Lattice-theoretic Characterization of Secret Sharing Representable Connected Matroids

A. N. Alekseychuk

Institute of Special Communication and Information Security,
National Technical University of Ukraine (KPI)

alex-crypto@mail.ru

Abstract. Necessary and sufficient conditions for a connected matroid to be secret sharing (ss-)representable are obtained. We show that the flat lattices of ss-representable matroids are closely related with well-studied algebraic objects called linear lattices. This fact implies that new powerful methods (from lattice theory and mathematical logic) for investigation of ss-representable matroids can be applied. We also obtain some necessary conditions for a connected matroid to be ss-representable. Namely, we construct an infinite set of sentences (like to Haiman's "higher Arguesian identities") which are hold in all ss-representable matroids.

Introduction. In this paper, we present a necessary and sufficient condition for a connected matroid to be ss-representable.

We assume that the reader is familiar with elementary properties of matroids and finite lattices (see [1, 2] for complete details), and also with previous works dealing with the characterization of ss-representable matroids (see [3 – 5] for a comprehensive survey).

In Section 1, we recall some definitions and known facts on matroids, lattices, and partitions. Our results are formulated and discussed in Section 2. Finally, in Section 3, the proof of our Main Theorem is given. The following results describing the structure of matroid representations by partitions that commute under the relative product will be published later.

1. Preliminaries. Let M be a connected matroid with ground set $P=\{1, 2, ..., n\}$, the rank function r, and the closure operator

$$A \mapsto \overline{A} = \{i \in P : r(A \cup \{i\}) = r(A)\},\ A \subseteq P$$

such that

$$\overline{\varnothing} = \varnothing,\ \overline{\{i\}} = \{i\}\ \textit{for all}\ i \in P. \tag{1}$$

Let's denote by $L(M)$ the lattice of *flats* (i.e., closed subsets) of M. The join and the meet of $A, B \in L(M)$ are defined as follows:

$$A \vee B = \overline{A \cup B},\ A \wedge B = A \cap B.$$

It is well known that $L(M)$ is a geometric (i.e., atomistic and submodular) lattice that uniquely determines the matroid M (the Bikhoff-Whitney theorem; see, for example [1], Ch. II). The submodular law means that for all $A, B \in L(M)$

$$r(A \vee B) + r(A \wedge B) \leq r(A) + r(B).$$

We say that (A, B) is a *modular pair* in the lattice $L(M)$ and write $A\mathrm{M}B$ if

$$r(A \vee B) + r(A \wedge B) = r(A) + r(B). \qquad (2)$$

Note that for every $A, B \in L(M)$ the equality (2) is equivalent to the following implication (see [2], Ch. IV):

$$\forall C \in L(M):\ C \subseteq B \Rightarrow C \vee (A \wedge B) = (C \vee A) \wedge B.$$

A matroid M is called *secret sharing representable* (*ss-representable*) if there exist a finite set Q of cardinality $q \geq 2$ and a set $S \subseteq Q^n$ such that for every $A = \{i_1, ..., i_k\} \subseteq P$

$$\#\{(a_1, ..., a_k) \in Q^k : a_1 = x_{i_1}, ..., a_k = x_{i_k} \ \mathit{for\ some}\ (x_1, ..., x_n) \in S\} = q^{r(A)}. \qquad (3)$$

In this case S is said to be an *ideal secret sharing scheme* (*ISSS*) (or an *almost affine code*) representing the matroid M.

The relation between ISSS and matroids was stated by Brikell and Davenport [6]. Note that the definition of ISSS given above is equivalent to its well-known ordinary definition (see [6, 7]).

Matúš [3] has introduced and studied representations of matroids by partitions.

