

Appendix of Matroid Cryptomorphisms

Thomas Brylawski

The following is a survey of 13 of the more common ways to describe matroids. In the first section, an axiomatization is given for each description. The axiom A0 is usually a nontriviality or normalization condition (such as, for bases, that the family is nonempty) to rule out degeneracy, and A1 describes a general mathematical structure (e.g., that bases form a clutter in that no two are comparable). Finally, A2 is the characteristic axiom (basis exchange in our example) that distinguishes the family of matroidal bases from other clutters (such as k -edge paths in a graph, maximal antichains in a poset, etc.).

As a comparison, consider point-set topology. There, for example, the characteristic axiom for the (topological) closure operator, cl , would be

$$\text{CL2}_T. \text{cl}(A \cup B) = \text{cl}(A) \cup \text{cl}(B)$$

(whereas the normalization axiom would be that $\bar{\emptyset} = \emptyset$).

Similarly, for the family $\mathcal{F}$ of closed sets, the topological axioms would be

F0_T. X and the empty set are closed.

F2_T. Finite unions of closed sets are closed.

Primed axioms, in general, can replace their unprimed counterparts to give an equivalent axiomatization. Thus, for example, bases can be axiomatized by B0, B1, B2, as well as by B0, B1, B2⁽⁵⁾, or by B0, B1', B2.

Note that, for example, B_1 and B_1' are not equivalent per se, but among families of subsets of X that obey B_0 and B_2 , they describe the same subclass of families. (In other words, B_0, B_1, B_2 together prove B_1' , and B_0, B_1', B_2 prove B_1 .) Note that bases give the largest number of equivalent axiomatizations from the apparently modest B_2 [basis exchange] to the apparently much stronger $B_2^{(2)}$ [symmetric subset exchange] to the (new) axiom $B_2^{(9)}$ [algorithmic duality]. We remark that B_2 and $B_2^{(2)}$ were proved equivalent for nonlinear matroids only in the 1970s. Note that the first three axiomatizations involve special structures (lattice, subset operator, and integer-valued function on subsets), and the final 10 all axiomatize special families of subsets of the groundset.

In the second section we give the matroid cryptomorphisms that relate one matroid structure in an invertible way with another. Some of these cryptomorphisms are quite general (such as those that relate a simplicial complex with its clutter of maximal elements, or a closure system in which each point is closed with a point lattice). These are the cryptomorphisms $f_{\mathcal{M} \rightarrow \mathcal{M}'}$ that can be generalized to those that pair structures axiomatized by A_0 and A_1 with structures axiomatized by A'_0 and A'_1 . Axiom A_2 is then interpreted in $\mathcal{M}'$ by axiom A'_2 . Other cryptomorphisms, however, are more subtle, so that, for example, general closure systems do not satisfy a chain condition, and thus a rank function such as that given by $f_{CL \rightarrow r}$ would not, in general, be well defined if the closure system obeyed only axioms CL_0 and CL_1 .

The reader is encouraged to show that primed axioms are equivalent to their unprimed counterparts or to prove that any of the cryptomorphism pairs $f_{\mathcal{M} \rightarrow \mathcal{M}'}$ and $f_{\mathcal{M}' \rightarrow \mathcal{M}}$ are inverses and do, indeed, prove one axiom system from the other. One can also develop one's own cryptomorphic theory of matroids [two recent examples have been by the family of nonspanning sets and by the boundary operator: $A \mapsto cl(A) \cap cl(X - A)$].

In conclusion, we interpret our cryptomorphic descriptions for four important classes of matroids (vector, affine, transversal, and graphic) and then give a sampling of when an axiom or cryptomorphism has a special version that characterizes binary matroids. Research problems here could include giving cryptomorphic descriptions for other classes (orientable matroids, gammoids, etc.) or describing a class of structures that obeys a particular weaker or stronger set of axioms. [A recent example of the former is the class of "greedoids" that satisfy a generalization to strings of $B_2^{(7)}$. An example of the latter is the class of matroids that satisfy bijective subset exchange (see footnote 11).]

In the following, we remind the reader that $B \supsetneq A$ means that the subset B properly contains A . Further, B covers A in the family $\mathcal{M}$, denoted $B \succ A$ if $B \supsetneq A$, but for no member C of $\mathcal{M}$ do we have that $B \supsetneq C \supsetneq A$. A similar definition of cover is used for lattices (posets) L , where *atoms* are lattice elements that cover the minimum element $\hat{0} \in L$.

