is $n$, and the chain is *maximal* if $x_i$ cover $x_{i-1}$ for all $i \in \{1, 2, \ldots, n\}$. If, for every pair $\{a, b\}$ of elements of $P$ with $a < b$, all maximal chains from $a$ to $b$ have the same length, then $P$ is said to satisfy the *Jordan-Dedekind chain condition*.

**Definition 5.** (see [17]) A lattice is a poset $\mathbb{L}$ such that, for every pair of elements, the least upper bound and the greatest lower bound of the pair exists. Formally, if $x$ and $y$ are arbitrary elements of $\mathbb{L}$, then $\mathbb{L}$ contains elements $x \vee y$ and $x \wedge y$, the *join* and *meet* of $x$ and $y$, such that

($L_1$) $x \vee y \geq x$ and $x \vee y \geq y$ hold; if $z \geq x$ and $z \geq y$ hold then $z \geq x \vee y$ holds;

($L_2$) $x \wedge y \leq x$ and $x \wedge y \leq y$ hold; if $z \leq x$ and $z \leq y$ hold then $z \leq x \wedge y$ holds.

If a poset $P$ has an element $z$ such that $z \leq x$, for all $x \in P$, then we call $z$ a *zero* of $P$ and denote it by 0. Similarly, if $P$ has an element $w$ such that $w \geq x$, for all $x \in P$, then $w$ is called the *one* of $P$. Suppose that $P$ is a poset having a zero. An element $x$ is called an *atom* of $P$ if $x$ covers 0. The *height* $h(y)$ of an element $y$ of $P$ is the maximum length of a chain from 0 to $y$. It is straightforward to see that every finite lattice has a zero and an one. If $M$ is a matroid, then $\mathbb{L}(M)$ denotes the set of flats of $M$ ordered by inclusion. In particular, the zero of $\mathbb{L}(M)$ is $cl(\emptyset)$, while the one is $E(M)$. According to these results, Lemma 6 classifies the set $\mathbb{L}(M)$.

**Lemma 6.** (see [17]) *$\mathbb{L}(M)$ is a lattice and, for all flats $X$ and $Y$ of $M$, we have $X \wedge Y = X \cap Y$ and $X \vee Y = cl(X \cup Y)$.*

A finite lattice $\mathbb{L}$ is *semimodular* if it satisfies the Jordan-Dedekind chain condition and, for every pair $x$ and $y$ of elements of $\mathbb{L}$, $h(x) + h(y) \geq h(x \vee y) + h(x \wedge y)$. A *geometric lattice* is a finite semimodular lattice in which every element is a join of atoms. Theorem 7 characterizes geometric lattices:

**Theorem 7.** (see [17]) *A lattice $\mathbb{L}$ is geometric if and only if it is the lattice of flats of a matroid.*

Let us recall two well-known results in coding theory (see, for instance, [16, 18]):

**Corollary 8.** *Let $C(n,k)$ be a linear block code with parity-check matrix $H$. Then $C(n,k)$ has minimum weight (and hence minimum distance) at least $d$ if and only if every combination of $d-1$ or fewer columns of $H$ is linearly independent.*

**Corollary 9.** *Let $C(n,k)$ be a linear code with parity-check matrix $H$. The minimum weight (and hence minimum distance) of $C(n,k)$ equals to the smallest number of linearly dependent columns of $H$.*

Theorem 10 is well-known in the literature:

**Theorem 10.** *Let $C(n,k)$ be a linear block code with parity-check matrix $H_{n-k,n}$. Let $E = \{1, 2, \ldots, n\}$ be the set of labels of the $n$ columns of $H$ and let $\mathcal{I}$ be the set of column labels of $H$ such that the respective vectors are linearly independents over $V(n-k, F_q)$. Then, the ordered pair $(E, \mathcal{I})$ is the vector matroid of the matrix $H$ over $F_q$. Conversely, if $M$ is a $F_q$-representable matroid of a matrix $A_{m \times n}$, such that the rows of $A$ are linearly independent*

*vectors over $V(n, F_q)$, then the matroid $M(E,(I))$ gives rise to a parity-check matrix of a linear block code $C(n, n-m)$.*

The matroid derived from the code $C(n,k)$ will be denoted by $M_C$. Conversely, a code $C(n,k)$ derived from a matroid $M$ will be denoted by $C_M$.