Let's denote by Π_X the *partition lattice* of a finite set X. We identify a partition $\rho \in \Pi_X$ with the associated equivalence relation on X and write $x\rho y$ if x and y are in the same block (i.e., equivalence class) of ρ. For a equivalence relation $\rho \subseteq X^2$ let's denote by X/ρ the set of all ρ-equivalence classes; put $n(\rho) = \#(X/\rho)$ (the number of the blocks of the partition ρ). The kernel of a mapping $f : X \to Y$ is the equivalence relation

$$\ker f = \{(x, y) \in X^2 :\ f(x) = f(y)\}.$$

Recall that Π_X is a submodular lattice with respect to the partial order

$$\rho_1 \leq \rho_2 \ \Leftrightarrow\ \rho_1 \subseteq \rho_2 \ \mathit{in}\ X^2$$

(see [1], Ch. II). The greatest element of Π_X is $1_X = X^2$. We denote by $\rho_1 \vee \rho_2$ and $\rho_1 \wedge \rho_2$ respectively the join and the meet of partitions $\rho_1, \rho_2 \in \Pi_X$. The *relative product* of ρ_1 and ρ_2 is defined as follows:

$$\rho_1 \circ \rho_2 = \{(x, y) \in X^2 \mid \exists z \in X : x\rho_1 z,\ z\rho_2 y\}.$$

We say that two equivalence relations ρ_1 and ρ_2 *commute* if $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$.

The following statement is well known.

Lemma. *Let X be a finite set and $\rho_1, \rho_2 \in \Pi_X$. Then*

$$\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1 \ \Leftrightarrow\ \rho_1 \circ \rho_2 \in \Pi_X \ \Leftrightarrow\ \rho_1 \circ \rho_2 = \rho_1 \vee \rho_2.$$

In addition, ρ_1 and ρ_2 commute iff for every blocks U, U_1, U_2 of the partitions $\rho_1 \vee \rho_2, \rho_1, \rho_2$ respectively the following condition holds:

$$U_1, U_2 \subseteq U \Rightarrow U_1 \cap U_2 \neq \varnothing.$$

2. Main results. One of the open problems of secret sharing is the characterization of ss-representable matroids [3 – 7]. It is known that there exist non-ss-representable matroids [3, 8] but all linearly representable matroids (i.e., matroids that can be represented by a matrix over some finite field) are ss-representable [6].

The following theorem provides a necessary and sufficient condition for a connected matroid to be ss-representable.

Main Theorem (MT). *Suppose the connected matroid M satisfies the condition* (1). *Then M is ss-representable iff there exist a finite set X and a injective mapping $\varphi : L(M) \to \Pi_X$ such that for all $A, B \in L(M)$*

(a) $\varphi(A \vee B) = \varphi(A) \wedge \varphi(B)$;

(b) $A\mathrm{M}B \Rightarrow \varphi(A \wedge B) = \varphi(A) \circ \varphi(B)$.

The proof is given in Section 3.

It follows directly from (a), (b) that ss-representable martoids are closely related with linear lattices, which has been extensively studied since 1953 [9 – 15]. A lattice is called *linear* if it can be represented by a lattice of equivalence relations that commute under the relative product.

Let L be a finite lattice and L^* be the lattice dual to L. Then L^* is linear if there exists an injection $\varphi : L \to \Pi_X$ such that for all $A, B \in L$

(a′) $\varphi(A \vee B) = \varphi(A) \wedge \varphi(B)$;

(b′) $\varphi(A \wedge B) = \varphi(A) \circ \varphi(B)$.

Thus, the class of *ss*-representable matroids can be regarded as an extension of certain subclass of lattices dual to linear (see (b) and (b′)). It is not difficult to prove that if $L(M)^*$ is a linear lattice, then it is isomorphic to the lattice of subspaces of a finite-dimensional vector space over a finite field and the matroid M can be represented by the parity-check matrix of the Hamming code over this field.

An extensive class of sentences (*lattice implications* and *lattice identities*) valid in all linear lattices is known [9 – 11, 14, 15]. In many cases, a slight modification of these sentences allows to obtain some necessary conditions for a connected matroid to be ss-representable.

Example 1. A lattice L is called *Arguesian* if it satisfies

$$(a_0 \vee b_0) \wedge (a_1 \vee b_1) \leq a_2 \vee b_2 \;\Rightarrow\; c_2 \leq c_0 \vee c_1, \tag{4}$$

where $c_i = (a_j \vee a_k) \wedge (b_j \vee b_k)$ for $\{i, j, k\} = \{0, 1, 2\}$. It is known that every linear lattice is Arguesian [9, 10] but the converse is false [12].