AXIOMATIZATIONS FOR THE MATROID $M(E)$

- (1) *Geometric lattice* L : $f: E' \rightarrow A(L)$
- L0. f maps a subset E' (the *nonloops*) of E onto the atoms A of a lattice L .
- L1. [Point lattice] All elements of L are suprema of atoms.
- L1'. [Relative complementation] For all lattice elements c, d , and e , with $c < d < e$, there is $d' \in L$ such that $d' \vee d = e$ and $d' \wedge d = c$.
- L1''. No two join-irreducible elements of L are comparable ($c \in L$ is join-irreducible if $c = d \vee e$ implies $c = d$ or $c = e$).
- L2. [Semimodularity] There is a rank function ρ on L [$\rho(\hat{0}) = 0$, and $\rho(d) = \rho(c) + 1$ whenever $d \succ c$] such that for all $d, e \in L$,
- $$\rho(d) + \rho(e) \geq \rho(d \vee e) + \rho(d \wedge e).$$
- L2'. [Birkhoff covering property] If c and d both cover $c \vee d$, then $c \vee d$ covers both c and d .
- L2''. For all b, c , and d , if c covers or equals b , then $c \vee d$ covers or equals $b \vee d$.
- L2'''. [Atom modularity] If $a \succ \hat{0}$, then
- $$\rho(b) + \rho(a) = \rho(b \vee a) + \rho(b \wedge a).^1$$
- (2) *Closure operator*: $\text{cl}: 2^E \rightarrow 2^E$
- CL1. [Closure axioms]
- (a) [Increasing] $A \subseteq \text{cl}(A)$.
- (b) [Monotone] If $A \subseteq B$, then $\text{cl}(A) \subseteq \text{cl}(B)$.
- (c) [Idempotent] $\text{cl}[\text{cl}(A)] = \text{cl}(A)$.
- CL1'. (a) $A \subseteq \text{cl}(A)$.
- (b) If $A \subseteq \text{cl}(B)$, then $\text{cl}(A) \subseteq \text{cl}(B)$.
- CL1''. $A \cup \text{cl}[\text{cl}(A)] \subseteq \text{cl}(A \cup B)$.
- CL2. [MacLane-Steinitz exchange] If $x \in \text{cl}(A \cup \{y\}) - \text{cl}(A)$, then $y \in \text{cl}(A \cup \{x\})$.
- CL2'. If $\text{cl}(A) \subsetneq B \subseteq \text{cl}(A \cup \{x\})$, then $\text{cl}(B) = \text{cl}(A \cup \{x\})$.
- (3) *Rank function*: $r: 2^E \rightarrow \mathbb{Z}$
- R0. [Normalization] $r(\emptyset) = 0$.
- R1. [Unit rank increase] $r(A \cup \{x\}) = r(A)$ or $r(A) + 1$.
- R1'. $r(\{x\}) = 0$ or 1 for all $x \in E$.²

¹ We can add a converse to L2''' and obtain one axiom equivalent to both L1 and L2: $d \succ c$ if and only if $d = c \vee a$ for any element in the nonempty set of atoms $\{a: a \leq d, a \not\leq c\}$.

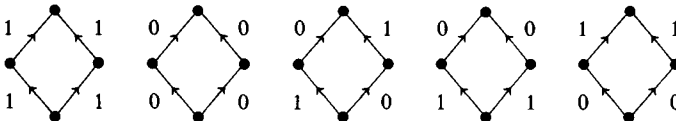
² R1 is implied by R0, R1', and R2 (or R2''), not by R0, R1', and R2'.

- R2. [Semimodularity] $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$.
 R2'. [Local semimodularity] If $r(A) = r(A \cup \{x\}) = r(A \cup \{y\})$, then $r(A \cup \{x, y\}) = r(A)$.
 R2''. If $A \supseteq B$, then $r(A) - r(B) \geq r(A \cup C) - r(B \cup C)$.³

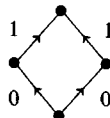
Families of Subsets of E

- (4) *Closed sets or flats:* $\mathcal{F}$
 F0. $E \in \mathcal{F}$.
 F1. [Closed-set family] If $F_1, F_2 \in \mathcal{F}$, then $F_1 \cap F_2 \in \mathcal{F}$.
 F2. If $F_1, \dots, F_k$ is the family of closed sets that cover F (i.e., each F_i contains F properly with no closed set between), then $F_1 - F, \dots, F_k - F$ partition $E - F$.
 F2'. $\cup\{F' : F' \supset F\} = E$.
 (5) *Hyperplanes:* $\mathcal{H}$
 H0. $E \notin \mathcal{H}$.
 H1. [Clutter; Incomparability] One hyperplane cannot properly contain another.
 H2. [Weak inclusion] For all distinct $H_1, H_2 \in \mathcal{H}$ and $x \in E$ there is a hyperplane H such that $(H_1 \cap H_2) \cup \{x\} \subseteq H$.
 H2'. [Strong inclusion] For all distinct hyperplanes H_1, H_2 , $x \notin H_1 \cup H_2$, and $y \in H_1 - H_2$, there exists $H \in \mathcal{H}$ such that $(H_1 \cap H_2) \cup \{x\} \subseteq H$ and $y \notin H$.
 (6) *Circuits:* $\mathcal{C}$
 C0. $\emptyset \notin \mathcal{C}$.
 C1. [Incomparability] One circuit cannot properly contain another.
 C2. [Weak elimination] $(C_1 \cup C_2) - \{x\}$ contains a circuit for all distinct circuits C_1 and C_2 , and $x \in E$.

³ The rank function is easily shown to be cryptomorphic to an *edge-labeled Boolean algebra*, where the edge (of the Hasse diagram)  is labeled by $r(A \cup x) - r(A)$. R1 is equivalent to having all squares labeled as follows:



R2 is equivalent to further eliminating



- C2'. If $I \subseteq E$ contains no circuit, then $I \cup \{x\}$ contains at most one circuit.
- C2''. [Strong elimination] For all circuits C_1 and C_2 with $x \in C_1 \cap C_2$ and $y \in C_1 - C_2$, there is a circuit C containing y such that $C \subseteq (C_1 \cup C_2) - \{x\}$.⁴
- C2'''. For all circuits $C_1, \dots, C_k$ such that, for all i , $C_1 \not\subseteq \bigcup_{j=1}^{i-1} C_j$, and for all $E' \subseteq E$ with $|E'| < k$, there is a circuit C such that $C \subseteq (\bigcup_{j=1}^k C_j) - E'$.⁵
- (7) *Bonds*: $\mathcal{C}^*$ are axiomatized the same as entry (6), Circuits.
- (8) *Open sets*: $\mathcal{O}$
- O0. $\emptyset \in \mathcal{O}$.
- O1. Unions of open sets are open.
- O2. For all open sets O_1 and O_2 , and $x \in O_1 \cap O_2$, there is an open set O such that
- $$(O_1 \cup O_2) - \{x\} \supseteq O \supseteq (O_1 \cup O_2) - (O_1 \cap O_2).$$
- O2'. (a) Every open set is a union of minimal (nonempty) open sets, and (b) for all $O_1 \neq O_2$, $x \in O_1 \cap O_2$, there is a nonempty open set $O \subseteq (O_1 \cup O_2) - \{x\}$.⁶
- O2''. If $O_1, \dots, O_k$ is the family of open sets covered by O then $\bigcap_{j=1}^k O_j = \emptyset$.
- (9) *Cycles*: $\mathcal{O}^*$ are axiomatized the same as entry (8), Open sets.
- (10) *Spanning sets*: $\mathcal{S}$
- S0. $E \in \mathcal{S}$ (or: S0'. $\mathcal{S} \neq \emptyset$).
- S1. [Order filter] If $S \in \mathcal{S}$ and $S' \supseteq S$, then $S' \in \mathcal{S}$.
- S2. If S and S' are spanning sets with $|S| = |S'| + 1$, then there is an element $x \in S - S'$ such that $S - \{x\}$ spans.⁷
- S2'. Minimal spanning sets containing a fixed subset $E' \subseteq E$ are equicardinal.
- (11) *Independent sets*: $\mathcal{I}$
- I0. $\emptyset \in \mathcal{I}$ (or: I0'. $\mathcal{I} \neq \emptyset$).

⁴ Weak elimination implies its strong counterpart directly only by a rather involved induction argument. However, the cryptomorphisms of the next section provide an alternate method of showing that C2 implies C2'. In particular, C0, C1, and C2 imply the independent-set axioms (using induction on $|I' - I|$ to prove I2). We then easily prove the rank-function axioms R0, R1, and R2. Finally, we use R0, R1, and R2' (an easy consequence of R2) to prove strong circuit elimination.

⁵ An important analogue of C2 that is a consequence of the circuit axioms (but does not imply C2) is *circuit transitivity*:

If $x \in C_1 - C_2$, $y \in C_2 - C_1$, and $z \in C_1 \cap C_2$, then there is a circuit $C \subseteq C_1 \cup C_2$ that contains both x and y . (It may or may not contain z .)

⁶ The family $\{\emptyset, x, y, xy, xyz\}$ shows that axiom O2'(b) alone does not imply O2.

⁷ Complementing the family in footnote 8, we see that we cannot remove the restriction that x be not in S' .

- I1. [Order ideal; Simplicial complex] If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.
- I2. If I and I' are independent sets, with $|I| = |I'| + 1$, then there is an element $x \in I - I'$ such that $I' \cup \{x\}$ is independent.⁸
- I2'. [Pure subcomplexes] For all $E' \subseteq E$, the maximal independent subsets of E' are equicardinal.
- (12) *Dependent sets:* $\mathcal{D}$
- D0. $\emptyset \notin \mathcal{D}$.
- D1. [Order filter] If $D \in \mathcal{D}$ and $D' \supseteq D$, then $D' \in \mathcal{D}$.
- D2. If D_1 and D_2 are dependent sets, then either $D_1 \cap D_2$ is dependent or $(D_1 \cup D_2) - \{x\}$ is dependent for all $x \in E$.
- D2'. If $I \notin \mathcal{D}$ but $I \cup \{x\}$ and $I \cup \{y\}$ are both in $\mathcal{D}$, then all $(|I| + 1)$ -element subsets of $D = I \cup \{x, y\}$ are dependent.⁹
- (13) *Bases:* $\mathcal{B}$
- B0. $\mathcal{B} \neq \emptyset$.
- B1. [Incomparability] One basis cannot properly contain another.
- B1'. [Equicardinality] All bases have the same size.
- B2. [Weak exchange] For all bases B and B' and $x \in B$, there is a $y \in B'$ such that $(B - x) \cup \{y\}$ is a basis.
- B2'. [Symmetric exchange] For all $B, B' \in \mathcal{B}$ and $x \in B$, there is a $y \in B'$ such that both $(B - x) \cup \{y\}$ and $(B' - y) \cup \{x\}$ are bases.¹⁰
- B2⁽²⁾. [Symmetric-subset exchange; Matroidal Laplace expansion] For all $B, B' \in \mathcal{B}$ and $A \subseteq B$, there is a subset $A' \subseteq B'$ such that $(B - A) \cup A'$ and $(B' - A') \cup A$ are both bases.
- B2⁽³⁾. [Bijective exchange] For all $B, B' \in \mathcal{B}$, there is a bijection $f: B \rightarrow B'$ such that $(B - x) \cup \{f(x)\}$ is a basis for all $x \in B$.¹¹
- B2⁽⁴⁾. [Dual exchange] For all $B, B' \in \mathcal{B}$, $y \in B' - B$, there is an $x \in B - B'$ such that $(B - x) \cup \{y\}$ is a basis.¹²

⁸ Weakening the stipulation $x \in I - I'$ in I2 by the statement $x \in I$ results in an axiom that does not imply I2, as is shown by the family $\{\emptyset, w, x, y, z, wx, wy, wz, xy, xz, yz, wxy\}$.

⁹ D2' is D2 with the restriction on the hypothesis that $|D_1 - D_2| = |D_2 - D_1| = 1$.

¹⁰ For both B2 and B2', we get an equivalent axiom by replacing "... $x \in B \dots y \in B'$..." with "... $x \in B - B' \dots y \in B' - B \dots$."