**Remark 11.** Given a $C(n,k)$ block code, the corresponding matroid $M_C$ does not depend on the choice of the parity-check matrix $H$.

**Remark 12.** We can always suppose that the rows of $A_{m\times n}$ that generate the vector matroid $M[A]$ are linearly independents, otherwise one can make elementary operations with rows and columns of matrix $A$, that remain unchanged the vector matroid $M[A]$ (see [17] Section 2.2, Properties 2.2.1 - 2.2.6).

Theorem 13 is well-known; it is an alternative method to compute the minimum distance of a linear block code.

**Theorem 13.** *Let $C(n,k)$ be a block code with parity-check matrix $H$ and let $M_C$ be the matroid derived from $C(n,k)$. Suppose $\mathcal{C}$ is a circuit of $M_C$ of smallest cardinality among all circuits of $M_C$. Then one has $d_{min} = c$, where $d_{min}$ is the minimum distance of $C(n,k)$.*

## 3. The Results

This section is devoted to present the results of this note. More precisely, Subsection 3.1 presents a novel proof by means of matroid theory for the fact that the minimum distance of a graph-theoretic code $C$ is the smallest number of edges among all edge sets of cycles of $G$, the graph arising $C$; Subsection 3.2 presents new relationships between matroids and classical information theory.

### 3.1. Matroid and graph-theoretic codes

We suppose the reader is familiar with the theory of graph-theoretic codes. For more details we refer to [12, 11, 1, 7, 8].

Let $G = (V, E)$ (or $G$ for short) be a graph, where $V$ is the vertex-set and $E$ is the edge-set of $G$. Let $T$ be a tree of $G$, i. e., a maximal set of edges containing no circuits. Then the nullity of $G$, denoted by $N(G)$, is equal to the number of edges containing in the complement of $T$. It is well-known that the fundamental circuit (or cut-set) matrix of $G = (V, E)$ generates a binary block code of length $n$, dimension $k$ and minimum distance $d$, i. e., an $(n, k, d)$ code, where $n$ is the number of edges in $G$, $k = N(G)$, and $d$ is the minimum number

of edges in a circuit (or cut set) in $G$. These codes are called *graph-theoretic codes*. Thus, the minimum distance of this class of codes is the smallest number of edges of a minimal cycle in the graph that arises the respective code. In the following we present a new proof of this result by applying matroid theory:

**Theorem 14.** *Let $G = (V, E)$ be a connected graph with $l$ edges and $n$ vertex. Then $G$ generates a linear block code $C(n, k)$ with minimum distance $d$, where $d$ is the smallest number of edges among all edge sets of cycles of $G$.*

*Proof.* In order to prove this theorem, consider $G = (V, E)$ be a connected graph with $l$ edges and $n$ vertex. By Theorem 3, it follows that there exists a matroid $M(G)$ associated with $G$ such that the set of circuits of $M(G)$ is the set of all edge sets of cycles of $G$. Moreover, from Theorem 4, $M(G)$ is $F$-representable, for all field $F$; in particular, $M(G)$ is $F_2$-representable. Then there exists a matrix $A_G$ over $F_2$ that represents $M(G)$. We can suppose that all rows of $A_G$ are linearly independents in $V(n, F_2)$, otherwise, we can realize elementary operations on rows and columns of $A_G$ that remain unchanged the matroid $M = M[A_G]$. Thus $M(G)$ is isomorphic to $M[A_G]$, i. e., $M(G) \cong M[A_G]$. Since all the rows of $A_G$ are linearly independents, $A_G$ can be considered as the parity-check matrix of a code $C(n, k)$ with minimum distance $d$. We claim that $d$ is the smallest number of edges among all edge sets of cycles of $G$.

To check this claim, note that since $M(G) \cong M[A_G]$ (as matroid) it follows that all circuits in $M(G)$ are sent to circuits in $M[A_G]$ by means of the isomorphism $f$ between $M(G)$ and $M[A_G]$. Thus the corresponding circuits have the same length. From Theorem 13, the minimum distance $d$ of the code $C(n, k)$ whose parity-check matrix is the matrix $A_G$ is the smallest length among the lengths of all circuits of $M[A_G]$. Since $M(G) \cong M[A_G]$ holds, from Theorem 3 it implies that $d$ is the smallest number of edges among all the edge sets of cycles of $G$, and the result follows. □

### 3.2. Matroid and classical information theory

We begin this subsection by defining some concepts and results on classical information theory. For more details we refer to [5].