Let $L = L(M)$, $a_i = A_i, b_i = B_i \in L(M)$, $i = 0, 1, 2$. Then the dual implication to (4) can be written as follows:

$$(A_0 \wedge B_0) \vee (A_1 \wedge B_1) \supseteq A_2 \wedge B_2 \;\Rightarrow\; \big((A_1 \wedge A_2) \vee (B_1 \wedge B_2)\big) \wedge$$

$$\wedge \big((A_0 \wedge A_2) \vee (B_0 \wedge B_2)\big) \subseteq (A_0 \wedge A_1) \vee (B_0 \wedge B_1)\,. \tag{5}$$

Corollary 1. *Suppose the connected ss-representable matroid M satisfies the condition* (1). *Then for all* $A_i, B_i \in L(M)$ ($i = 0, 1, 2$) *such that*

$$A_0 \mathrm{M} A_1,\; B_0 \mathrm{M} B_1,\; A_2 \mathrm{M} B_2 \tag{6}$$

the implication (5) *holds*.

The proof is straightforward: by MT, it is sufficient to prove that under the condition (6)

$$\varphi((A_0 \wedge B_0) \vee (A_1 \wedge B_1)) \leq \varphi(A_2 \wedge B_2)$$

implies

$$\varphi((A_0 \wedge A_1) \vee (B_0 \wedge B_1)) \leq \varphi\big((A_1 \wedge A_2) \vee (B_1 \wedge B_2)) \wedge ((A_0 \wedge A_2) \vee (B_0 \wedge B_2)\big).$$

The last statement can be verified directly draw on the conditions (a), (b).

Example 2. Haiman [11, 12] has introduced “higher Arguesian identities”:

$$a_0 \wedge \left(b_0 \vee \bigwedge_{i=1}^{m} (a_i \vee b_i) \right) \leq a_1 \vee \left((b_0 \vee b_1) \wedge \bigvee_{i=1}^{m} ((a_i \vee a_{i+1}) \wedge (b_i \vee b_{i+1})) \right) \tag{7}$$

(where $m \geq 2$ and all indexes are modulo $m+1$) which hold in all linear lattices. For the lattice $L(M)$, $a_0 = A_0 = \varnothing$, $B_0 = P$ (the ground set of matroid M), and $a_i = A_i, b_i = B_i \in L(M)$, $i = \overline{1,m}$, the dual identity to (7) is

$$\bigvee_{i=1}^{m}(A_i \wedge B_i) \supseteq A_1 \wedge B_m \wedge \left(\bigwedge_{i=1}^{m}((A_i \wedge A_{i+1}) \vee (B_i \wedge B_{i+1})) \right). \tag{8}$$

The next statement can be proved in the same way as Corollary 1.

Corollary 2. *Suppose the connected ss-representable matroid M satisfies the condition* (1). *Then for all* $A_i, B_i \in L(M)$ *such that* $A_i \mathrm{M} B_i$ $(i = \overline{1,m},\ m \geq 2)$ *the inclusion* (8) *holds.*

The list of such examples can be continued. Haiman [11] has developed a proof theory for implication valid in linear lattices and showed how to characterize it by an infinite set of universal Horn sentences (note that no finite set of such sentences can completely characterize linearity [12]). Haiman's proof theory was simplified by Finberg, *et. al.* [13]. Powerful methods for obtaining identities valid in all (or some) linear lattices are proposed by Mainetti and Yan [14, 15]. It seems likely that the complete "intrinsic" characterization of ss-representable matroids can be obtained by the extension of methods described in [11, 13 – 15] to the class of finite geometric lattices satisfies the conditions of MT.

3. Proof of Main Theorem. Suppose that the matroid M is ss-representable and let's denote by S an ISSS satisfying the condition (3). To construct an injection $\varphi : L(M) \to \Pi_X$ with the properties (a), (b) let's consider the partition representation of M described in [3].

