

GENERATING CRYPTOMORPHIC AXIOMATIZATIONS OF MATROIDS

G. Nicoletti
Istituto di Geometria
"L. Cremona"
Università di Bologna
(ITALIA)

There exist many ways to define equivalently (cryptomorphically) the concept of matroid (in his "Matroid Theory", D.J.A. Welsh writes: "Deciding which set of axioms would be the most natural to start with was difficult"). In this note I show a deep symmetry between these axiomatizations: in this symmetry the family of bases has a central role; it is possible to define recursively new families of sets which axiomatize cryptomorphically the concept of matroid.

A *matroid* is an ordered pair (S, I) , where $S \neq \emptyset$ is a finite set, and I is a collection of subsets of S such that:

- i1) $I_1 \in I, I_2 \subseteq I_1 \rightarrow I_2 \in I$; (I is a descending family of subsets of S);
- i2) $I \neq \emptyset$;
- i3) $\forall I_1, I_2 \in I, |I_1| < |I_2|, \exists x \in I_2 - I_1: I_1 \cup x \in I$.

The subsets in I are called *independent sets*. If $A \subseteq S$, the maximal independent sets contained in A have the same cardinality. Hence, we can define the *rank* of a subset A as follows:

$$r(A) := \max\{|I|; I \subseteq A, I \in I\};$$

the rank satisfies the following conditions:

- r1) $r(\emptyset) = 0$;
- r2) $r(A) \leq r(A \cup x) \leq r(A) + 1$;
- r3) $r(A \cup x) = r(A \cup y) = r(A) \rightarrow r(A \cup x \cup y) = r(A)$.

We have $I \in I \iff r(I) = |I|$.

The family of *bases* is the collection

$$\mathcal{B} := \{B \in I \mid B \text{ maximal}\}.$$

The family \mathcal{B} has the following properties:

- b1) $B_1, B_2 \in \mathcal{B}, B_1 \subseteq B_2 \rightarrow B_1 = B_2$; (\mathcal{B} is an antichain of subsets of S);
- b2) $\mathcal{B} \neq \emptyset$;
- b3) $\forall B_1, B_2 \in \mathcal{B}, \forall x \in B_1 \exists y \in B_2: (B_1 - x) \cup y \in \mathcal{B}$ (exchange axiom).

The bases have obviously the same cardinality, which is defined to be the *rank* of the matroid.

The independent sets are precisely all subsets of bases:

$$I = \{I \subseteq S \mid \exists B \in \mathcal{B}: I \subseteq B\}.$$

The family of *spanning sets* is the collection of all supersets of bases:

$$G := \{G \subseteq S \mid \exists B \in \mathcal{B}: I \subseteq B\};$$

the family G has the following properties:

- g1) $G_1 \in G, G_2 \supseteq G_1 \rightarrow G_2 \in G$; (G is an ascending family of subsets of S);
- g2) $G \neq \emptyset$;
- g3) $\forall G_1, G_2 \in G, |G_1| > |G_2|, \exists x \in G_1 - G_2: G_1 - x \in G$.

The bases are precisely the minimal spanning sets:

$$\mathcal{B} = \{G \in G \mid G \text{ minimal}\}.$$

Dependent sets are the subsets of S which are not independent sets; the family \mathcal{D} of all dependent sets satisfies the following properties:

- d1) $D_1 \in \mathcal{D}, D_2 \supseteq D_1 \rightarrow D_2 \in \mathcal{D}$; (\mathcal{D} is an ascending family of subsets of S);
- d2) $\emptyset \notin \mathcal{D}$;
- d3) $\forall D_1, D_2 \in \mathcal{D}: D_1 \cap D_2 \notin \mathcal{D} \rightarrow \forall x \in S: D_1 \cup D_2 - x \in \mathcal{D}$.

The minimal dependent sets are called *circuits*; the family \mathcal{C} of all circuits satisfies the following properties:

- c1) $C_1, C_2 \in \mathcal{C}, C_1 \subseteq C_2 \rightarrow C_1 = C_2$; (\mathcal{C} is an antichain of subsets of S);
- c2) $\emptyset \notin \mathcal{C}$;
- c3) $\forall C_1, C_2 \in \mathcal{C}, C_1 \neq C_2, \forall x \in S \exists C_3 \in \mathcal{C}: C_3 \subseteq C_1 \cup C_2 - x$.

Dependent sets are precisely all supersets of circuits:

$$\mathcal{D} = \{D \subseteq S \mid \exists C \in \mathcal{C}: C \subseteq D\}.$$

A subset A is called a *closed set* if $\forall x \notin A: r(A \cup x) = r(A) + 1$; a maximal closed set different from S is called a *hyperplane*. The family \mathcal{H} of all hyperplanes satisfies the following properties:

- h1) $H_1, H_2 \in \mathcal{H}, H_1 \subseteq H_2 \rightarrow H_1 = H_2$; (\mathcal{H} is an antichain of subsets of S);
- h2) $S \notin \mathcal{H}$;
- h3) $\forall H_1, H_2 \in \mathcal{H}, H_1 \neq H_2, \forall x \in S \exists H_3 \in \mathcal{H}: H_3 \supseteq (H_1 \cap H_2) \cup x$.

Circuits, dependent sets, independent sets, bases, spanning sets and hyperplanes can be used equivalently to axiomatize matroids: their respective axiom systems are given by the properties listed above. Now, we have three antichain of subsets of S , namely $\mathcal{C}, \mathcal{B}, \mathcal{H}$, two ascending families of subsets of S , namely \mathcal{D}, G , and only one descending family of subsets of S , namely I .

Now, the situation is the following:

- \mathcal{C} : circuits, or minimal dependent sets;
- \mathcal{D} : dependent sets, or supersets of circuits, or non-independent sets;
- I : independent sets, or non-dependent sets, or subsets of bases;
- \mathcal{B} : bases, or maximal independent sets, or minimal spanning sets;
- G : spanning sets, or supersets of bases.

What about hyperplanes and subsets of hyperplanes? It has been shown (M. Barnabei, G. Nicoletti: Axiomatizing Matroids by Means of the Set of Non-Generators, to appear