Suppose $X$ be a random variable with alphabet $\mathcal{X}$ and probability mass function $p(x) = Pr\{X = x\}, x \in \mathcal{X}$.

**Definition 15.** (see [5]) The (Shannon) entropy $H(X)$ of a discrete random variable $X$ is defined by

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x),$$

where the log function is to the base 2.

More generally, we define the join related entropy of discrete random variables $X_1, X_2, \ldots, X_n$, with alphabets $\mathcal{X}_i$, $i = 1, 2, \ldots, n$, respectively, and the join distribution $p(x_1, x_2, \ldots, x_n)$ :

**Definition 16.** (see [5]) The join entropy $H(X_1, X_2, \ldots, X_n)$ of discrete random variables $(X_1, X_2, \ldots, X_n)$ with join distribution $p(x_1, x_2, \ldots, x_n)$ is defined as

$$H(X_1, X_2, \ldots, X_n) = - \sum_{x_1, x_2, \ldots, x_n} \sum_{y \in \mathcal{Y}} p(x_1, x_2, \ldots, x_n) \log p(x_1, x_2, \ldots, x_n).$$

Fujishige [9] and Dougherty *et al.* [6] presented a connection between matroid theory and classical information theory. More precisely, they proved that the rank function $r$ of a matroid and the entropy function $H$, both satisfy the polymatroidal axioms:

**Definition 17.** (see [17]) Let $S$ be a finite set and $f : 2^S \longrightarrow \mathbb{R}$ be a function. Conditions $(P1) - (P3)$ below are called *polymatroidal axioms* for $f$:

(P1) $f(\emptyset) = 0$;

(P2) If $A \subset B \subset S$ then $f(A) \leq f(B)$;

(P3) If $A, B \subset S$, then $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$;

(P4) If $A, B, C \subset S$, then $f(A \cup C) + f(B \cup C) \geq f(C) + f(A \cup B \cup C)$.

Theorem 18 is the main result of this subsection. It asserts that the height function of the lattice of a matroid satisfies the polymatroidal axioms:

**Theorem 18.** *Let $\mathbb{L}(M)$ be a set of flats of a matroid $M$ such that, for every $X, Y \in \mathbb{L}(M)$ one has $X \cup Y \in \mathbb{L}(M)$. Let $h$ be the height function of $\mathbb{L}(M)$. Then $h$ satisfies the polymatroidal axioms.*

*Proof.* We first note that, from Lemma 2.8, $\mathbb{L}(M)$ is a lattice. We next prove that the function $h$ satisfies the Axioms (P1)-(P3). It is clear that $h$ satisfies (P1) because the length of the empty chain is zero.

To prove (P2), assume that $X, Y \in \mathbb{L}(M)$ and $X \subset Y$ hold.
Let $C = \{0, X_1, X_2, \ldots, X_n = X\}$ be a chain of maximum length from 0 to $X$. Then one obtains

$$0 \subset X_1 \subset X_2 \ldots \subset X_n = X.$$

Since $X \subset Y$, one has two cases:

*Case 1.* If $Y$ cover $X$ then $C$ is a maximal chain from 0 to $Y$. Thus it implies that $h(Y) = h(X) + 1$, if $X \subsetneqq Y$ and $h(Y) = h(X)$ if $X = Y$. Therefore, $h(X) \leq h(Y)$ holds as well.

*Case 2.* If $Y$ does not cover $X$ then there exists at least a flat $Z \in \mathbb{L}(M)$ such that

$$0 \subset X_1 \subset X_2, \ldots \subset X_n = X \subset Z \subset Y,$$

so $h(X) < h(Y)$. Therefore, $h$ satisfies Axiom (P2).

Next we show that $h$ satisfies (P3). From Theorem 7, we know that $\mathbb{L}(M)$ is a geometric lattice. Since a geometric lattice is a finite semimodular lattice it follows that the function $h$ satisfies the following inequality

$$h(X) + h(Y) \geq h(X \vee Y) + h(X \wedge Y).$$

From hypothesis, if $X, Y \in \mathbb{L}(M)$ holds then $X \cup Y \in \mathbb{L}(M)$ holds and so, $X \cup Y = cl(X \cup Y)$, because $X \cup Y$ is a flat. Additionally, from Lemma 6, we know that $X \wedge Y = X \cap Y$ and $X \vee Y = cl(X \cup Y) = X \cup Y$ hold. Therefore one has $h(X) + h(Y) \geq h(X \cup Y) + h(X \cap Y)$, and the result follows. □

Proposition 19 shows that free matroids $U_{n,n}$ $(n \geq 1)$, i. e., matroids having no dependent sets, satisfy the property given in the hypothesis of the previous theorem, that is, if $X, Y \in \mathbb{L}(M)$ then $X \cup Y \in \mathbb{L}(M)$.