¹¹ Axiom B2⁽³⁾ is, in fact, equivalent to both B1 and B2. In general, we cannot combine B2' and B2⁽³⁾ to get bijective symmetric exchange {where both $(B - x) \cup \{f(x)\}$ and $(B' - f(x)) \cup \{x\}$ are bases}. The matroid of the complete graph K_4 does not satisfy bijective symmetric exchange. On the other hand, transversal matroids and their minors (*gammoids*) satisfy the stronger combination of B2⁽²⁾ and B2⁽³⁾: *bijective subset exchange*, where there exists a bijection $f: B \rightarrow B'$ such that $(B - A) \cup f(A)$ is a basis for all $A \subseteq B$.

¹² Axiom B2⁽⁴⁾, with "... $y \in B' - B \dots x \in B - B'$..." replaced by $\bar{B}2^{(4)}$ ("... $y \in B' \dots x \in B \dots$ ") is too weak. For example, the equicardinal family $\{xyu, xvy, xyw, uvx, uvv, uvw\}$ satisfies B2⁽⁴⁾ but not B2.

- B2⁽⁵⁾.** [Basis interpolation or Middle basis axiom] For all $I \subseteq B' \in \mathcal{B}$ and $S \supseteq B'' \in \mathcal{B}$, with $I \subseteq S$, there is a basis B such that $I \subseteq B \subseteq S$.
- B2⁽⁶⁾.** For any total order $<$ on E ($|E| = n$), associate the n -ary relation $\mathcal{B}^<$ with the family $\mathcal{B}$, where $(x_1, x_2, \dots, x_k, x_k, \dots, x_k) \in \mathcal{B}^<$ if $\{x_1, \dots, x_k\} \in \mathcal{B}$ and $x_i > x_{i+1}$ for all i . Then the lexicographically maximum member of $\mathcal{B}^<$ is also the componentwise maximum.¹³
- B2⁽⁷⁾.** The “greedy algorithm” gives the optimal member of $\mathcal{B}$: If $w: E \rightarrow \mathbb{R}$ is any assignment of weights giving $w(x_1) \geq w(x_2) \geq \dots \geq w(x_n)$, and if we define $w(B) = \sum_{x \in B} w(x)$, then $w(I_n) \geq w(B)$ for all $B \in \mathcal{B}$, where $I_0 = \emptyset$, and, for all i ,
- $$I_i = \begin{cases} I_{i-1} \cup \{x_i\} & \text{if this subset is contained in a basis,} \\ I_{i-1} & \text{otherwise.} \end{cases}^{14}$$
- B2⁽⁸⁾.** The “stingy algorithm” gives the optimal member of $\mathcal{B}$: If $w: E \rightarrow \mathbb{R}$ is any assignment of weights giving $w(x_1) \geq \dots \geq w(x_n)$, then $w(S_0) \geq w(B)$ for all $B \in \mathcal{B}$, where $S_n = E$, and, for $i = n-1, n-2, \dots, 0$,
- $$S_i = \begin{cases} S_{i+1} - \{x_{i+1}\} & \text{if this subset contains a basis,} \\ S_{i+1} & \text{otherwise.} \end{cases}$$
- B2⁽⁹⁾.** [Algorithmic duality] For all one-to-one assignments of weights, the greedy algorithm and the stingy algorithm return the same subset.¹⁵

CRYPTOMORPHISMS

In this section, for any matroid M described by the axiom system $\mathcal{M}$, we show how to get a structure that satisfies $\mathcal{M}'$. Using this *cryptomorphism* we can prove the axioms for $\mathcal{M}'$ from the axioms for $\mathcal{M}$. Often, but not always,

¹³ $(x_1, \dots, x_n) < (x'_1, \dots, x'_n)$ in the lexicographic order if for some k ($1 \leq k \leq n$), $x_k < x'_k$, while $x_i = x'_i$ for all $i < k$. $(x_1, \dots, x_n)$ is a componentwise maximum if $x_i \geq x'_i$ for all $(x'_1, \dots, x'_n) \in \mathcal{B}^<$ and all i . The least element of each basis is repeated to “fill out” the n -tuple. This convention is not necessary under the equicardinality assumption B1'.

¹⁴ If w is allowed to take on negative values, B2⁽⁷⁾ will imply B1 as well as B2. An equivalent axiom would result if we considered only one-to-one weight functions, in which case we would have the conclusion that $w(I_n) > w(B)$ for all $B \in \mathcal{B}$, $B \neq I_n$. This axiomatization, at the heart of algorithmic matroid theory, shows that if we have weighted subsets over a family known to be the bases of a matroid, we can find the maximum in time $O\{n[\log n + I(n)]\}$, where we sort in time $O(n \log n)$ and check independence in time $I(n)$.

¹⁵ Axiom B2⁽⁹⁾ is easily shown to imply the same axiom for the family $\mathcal{B}^*$ of complementary subsets and is therefore a good way to prove matroid duality. Similar “self-dual” axioms are B2' and B2⁽⁵⁾.

the i th axiom for $\mathcal{M}$ implies the i th axiom for $\mathcal{M}'$ ($i = 0, 1, 2$). Sometimes, however, the axioms for $\mathcal{M}$ are used to make the cryptomorphism well defined, and once it is, the axioms for $\mathcal{M}'$ follow easily.

Note that although it has little intuitive appeal, the rank function gives straightforward descriptions for all other axiomatizations.

We do not give cryptomorphic descriptions from open sets, spanning sets, or dependent sets, because matroids are seldom defined by these families. In addition, we do not present any cryptomorphisms to lattices, because most are quite awkward. [The only two natural ones are in terms of closed sets (L is obtained by ordering the members of $\mathcal{F}$ by inclusion) or hyperplanes (L is the infimum subsemilattice of the Boolean algebra 2^E generated by $\mathcal{H}$).] For cryptomorphisms in terms of the geometric lattice L , we assume that the matroid is a combinatorial geometry on the atoms of L .

