Researches in Mathematics `https://vestnmath.dnu.dp.ua`

Res. Math. **31**(2), 2023, p. 8–13
doi:10.15421/242309

ISSN (Print) 2664-4991
ISSN (Online) 2664-5009

UDK 512.53

D. I. Bezushchak
Taras Shevchenko National University of Kyiv,
Kyiv 01033. *E-mail: bezushchak@gmail.com*

Matroids related to groups and semigroups

Abstract. Matroid is defined as a pair $(X, \mathcal{I})$, where X is a nonempty finite set, and $\mathcal{I}$ is a nonempty set of subsets of X that satisfies the Hereditary Axiom and the Augmentation Axiom. The paper investigates for which semigroups (primarily finite) S, the pair $(\widehat{S}, \mathcal{I})$ will be a matroid.

Key words: semigroup, matroid

Анотація. Матроїдом називається пара $(X, \mathcal{I})$, що складається з непустої скінченної множини X та непустої множини $\mathcal{I}$ підмножин множини X, де $\mathcal{I}$ задовольняє Аксіоми спадковості та поповнення. У роботі досліджується для яких напівгруп (насамперед скінченних) S пара $(\widehat{S}, \mathcal{I})$ буде матроїдом.

Ключові слова: напівгрупа, матроїд

MSC2020: Pri 20M75, Sec 20M99

1. Introduction

The concept of a matroid generalizes the notion of the family of all linearly independent subsets of a vector space. This concept was first introduced by G. Whitney in 1935. Matroids have since found numerous applications in various fields, including geometry, topology, combinatorial optimization, network theory, and coding theory; for more details, see [3].

Recall (see [1, 4]) that a *matroid* is defined as a pair $\mathbf{M} = (X, \mathcal{I})$, where X is a nonempty finite set, and $\mathcal{I}$ is a nonempty set of subsets of X that satisfies the following conditions:

(M1) *Hereditary Axiom*: if $Y \in \mathcal{I}$ and $Z \subseteq Y$, then $Z \in \mathcal{I}$;

(M2) *Augmentation Axiom*: if $Y, Z \in \mathcal{I}$ and $|Z| > |Y|$, then there exists an element $z \in Z \setminus Y$ such that $Y \cup \{z\} \in \mathcal{I}$.

The set X is called the *base* of the matroid $\mathbf{M} = (X, \mathcal{I})$, and the elements of the family $\mathcal{I}$ are called the *independent sets* of the matroid. A consequence of axiom (M2) is that all maximal independent sets of the matroid have the same cardinality. These maximal independent sets of a matroid are called *bases*, and their cardinality is called the *rank* of the matroid.

Now, let's consider a semigroup S. For convenience, we define the empty subset as a subsemigroup of S, generated by an empty set of generators. We denote the set $\widehat{S}$ as follows: if the semigroup S contains the unit e and nontrivial inverse elements, then $\widehat{S}$ is defined as $S \setminus e$; otherwise, it is simply equal to S itself when considering the opposite direction. A subset $M \subseteq \widehat{S}$, which serves as an irreducible system of generators for the subsemigroup $\langle M \rangle \subseteq S$, is called independent. The collection of all independent subsets $M \subseteq \widehat{S}$, including the empty set, is denoted by the symbol $\mathcal{I}$.

We are exploring the following questions: under what conditions, primarily for finite semigroups S, does the pair $(\widehat{S}, \mathcal{I})$ constitute a matroid?

A semigroup S for which the pair $(S, \mathcal{I})$ forms a matroid will be referred to as *matroidal*.

2. Main results

Note that the pair $(\widehat{S}, \mathcal{I})$ always satisfies the Hereditary Axiom (M1). Therefore, it is only necessary to verify the fulfillment of the Augmentation Axiom (M2).

Example 1. Let G be a finite elementary abelian p-group. Then G can be considered as a finite-dimensional vector space over the field $\mathbb{Z}_p$, and the subgroups of the group G can be regarded as subspaces. A set $M \subseteq G$ will be independent if and only if it is linearly independent. Therefore, in this case $\mathcal{I}$ coincides with the set of all linearly independent subsets of G, and the pair $(G, \mathcal{I})$ forms what is known as a matrix matroid *([1, 4])*.

Example 2. Let S be a semigroup of left or right zeros *([2])*. In this case, every subset $M \subseteq S$ will be a subsemigroup. Hence, $\mathcal{I}$ coincides with the set of all subsets of S and the pair $(S, \mathcal{I})$ forms what is known as a discrete matroid.

From the fact that for an arbitrary matroid $(X, \mathcal{I})$ its restriction $(Y, \mathcal{J})$ with $\mathcal{J} = \{A \cap Y \mid A \in \mathcal{I}\}$ on a subset $Y \subseteq X$ is also a matroid, it follows that:

Proposition 1. Every subsemigroup of a matroidal semigroup is matroidal.