Put $X = S$,

$$\pi_i = \ker f_i,\ i \in P, \tag{9}$$

$$\pi_A = \bigwedge_{i \in A} \pi_i,\ A \subseteq P, \tag{10}$$

where the mapping $f_i : X \to Q$ is defined as follows:

$$f_i(x_1,...,x_n) = x_i,\ (x_1,...,x_n) \in X .$$

It follows from (9), (10), and (3) that for all $A, B \subseteq P$

$$\pi_{A \cup B} = \pi_A \wedge \pi_B,\ A \subseteq B \Rightarrow \pi_A \supseteq \pi_B,\ n(\pi_A) = q^{r(A)}.$$

Thus (since $A \subseteq \overline{A}$ and $r(A) = r(\overline{A})$) we obtain that $\pi_A = \pi_{\overline{A}}$ for all $A \subseteq P$.

Let $A, B \in L(M)$ and $\pi_A = \pi_B$. We claim that $A = B$. Indeed, assume that there exists $i \in A \setminus B$; then

$$\pi_B = \pi_A \subseteq \pi_i \Rightarrow \pi_{B \cup \{i\}} = \pi_B \wedge \pi_i = \pi_B \Rightarrow n(\pi_{B \cup \{i\}}) = n(\pi_B).$$

On the other hand,

$$r(B \cup \{i\}) = r(B) + 1 \Rightarrow n(\pi_{B \cup \{i\}}) = q^{r(B)+1} = n(\pi_B)q.$$

Hence, $A \subseteq B$ and by symmetry $A = B$, which we had to proved.

Put

$$\varphi(A) = \pi_A, \ \ A \in L(M).$$

It follows from above that φ is an injective map of $L(M)$ to Π_X satisfying the condition (a).

Let now (A, B) be a modular pair in the lattice $L(M)$. Let us be prove that $\varphi(A \wedge B) = \varphi(A) \circ \varphi(B)$. By Lemma and the inclusions

$$\varphi(A \wedge B) \supseteq \varphi(A) \vee \varphi(B) \supseteq \varphi(A) \circ \varphi(B) \ (in \ X^2)$$

it is sufficient to prove that for all blocks U, U_1, U_2 of the partitions $\varphi(A \wedge B), \varphi(A), \varphi(B)$ respectively the following implication holds:

$$U_1, U_2 \subseteq U \Rightarrow U_1 \cap U_2 \neq \varnothing.$$

To prove this statement fix any blocks U, U_1 of the partitions $\varphi(A \wedge B), \varphi(A)$ respectively and let's calculate the number $N(U, U_1)$ of the blocks $U_2 \in X / \varphi(B)$ such that

$$U_2 \subseteq U \ and \ U_1 \cap U_2 \neq \varnothing. \tag{11}$$

Observe that there are exactly $N = q^{r(B) - r(A \wedge B)}$ blocks $U_2 \in X / \varphi(B)$ contained in U (see Prop. 2 in [7]). On the other hand, there is a one-to-one correspondence between the blocks $U_2 \in X / \varphi(B)$ satisfying the condition (11) and all blocks $\widetilde{U} \in X / \varphi(A \vee B)$ contained in U_1. Thus, it follows from Prop. 2 in [7] and the equality (2) that

$$N(U, U_1) = q^{r(A \vee B) - r(A)} = q^{r(B) - r(A \wedge B)} = N.$$

Therefore, all blocks $U_2 \in X / \varphi(B)$ contained in U satisfying the condition (11). This completes the proof of the last statement and so also that of validity of the condition (b).

Assume now that there exists an injection $\varphi : L(M) \to \Pi_X$ with the properties (a), (b). Let us prove that M is a ss-representable matroid.