The statement “(use $\mathcal{M}$)” in the $(\mathcal{M}, \mathcal{M}')$ coordinate in Table A.1 means that there is no natural way to go directly from $\mathcal{M}$ to $\mathcal{M}'$ without using an intermediate cryptomorphism: $\mathcal{M} \rightarrow \mathcal{M} \rightarrow \mathcal{M}'$. The most straightforward dual cryptomorphisms are mentioned in brackets: $[* \dots]$. Hence, $[*\text{Dual set}]$ in the $(7.\mathcal{C}^*, 6.\mathcal{C})$ coordinate means that the circuit family of M^* coincides with the bond family of M . Although these are not strictly cryptomorphisms, in that they do not relate one structural description of a matroid with another description of the same matroid, they do, for example, explain why circuits and bonds have the same axiom system.

PROTOTYPICAL EXAMPLES

We describe, where natural, each cryptomorphic description for the classes of vector matroids, affine matroids, transversal matroids, and graphical matroids. A check means that this example furnished the name of the cryptomorphism (such as circuits of graphs), and an arrow means that the corresponding axiom system is relatively easy to verify on the class. All matroids are on the set E .

Vector (or Linear)

E is the set of column vectors of an $r \times n$ matrix M' over the field F , where M' has linearly independent rows. $\hat{F}$ is a sufficiently large extension field of F .

1. L : $L(M)$ is the supremum semilattice of $\text{PG}(r-1, F)$ generated by the one-dimensional subspaces spanned by members of E .
- ✓ 2. cl: Linear closure $[\mathbf{x} \in \text{cl}(A) \text{ if } \mathbf{x} = \sum f_i \mathbf{a}_i, f_i \in F, \mathbf{a}_i \in A]$.
- ✓ 3. r : Linear rank $[r(A) \text{ is the size of a largest square nonsingular submatrix contained in the submatrix } A]$.
- ✓ 4. $\mathcal{F}$: Linearly closed subsets; subspaces of F^r intersected with E .

TABLE A.1

To define: In terms of:	2. Closure operator For all $A \subseteq E$, $\text{cl}(A) =$	3. Rank function $r(A) =$	4. Closed sets $F \in \mathcal{F}$ if	5. Hyperplanes $H \in \mathcal{H}$ if	6. Circuits $C \in \mathcal{C}$ if $C \neq \emptyset$ and
1. Lattice L (with atoms E)	$\{x \in E: x \leq \vee \{y: y \in A\}\}$	$\rho(\vee \{y: y \in A\})$, where ρ is the lattice rank (= length of a maximal chain from $\hat{0}$).	F is (the set of atoms below) some element in L	H is (the set of atoms below) some element covered by $\hat{1}$	The supremum semilattice generated by C is a (once) truncated Boolean algebra
2. Closure operator cl		(By recursion) if $A = B \cup \{x\}$, $r(B) + \begin{cases} 0 & x \in \text{cl}(B), \\ 1 & \text{otherwise.} \end{cases}$	$\text{cl}(F) = F$	$H \neq E$, and $x \notin H$ if and only if $\text{cl}(H \cup \{x\}) = E$	For $C' \subseteq C$, $\text{cl}(C') = C$ if and only if $ C - C' = 1$
3. Rank function r	$\{x: r(A) = r(A \cup x)\}$		$r(F \cup \{x\}) = r(F) + 1$ for all $x \notin F$	$r(H) = r(E) - 1 = r(H \cup \{x\}) - 1$ for all $x \notin H$ H is a maximal proper closed set	$r(C) = C - 1 = r(C - \{x\})$ for all $x \in C$ (Use cycles: add “ C is minimal such that” in 4 $\rightarrow$ 9)
4. Closed sets $\mathcal{F}$	$\cap \{F: F \supseteq A, F \in \mathcal{F}\}$	Maximum size of chain of closed sets, all properly contained in A			
5. Hyperplanes $\mathcal{H}$	$\cap \{H: H \supseteq A, H \in \mathcal{H}\}$ (where the empty intersection equals E)	$\text{cl}(\emptyset) - \text{cl}(A)$, where for $A \subseteq E$, $\text{cl}(A) = \max\{k: \text{there exist } H_1, \dots, H_k \in \mathcal{H} \text{ where for all } j, H_j \supseteq A, \text{ and } H_j \supseteq H_1 \cap \dots \cap H_{j-1}\}$	F is an intersection of hyperplanes		(Use cycles: add “ C is minimal such that” in 5 $\rightarrow$ 9) [*Dual complement]
6. Circuits $\mathcal{C}$	$\{x: x \in A, \text{ or there is a } C \in \mathcal{C} \text{ with } x \in C \subseteq A \cup \{x\}\}$	$ A - \max\{k: \text{there are } k \text{ circuits } C_1, \dots, C_k \text{ such that for all } j, C_j \subseteq A, \text{ and } C_j \not\subseteq C_1 \cup \dots \cup C_{j-1}\}$	$ C - F \neq 1$ for all $C \in \mathcal{C}$	(Use closed sets)	
7. Bonds $\mathcal{C}^*$	$E - \cup \{B: B \in \mathcal{C}^*, B \cap A = \emptyset\}$	(Use hyperplanes)	(Use hyperplanes)	H is the complement of a bond	(Use cycles: add “ C is minimal such that” in 7 $\rightarrow$ 9) [*Dual set]
9. Cycles $\mathcal{C}^*$	$\{x: x \in A, \text{ or there is a } C \in \mathcal{C}^* \text{ with } x \in C \subseteq A \cup \{x\}\}$	$ A - \max\{k: \emptyset \subsetneq C_1 \subsetneq C_2 \subsetneq \dots \subsetneq C_k \subseteq A\}$	$ C - F \neq 1$ for all $C \in \mathcal{C}^*$ [*Dual complement]	(Use closed sets)	C is a minimal cycle
11. Independent sets $\mathcal{I}$	$E - \{x: x \notin A \text{ and } I \cup \{x\} \in \mathcal{I} \text{ for all } I \in \mathcal{I}, I \subseteq A\}$	$\max\{ I : I \in \mathcal{I}, I \subseteq A\}$	$I \cup \{x\} \in \mathcal{I}$ whenever $I \subseteq F$, $I \in \mathcal{I}$, and $x \notin F$	(Use bases)	(Use dependent sets: add “ C is minimal such that” in 11 $\rightarrow$ 12)
13. Bases $\mathcal{B}$	(Use independent sets)	$\max\{ B \cap A : B \in \mathcal{B}\}$	(Use independent sets)	H is maximal with respect to containing no basis	(Use dependent sets: add “ C is minimal such that” in 13 $\rightarrow$ 12)