Example 3. A free group is not matroidal. For instance, consider a free group of rank 1 which is isomorphic to $(\mathbb{Z}, +)$. It has irreducible systems of generators of arbitrary finite cardinality, such as sets $\{2, 3\}$ and $\{6, 10, 15\}$. However, for these two sets, the Augmentation Axiom (M2) is not satisfied. The non-matroidal nature of free groups of rank ≥ 2 can now be inferred from Proposition 1.

Example 4. A free semigroup is not matroidal. Let's consider the free semigroup $\langle a\rangle$ and subsets $A = a^2, a^3$ and $B = a^3, a^5, a^7$, which are irreducible systems of generators of subsemigroups $\langle A\rangle$ and $\langle B\rangle$, respectively, with $|A| < |B|$. However, because $\langle B\rangle \subset \langle A\rangle$, it follows that the Augmentation Axiom (M2) is not satisfied. The non-matroidal nature of non-cyclic free semigroups can be deduced from Proposition 1.

Theorem 1. *For a rectangular lattice $S = I \times J$, the pair $(S, \mathcal{I})$ forms a matroid if and only if the cardinality of at least one of the sets I or J does not exceed* 2.

Proof. For any subset $A \subseteq S$, we denote the projections of A onto the first and second coordinates as $\mathrm{pr}_I A$ and $\mathrm{pr}_J A$, respectively. From the multiplication rule

$$(a, b)(c, d) = (a, d),$$

it follows that $\langle A\rangle = \mathrm{pr}_I A \times \mathrm{pr}_J A$.

Necessity. Let $I = \{1, 2, \ldots, m\}$, $J = \{1, 2, \ldots, n\}$, where m and n are both greater than 2. It can be easily verified that each of the sets $A = \{(1, 1), (2, 2), (3, 3)\}$ and $B = \{(1, 1), (2, 2), (2, 3), (3, 1)\}$ will be an irreducible system of generators of the subsemigroup $T = \{1, 2, 3\} \times \{1, 2, 3\}$. However, it is evident that each of the sets $A \cup \{(2, 3)\}$ and $A \cup \{(3, 1)\}$ will also be an irreducible system of generators of the subsemigroup T. Therefore, the Augmentation Axiom (M2) is not satisfied.

Sufficiency. It is sufficient to prove that the matroidal property holds for the rectangular lattice $S = I \times J$, where $I = \{1, 2, \ldots, n\}$, and either $J = \{1\}$ or $J = \{1, 2\}$.

In the first case, when $J = \{1\}$, S is a semigroup of right zeros, and therefore, it is matroidal.

Now, let's consider the case, where $J = \{1, 2\}$, and let $A \subseteq S$. If all elements from A lie in the same row (i.e., they have the same second component), then $\langle A\rangle = A$, and A is an irreducible system of generators.

Now, suppose $\mathrm{pr}_J A = \{1, 2\}$. If $|A| = 2$, then the set A is independent. However, if $|A| > 2$, then A is independent if and only if A does not contain two elements with the same first component. Indeed, if A contains elements $(a, 1)$, $(a, 2)$, and (b, c), then from the equation $(a, 3-c)(b, c) = (a, c)$, it follows that A is a reducible system of generators. On the other hand, if A does not contain two elements with the same first component, then $|A| = \mathrm{pr}_I A$, and from the equation $\langle A\rangle = \mathrm{pr}_I A \times \mathrm{pr}_J A$, it follows that A is an independent set.

Thus, the set $\mathcal{I}$ consists of those and only those subsets $A \subseteq S$ for which $|A| = \mathrm{pr}_I A$. It is evident that it satisfies both axioms of a matroid.

If we define multiplication on the set I to make it a semigroup of left zeros and multiplication on J to make it a semigroup of right zeros, then the rectangular lattice $I \times J$ becomes the direct product of the semigroups I and

J. Therefore, from Theorem 1 and Example 2, it follows that the class of matroidal semigroups is not closed under direct products.

Theorem 3: A cyclic group $C_n = \langle a \rangle$ of order n will be matroidal if and only if n is a power of a prime number.

Proposition 2. A cyclic group $C_n = \langle a \rangle$ of order n will be matroidal if and only if n is a power of a prime number.

Proof. *Necessity.* If the order of the group C_n is not a power of a prime number, then n can be factored into a product $n = mk$ of mutually prime numbers m and k. In this case, both $\{a\}$ and $\{a^k, a^m\}$ will be an irreducible system of generators for the group G. However, this pair of sets does not satisfy the Augmentation Axiom (M2).