Put

$$\pi_i = \varphi(\{i\}),\ i \in P,$$

$$\pi_A = \varphi(\overline{A}),\ A \subseteq P.$$

It is clear that

$$\pi_1 \neq \pi_\varnothing. \tag{12}$$

Observe that $(\overline{A}, \{i\})$ is a modular pair for all $A \subseteq P$ and $i \in P$. Thus, it follows from (a), (b) that

$$\pi_{A\cup\{i\}} = \pi_A,\ \mathit{if}\ \ i \in \overline{A};\ \pi_A \circ \pi_i = \pi_\varnothing,\ \mathit{if}\ \ i \notin \overline{A}. \tag{13}$$

We may assume, without loss of generality, that $\pi_\varnothing = 1_X$ (in the opposite case we can replace X by a block $U \in X/\pi_\varnothing$ that contains two or more blocks of the partition π_1 and put $\pi_A = \pi_A \cap U^2$, $\pi_i = \pi_i \cap U^2$ for all $A \subseteq P$, $i \in P$; the conditions (12), (13) remains true). Thus, we obtain from (12), (13) that

$$\pi_1 \neq 1_X, \tag{14}$$

$$n(\pi_{A\cup\{i\}}) = n(\pi_A),\ \mathit{if}\ \ i \in \overline{A}, \tag{15}$$

and (by Lemma)

$$n(\pi_{A\cup\{i\}}) = n(\pi_A)n(\pi_i),\ \mathit{if}\ \ i \notin \overline{A}. \tag{16}$$

Since the matroid M is connected it follows from (15), (16) that

$$n(\pi_1) = n(\pi_2) = \ldots = n(\pi_n). \tag{17}$$

Finally, put

$$Q_i = X/\pi_i,\ i \in P,\ Q = Q_1.$$

Fix any bijection $\alpha_i : Q_i \to Q$ and let's denote by x/π_i the π_i-equivalence class containing any $x \in X$ ($i \in P$). It follows directly from (14) – (17) that

$$S = \{(\alpha_1(x/\pi_1), \ldots, \alpha_n(x/\pi_n)) :\ x \in X\}$$

is an ISSS representing the matroid M. This completes the proof of MT.

References

1. M. Aigner, *Combinatorial Theory*, Springer, Berlin, 1979.
2. G. Birkhoff, *Lattice Theory*, 3rd edn, Amer. Math. Soc., Providense R.I., 1967.
3. F. Matúš, Matroid representations by partitions, *Discrete Math.* **203** (1999), 169 – 194.
4. J. Martí-Farré, C. Padró, On secret sharing schemes, matroids and polymatroids, *Cryptology ePrint Arhive*, Report **2006/077**, http: // eprint.iacr. org/2006/077.
5. Ch. Hsu, S.-L. Ng, X. Tang, On representable matroids and ideal secret sharing, *Cryptology ePrint Arhive*, Report **2010/232**, http: // eprint.iacr. org/2010/232.
6. E.F. Brickell, D.M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology* **4** (1991), 123 – 134.
7. J. Simonis, A. Ashikhmin, Almost affine codes, *Des. Codes Cryptogr.* **14** (1998), 179 – 197.
8. P.D. Seymour, On secret-sharing matroids, *J. Combin. Theory Ser. B*, **56** (1992), 69 – 73.
9. B. Jónsson, On represrentations of lattices, *Math. Scand.* **1** (1953), 193 – 206.
10. B. Jónsson, G. Monk, Representation of primary Arguesian lattices, *Pacific J. Math.* 30 (1969), 95 – 139.
11. M. Haiman, Proof theory for linear lattices, *Adv. Math.* **58**, No. 3 (1985), 209 – 242.
12. M. Haiman, Arguesian lattices which are not linear, *Bull.* (*New Series*) *Amer. Math. Sci.*, **16**, No 1 (1987), 121 – 123.
13. D. Finberg, M. Mainetti, G.-C. Rota, The logic of commuting equivalence relations, *Logic and Algebra*, (A. Ursini and P. Agliano, Eds.), Lecture Notes in Pure and Applied Mathematics, **180**, Dekker, New York, 1996.
14. M. Mainetti, C.H. Yan, Arguesian identities in linear lattices, *Adv. Math.* **144** (1998), 50 – 93.
15. M. Mainetti, C.H. Yan, Geometric identities in lattice theory, *J. Combin. Theory Ser. A.*, **91** (2000), 411 – 450.