**Proposition 19.** *If $M = U_{n,n}$ is an uniform matroid then $X = cl(X)$ for all $X \subset E$.*

*Proof.* Since $M$ has only independent sets one has $X = cl(X)$ for all $X \subset E$. In fact, assume there exists an element $x \in E(M)$ satisfying $x \notin X$. Since $(X \cup x)$ is an independent set in $M$ then it is true that $r(X \cup x) =\mid X \cup x \mid= r(X) + 1$. Since $r(X \cup x) \neq r(X)$ holds, it follows that $x \notin cl(X)$ and so $cl(X) \subset X$. Because $X \subset cl(X)$ holds one obtains $X = cl(X)$, as required. □

**Corollary 20.** *The height function of a lattice of flats $\mathbb{L}(U_{n,n})$ of $U_{n,n}$ $(n \geq 1)$ satisfies the polymatroidal axioms.*

*Proof.* The result follows directly by applying Theorem 18. □

## 4. Notes and Comments

We have shown that the height function of the lattice of flats of suitable classes of matroids satisfies the polymatroidal axioms. Additionally, we have given a new proof for the well-known result concerning the minimum distance of graph-theoretic codes by applying matroid theory.

## Acknowledgments

We would like to thank professor Satoru Fujishige for valuable comments and Dr. J.H. Kleinschmidt for critical reading of the manuscript.

## References

[1] R.B. Ash, W.H. Kim, On realizability of a circuit matrix, *IRE Trans. on Circuit Theory* (1959), 1114-1118.

[2] A. Barg, The matroid of supports of a linear code, *Applicable Algebra in Engineering, Communication and Computing*, **8** (1997), 165-172.

[3] T. Britz, Extensions of the critical theorem, *Discrete Math.*, **305** (2005), 55-73.

[4] T. Britz, Higher support matroids, *Discrete Math.*, **307** (2007), 2300-2308.

[5] T.M. Cover, J.A. Thomas, *Elements of Information Theory*, Jonh Wiley and Sons (1991).

[6] R. Dougherty, C. Freiling, K. Zeger, Networks, matroids and non-Shannon information inequalities, *IEEE Trans. Inform. Theory*, **53** (2007), 55-72.

[7] G.D. Forney, Codes on graphs: normal realizations, *IEEE Trans. Inform. Theory*, **47** (2001), 520-548.

[8] G.D. Forney, Codes on graphs: Constraint complexity of cycle-free realizations of linear codes, *IEEE Trans. Inform. Theory*, **49** (2003), 1597-1610.

[9] S. Fujishige, Polymatroidal dependence structure of a set of a random variables, *Information and Control*, **39** (1978), 1949-1969.

[10] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Mathematics*, **55** (1976), 119-128.

[11] S.L. Hakimi, J.G. Bredeson, Graph theoretic error-correcting codes, *IEEE Trans. Inform. Theory*, **14** (1968), 584-591.

[12] S.L. Hakimi, H. Frank, Cut set matrices and linear codes, *IEEE Trans. Inform. Theory*, **11** (1965), 457.

[13] N. Kashyap, A decomposition theory for binary linear codes, *Submitted to IEEE Trans. Inform. Theory* (2006).

[14] N. Kashyap, Matroid pathwidth and code trellis complexity, *Submitted to SIAM Journal on Discrete Mathematics* (2007).

[15] S. Lin, D. J. Costello Jr., *Error Control Coding, Fundamentals and Applications*, Prentice-Hall (1983).

[16] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

[17] J.G. Oxley, *Matroid Theory*, Oxford University Press (1992).

[18] W.W. Peterson, W.J. Weldon Jr., *Error-Correcting Codes*, MIT Press (1972).

[19] D.J.A. Welsh, *Matroid Theory*, Academic Press, London (1976).

[20] H. Whitney, On the abstract properties of linear dependence, *Amer. J. Math.*, **57** (1935), 509-533.