Sufficiency. If n is a power of a prime number p, then the subgroups of the group $G = C_n$ form a chain by inclusion. From this, it follows that a subset $A \subseteq C_n$ will be independent if and only if it contains at least one element of order $|\langle A \rangle|$ and does not contain elements of larger order. Therefore, only one-element subsets from $\widehat{C_n}$ will be independent. It is evident that together with the empty subset, they form a matroid.

Proposition 3. A finite monogenic semigroup $S = \langle a \rangle$ will be matroidal if and only if none of its subsemigroups has an irreducible system of generators of cardinality ≥ 2.

Proof. It is obvious that if all irreducible systems of generators consist of single elements, then the semigroup is matroidal. On the other hand, S has a system of generators $\{a\}$ consisting of a single element. If some subsemigroup has an irreducible system of generators A of cardinality ≥ 2, then the pair $(\{a\}$, $A)$ does not satisfy the Augmentation Axiom (M2), so S is not matroidal.

Corollary 1. *Let p be a prime number. A monogenic semigroup $S = \langle a \rangle$ of (n, p) type will be matroidal if and only if $n < 4$, with the exception of the semigroup of $(3, 2)$ type.*

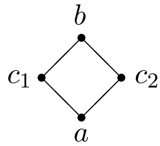
Proof. Monogenic semigroup of $(1, p)$ type coincides with a cyclic group C_p and is matroidal by Proposition 2.

Monogenic semigroup $S = \langle a \rangle$ of $(2, p)$ type takes the form $S = \{a, a^2, \ldots, a^{p+1}\}$ form, given that $a^{p+2} = a^2$. If a subset $A \subseteq S$ contains the element a, then $\langle A \rangle = S = \langle a \rangle$. Therefore, the only independent set among them will be $A = \{a\}$. If $a \notin A$, then $\langle A \rangle \subseteq \{a^2, \ldots, a^{p+1}\}$, which is a cyclic group of order p. As shown in the proof of Proposition 2, the irreducible systems of generators for this group consist of only one-element sets. Consequently, in this case, the set $\mathcal{I}$ consists of all subsets of S with a cardinality of at most 1, making S matroidal.

A monogenic semigroup $S = \langle a \rangle$ of $(3, p)$ type takes the form $S = \{a, a^2, \ldots, a^{p+2}\}$, given that $a^{p+3} = a^3$. Similar to the previous cases, the independent sets belonging to a cyclic subgroup $\{a^3, \dots, a^{p+2}\}$ of order p can only consist of single elements. A system of generators that includes the element a will be independent if and only if it consists of a single element. If $p > 2$, then $\langle a^2 \rangle = \{a^2, a^3, \dots, a^{p+2}\}$, and $\{a^2\}$ is the only independent set containing a^2. If $p > 2$, then in the semigroup of $(3, p)$ type, all independent sets consist of a single element. So, it is matroidal.

In a monogenic semigroup $S = \langle a \rangle$ of $(3, 2)$ type, a subsemigroup $\{a^2, a^3, a^4\}$ indeed has a system of generators consisting of two elements, specifically $\{a^2, a^4\}$. Then, by Proposition 3, it is not matroidal.

Any upper semilattice L can be considered as a semigroup with the operation $a * b = \sup(a, b)$. A four-element lattice with a Hasse diagram



is called a rhombus $\{a, b, c_1, c_2\}$.

Theorem 2. *A finite upper semilattice L with the operation $a * b = \sup(a, b)$ will be matroidal if and only if L is a chain or obtained from a chain by replacing some two-element intervals $[a, b]$ with rhombuses.*

Proof. *Sufficiency.* Let $L = \{a_0, a_1, \dots, a_n, c_1^{i_1}, c_2^{i_1}, \dots, c_1^{i_k}, c_2^{i_k}\}$, where $0 < i_1 < \dots < i_k \leq n$, and the elements $a_0, a_1, \dots, a_n$ form a chain $a_0 < a_1 < \dots < a_n$, and for each j, the set $\{aj - 1, a_j, c_1^j, c_2^j\}$ is a rhombus. A subset $A \subseteq L$ will be independent if and only if from each triple of elements of the form a_j, c_1^j, c_2^j, it contains no more than two elements.

Now, let A and B be independent subsets with $|A| < |B|$. If there exists a triple of elements a_j, c_1^j, c_2^j from some rhombus, such that A contains fewer elements than B, then we can add the element d from this triple, which belongs to $B \setminus A$, to A, and the set $A \cup \{d\}$ will remain independent.