7. Bonds $B \in \mathcal{C}^*$ if $B \neq \emptyset$ and	8. Open sets $O \in \mathcal{C}$ if	9. Cycles $C \in \mathcal{C}^*$ if $C = \emptyset$ or	10. Spanning sets $S \in \mathcal{S}$ if	11. Independent sets $I \in \mathcal{I}$ if	12. Dependent sets $D \in \mathcal{D}$ if	13. Bases $B \in \mathcal{B}$ if
1. (Use hyperplanes)	(Use closed sets)	$x \leq \bigvee \{y: y \in C - \{x\}\}$ for all $x \in C$	$\hat{1} = \bigvee \{x: x \in S\}$	Suprema of subsets of I form a Boolean algebra	There is a redundancy among the suprema of subsets of D	Suprema of subsets of B form a Boolean algebra that includes $\hat{1}$
2. B is minimal such that $\text{cl}(E - B) \neq E$	$\text{cl}(E - O) = E - O$	$\text{cl}(C - x) = \text{cl}(C)$ for all $x \in C$	$\text{cl}(S) = E$	$x \notin \text{cl}(I - \{x\})$ for all $x \in I$	$x \in \text{cl}(D - \{x\})$ for some $x \in D$	$\text{cl}(B) = E \neq \text{cl}(B - x)$ for all $x \in B$
3. B is minimal such that $r(E - B) = r(E) - 1$	$r(E - O) = r[E - O] \cup x] - 1$ for all $x \in O$	$r(C - x) = r(C)$ for all $x \in C$	$r(S) = r(E)$	$r(I) = I $	$r(D) < D $	$r(B) = B = r(E)$
4. B is a minimal complement of a closed set	O is a complement of a closed set	$ C - F \neq 1$ for all $F \in \mathcal{F}$ [*Dual complement]	S is contained in no proper closed set	For every $x \in I$, $I - F = \{x\}$ for some $F \in \mathcal{F}$	There is an $x \in D$ such that $D - F \neq \{x\}$ for all $F \in \mathcal{F}$	(Use spanning sets: add " B minimal such that")
5. B is a hyperplane complement	(Use bonds)	$ C - H \neq 1$ for all $H \in \mathcal{H}$	S is contained in no hyperplane	For every $x \in I$, $I - H = \{x\}$ for some $H \in \mathcal{H}$	There is an $x \in D$ such that $D - H \neq \{x\}$ for all $H \in \mathcal{H}$	(Use spanning sets: add " B minimal such that")
6. (Use open sets: add " B is minimal such that" in 6 $\rightarrow$ 8) [*Dual set]	$ O \cap C \neq 1$ for all $C \in \mathcal{C}$	C is a union of circuits	For all $x \notin S$, there is a circuit C such that $x \in C \subseteq S \cup \{x\}$	I contains no circuit	D contains some circuit	(Use independent sets: add " B maximal such that")
7.	$O = \emptyset$, or O is a union of bonds	$ C \cap B \neq 1$ for all $B \in \mathcal{C}^*$	S meets every bond	For every $x \in I$, some bond intersects I in only x	There is an $x \in D$ such that no bond intersects D in only x	(Use spanning sets: add " B minimal such that")
9. (Use open sets: add " B is minimal such that" in 9 $\rightarrow$ 8) [*Dual set]	$ O \cap C \neq 1$ for all $C \in \mathcal{C}^*$ [*Dual set]		For all $A \subseteq E - S$, there is a cycle C such that $C - S = A$	I contains no nonempty cycle	D contains a nonempty cycle	(Use independent sets: add " B maximal such that")
11. (Use bases)	For all $x \in O$, and independent sets I disjoint from O , $I \cup \{x\}$ is independent	For all $x \in C$, there is a maximal independent subset I of C with $x \notin I$	Maximal independent subsets of S are maximal in E [*Dual complement]		D is not independent	B is a maximal independent set
13. B is minimal with respect to meeting every basis	(Use independent sets)	For all bases B and $x \in C \cap B$, there is a $y \in C - B$ such that $(B - \{x\}) \cup \{y\}$ is a basis	S contains some basis	I is contained in some basis	D is contained in no basis	[*Dual complement]