However, if from each such triple, the sets A and B contain the same number of elements, then we will remove the elements of these triples from both A and B. The resulting sets A' and B' satisfy the inequality $|A'| < |B'|$, so $B' \setminus A' \neq \varnothing$. It is worth noting that $B' \setminus A' \subseteq B \setminus A$. Then, for any element $d \in B' \setminus A'$, the set $A \cup \{d\}$ will be independent.

Necessity. Let L be an upper semilattice for which the semigroup $(L, *)$ is matroidal. We will call an element b the successor of an element a if $a < b$ and the interval $[a, b]$ contains only 2 elements.

First, let's show that in L, each element has at most two successors. Suppose that pairwise distinct elements b_1, b_2, b_3 are successors of an element a. There are three possible cases:

1) The elements $b_1 * b_2$, $b_1 * b_3$, $b_2 * b_3$ are pairwise distinct. In this case, the elements b_1, b_2, b_3 generate a subsemigroup $\{b_1, b_2, b_3, b_1 * b_2, b_1 * b_3, b_2 * b_3, b_1 *$

$b_2 * b_3\}$ of order 7 in the semigroup $(L, *)$. It can be directly verified that the sets $\{b_1, b_1 * b_2, b_1 * b_2 * b_3\}$ and $\{b_3, b_1 * b_2, b_1 * b_3, b_2 * b_3\}$ are independent but do not satisfy the Augmentation Axiom (M2).

2) Two of the elements among $b_1 * b_2$, $b_1 * b_3$, $b_2 * b_3$ are the same. Without loss of generality, let us assume $b_1 * b_2 = b_1 * b_3$. In this case, the elements b_1, b_2, and b_3 generate a subsemigroup $\{b_1, b_2, b_3, b_1 * b_2, b_1 * b_2 * b_3\}$ of order 5 in $(L, *)$. It can be checked that the sets $\{b_1, b_1 * b_2, b_1 * b_2 * b_3\}$ and $\{b_3, b_1 * b_2, b_2 * b_3\}$ are independent but do not satisfy the Augmentation Axiom (M2).

3) All three elements among $b_1 * b_2$, $b_1 * b_3$, $b_2 * b_3$ are the same. In this case, the elements b_1, b_2, and b_3 generate a subsemigroup $\{b_1, b_2, b_3, b_1 * b_2 * b_3\}$ of order 4 in $(L, *)$. It can be checked that the sets $\{b_1, b_1 * b_2 * b_3\}$ and $\{b_1, b_2, b_3\}$ are independent but do not satisfy the Augmentation Axiom (M2).

Now, let's show that if an element a has two successors, then the interval $[a, b_1 * b_2]$ contains 4 elements. Suppose there is an intermediate element c between b_1 and $b_1 * b_2$. Then in the semigroup $([a, b_1 * b_2], *)$, the sets $\{b_1, c, b_1 * b_2\}$ and $\{b_2, b_1 * b_2\}$ are independent but do not satisfy the Augmentation Axiom (M2).

Therefore, if the semigroup $(L, *)$ is matroidal, then in the upper semilattice L, each element has at most two successors, and if an element a has two successors b_1 and b_2, then the interval $[a, b_1 * b_2]$ is a rhombus.

Let's show that if an element a has two successors b_1 and b_2, then each of the elements b_1 and b_2 has only one successor, which is $b_1 * b_2$. Suppose, for example, that element b_1 has another successor c. Then the elements b_1, b_2, c, $b_1 * b_2$, and $c * b_1 * b_2$ form a subsemigroup in the semigroup $(L, *)$. In this subsemigroup, the sets $\{c, c * b_1 * b_2\}$ and $\{b_2, b_1 * b_2, c * b_1 * b_2\}$ are independent but do not satisfy the Augmentation Axiom (M2).

Thus, if we take the upper semilattice L and remove the elements b_1 and b_2 from each rhombus $\{a, b_1, b_2, b_1 * b_2\}$, where b_1 and b_2 are successors of element a, the remaining elements will form a chain. This means that L is obtained from a chain by replacing certain two-element intervals with rhombuses.

Corollary 2. *An ordered by inclusion lattice L of subgroups of a finite abelian group G with the operation $a * b = \sup(a, b)$ will be matroidal if and only if G is a cyclic group of order p^k or pq, where p and q are distinct prime numbers.*

References

1. *Aigner M.*: Combinatorial Theory. Springer Verlag, 1996.
2. *Clifford A.H., Preston G.B.*: The Algebraic Theory of Semigroups. Vol. I. American Mathematical Soc., 1961.
3. *Neel D.L., Neudauer N.A.*: Matroids you have known. Mathematics Magazine 2009; 82(1): pp. 26–41. doi:10.4169/193009809X469020
4. *Wilson Robin J.*: Introduction to Graph Theory. Longman, 2010.

Received: 10.10.2023. *Accepted:* 13.12.2023