5. $\mathcal{H}$: Maximal subsets H of column indices such that the row space of M' contains a nonzero vector $\mathbf{v}$ whose zeros coincide with H . Equivalently, H is a maximal proper subset representable as the kernel of a linear functional $f: F^r \rightarrow F$ intersected with E .
- 6. $\mathcal{C}$: Minimal nonempty subsets C such that $\sum f_i \mathbf{c}_i = \mathbf{0}$, $f_i \in F - \{0\}$, $\mathbf{c}_i \in C$.
7. $\mathcal{C}^*$: Minimal supports of nonzero vectors in the row space of M' (see the foregoing item 5).
8. $\mathcal{O}$: Subsets O that index nonzero columns of NM' for some $d \times r$ matrix N . Equivalently, the supports of vectors in the row space of M' over the field $\hat{F}$.
9. $\mathcal{O}^*$: Subsets C such that there exist scalars $\hat{f}_i \in \hat{F} - \{0\}$ such that $\sum_{\mathbf{c}_i \in C} \hat{f}_i \mathbf{c}_i = \mathbf{0}$.
- ✓ 10. $\mathcal{L}$: Subsets S such that $\mathbf{x}_j = \sum_{\mathbf{s}_i \in S} f_{ij} \mathbf{s}_i$ for all $\mathbf{x}_j \in E$, and appropriate scalars $f_{ij} \in F$.
- ✓ 11. $\mathcal{I}$: Linearly independent subsets (subsets I such that if $\sum_{\mathbf{x}_i \in I} f_i \mathbf{x}_i = \mathbf{0}$, then $f_i = 0$ for all i).
- ✓ 12. Linearly dependent subsets (subsets D such that $\sum_{\mathbf{x}_i \in D} f_i \mathbf{x}_i = \mathbf{0}$, with $f_i \neq 0$ for some i).
- ✓ 13. $\mathcal{B}$: Vector bases (subsets B such that the columns B form a nonsingular matrix).

Affine Matroids

E is a set of distinct points in some affine space G (such as Euclidean space) of dimension $r - 1$ over a field F . Further E spans G in that it lies on no proper affine subspace. Here, E is a combinatorial geometry, and we shall assume that the point x has affine coordinates $\mathbf{x}$.

1. L : L is a supremum subsemilattice of $\text{AG}(r - 1, F)$.
- 2. cl : Affine closure [$x \in \text{cl}(A)$ if $\mathbf{x} = \sum_i f_i \mathbf{a}_i$, $f_i \in F$, $\mathbf{a}_i \in A$, $\sum_i f_i = 1$].
3. r : $r(A)$ is the size of a largest simplex contained in A ; it is 1 more than the dimension of the smallest affine flat containing A .
- ✓ 4. $\mathcal{F}$: Affine flats intersected with E .
- ✓ 5. $\mathcal{H}$: Subsets H such that for a unique $\bar{H}$, $H = \bar{H} \cap E$, where $\bar{H}$ is a hyperplane of G [i.e., $\bar{H} = f^{-1}(c)$ for $c \in F$, and f a nonzero linear functional].
6. $\mathcal{C}$: Three points on a line, four points on a plane no three on a line, $\dots$, $i + 2$ points in dimension i such that no smaller subset has this property. In Euclidean space they are subsets C with exactly one partition $C = C_1 \cup C_2$ whose parts have intersecting convex hulls. Analytically, they are minimal sets that satisfy the later item 12.
8. $\mathcal{O}$: (If F is large enough) Subsets O of E such that $O = \{x \in E: f(x) \neq c\}$ for some functional f and scalar c .
9. $\mathcal{O}^*$: Subsets C that are not cones (a cone is a subset $\{x\} \cup A$, where the apex x is not in the affine span of A).

10. $\mathcal{S}$: Sets of points that lie on no proper affine flat.
- 11. $\mathcal{J}$: Simplices (extreme points of a segment, triangle, tetrahedron, etc.).
- 12. $\mathcal{D}$: Sets of points D such that $\sum_{d_i \in D} f_i d_i = \mathbf{0}$ for scalars not all zero such that $\sum f_i = 0$.
13. $\mathcal{B}$: Spanning simplices.

Transversal Matroids

The transversal presentation is a relation $R \subseteq E \times Y$, where Y is matched by R^{-1} into E [i.e., $|Y| = r(E)$]. For a subset $A \subseteq E$, $R(A) = \{y \in Y: (x, y) \in R \text{ for some } x \in A\}$. $A \subseteq E$ is matched by R into Y' if $R \cap [A \times Y']$ contains $|A|$ vertex-disjoint edges.

2. cl : $x \in \text{cl}(A)$ if $x \in A$, or for some subset A' of A , A' is matched onto Y' , $R(A') = Y'$, and $R(x) \subseteq Y'$.
3. r : $r(A) = \min_{A' \subseteq A} (|A - A'| + |R(A')|) = \max_{A'' \subseteq A} [|A''|: A'' \text{ is matched into } Y]$.
4. $\mathcal{F}$: Flats that, as subgeometries, have isthmuses are not easily identified, but those that are also cycles are subsets F such that $F = R^{-1}[R(F)] = R^{-1}[R(F - \{x\})]$ for all $x \in F$.
5. $\mathcal{H}$: Cyclic hyperplanes are as in item 4, with the additional restriction that $|R(F)| = |Y| - 1$.
6. $\mathcal{C}$: Subsets C such that $|R(C)| = |C| - 1$, and $|R(C')| \geq |C'|$ for all $C' \subsetneq C$.
9. $\mathcal{O}^*$: See item 4.
10. $\mathcal{S}$: Subsets S that contain the image of a one-to-one function with domain Y contained in R^{-1} .
- 11. $\mathcal{J}$: Domains of one-to-one functions contained in R (subsets I matched into Y). Equivalently, subsets I such that $|J| \leq |R(J)|$ for all $J \subseteq I$.
12. $\mathcal{D}$: Sets D that contain a subset D' with $|D'| > |R(D')|$.
13. $\mathcal{B}$: Images of one-to-one functions with domain Y contained in R^{-1} . Equivalently, subsets B of size $|Y|$ such that $|B'| \leq |R(B')|$ for all $B' \subseteq B$. B is a system of distinct representatives for Y , where Y is viewed as the family $\{\dots, R^{-1}(y_i), \dots\}$ of subsets of E .

Graphs

The graph G with edge set E and vertex set V represents the matroid $M(E)$. Here, G is connected, and $|V| = r + 1$.

1. L : $L(M)$ is a supremum semilattice of the lattice Π_{r+1} of partitions of an $(r + 1)$ -element set.
2. cl : $\text{cl}(A) = \{x: x \text{ joins two vertices connected by a path in } A\}$.
3. r : $r(A) = r + 1 - c(A)$, where $c(A)$ is the number of connected components of V induced by the subgraph A .

4. $\mathcal{F}$: Subsets F such that, for some partition π of V , $x \in F$ whenever x connects two vertices in the same block of π .
5. $\mathcal{H}$: Maximal subsets H of edges such that the subgraph induced by H has two connected components.
- ✓ 6. $\mathcal{C}$: Polygons (closed simple paths).
- ✓ 7. $\mathcal{C}^*$: Minimal cut-sets of edges.
8. $\mathcal{O}$: Minimal sets of edges whose removal partitions the vertex-set into some partition π .
9. $\mathcal{O}^*$: Subsets of edges C such that for all $x \in C$, x is not a cut-set (isthmus) for the subgraph C .
- 10. $\mathcal{S}$: Subsets of edges that connect all the vertices.
- 11. $\mathcal{I}$: Forests.
- 13. $\mathcal{B}$: Spanning trees.

SPECIAL CRYPTOMORPHISMS CHARACTERIZING BINARY MATROIDS

In this section we give, for certain of the axioms in the first section of this appendix, a stronger version that identifies a structure as a binary matroid (a vector matroid over F_2). The first five axioms will be given in strong form:

A2_B. "For all n , $p(n)$."

Each such axiom is equivalent to its matroid (nonbinary) counterpart when n is set equal to 1, and, further, is equivalent (using A0 and A1) to the weaker version:

A2_{B'}. " $p(1)$ and $p(2)$."

For example, axiom B2' states the following (to characterize matroid basis families among all clutters): For all B , B' , and $x \in B$, if

$$|\{y \in B': (B - x) \cup \{y\} \text{ and } (B' - y) \cup \{x\} \text{ are bases}\}| = c,$$

then $c \neq 0$ (i.e., the foregoing set is nonempty). This is axiom B2_B (which is presented later) when $n = 1$. When $n = 2$, B2_B states (in its weak form) that a matroid M is binary if and only if c , the number of symmetric exchanges, is never equal to 2. The strong version of B2_B states that further, when M is binary, the number of symmetric exchanges is always odd (a consequence of the Laplace expansion formula for determinants over F_2).

A similar scheme holds for the eight binary cryptomorphisms that follow. For example, when $n = 1$, $f_{\mathcal{C} \rightarrow \mathcal{C}^*}^B$ is the usual $\mathcal{C} \rightarrow \mathcal{C}^*$ cryptomorphism that if $\mathcal{C}$ is the family of circuits of a matroid M , then $\mathcal{C}^*$, the family of minimal nonempty subsets B such that $|B \cap C| \neq 2 \cdot 1 - 1 = 1$ for all $C \in \mathcal{C}$, is the family of bonds of M . The matroid M is binary if and only if $|B \cap C| \neq 2 \cdot 2 - 1 = 3$ for all $B \in \mathcal{C}^*$, $C \in \mathcal{C}$. In addition, when M is binary, bonds

and circuits always intersect in an even number of points.¹⁶ Similar interpretations hold for the other cryptomorphisms.

When treating binary matroids, it is natural to define *binary* cycles and open sets. A *binary cycle* (respectively *binary open set*) is a *disjoint* union of circuits (respectively bonds). In the following, we shall use these specialized cycles and open sets.

Binary Axiomatizations

- CL_{2B}. [Binary closure] For all subsets $E' \subseteq E$, with $\{x_1, \dots, x_n\} \subseteq E'$, if $\{y, y'\} \subseteq \text{cl}(E') - \text{cl}(E' - \{x_i\})$ for $1 \leq i \leq n$, then $y' \in \text{cl}[(E' - \{x_1, \dots, x_n\}) \cup \{y\}]$.
- H_{2B}. If $A \cup \{x\}$ is contained in $n - 1$ hyperplanes, then A is contained in at most 2^{n-1} other hyperplanes.
- C_{2B}. If A contains $n - 1$ circuits, then $A \cup \{x\}$ contains at most 2^{n-1} additional circuits.
- B_{2B}. [Binary basis exchange] For all B, B' , and $x \in B$, $|\{y \in B': (B - x) \cup \{y\} \text{ and } (B' - y) \cup \{x\} \text{ are bases}\}| \neq 2n - 2$.
- B_{2B'}. [Binary basis subset exchange] For all B, B' , and $A \subseteq B$, $|\{A' \subseteq B': (B - A) \cup A' \text{ and } (B' - A') \cup A \text{ are bases}\}| \neq 2n - 2$.

Binary Cryptomorphisms

- $f_{\mathcal{C}^*, \emptyset^* \rightarrow \mathcal{C}^*}^B$. [Binary circuit-bond or cycle-bond cryptomorphism] Bonds are minimal nonempty subsets B such that $|B \cap C| \neq 2n - 1$ for all circuits (or binary cycles) C .
- $f_{\mathcal{C}^*, \emptyset \rightarrow \mathcal{C}^*}^B$. [Binary bond-circuit or open-set-circuit cryptomorphism] Circuits are minimal nonempty subsets C such that $|C \cap B| \neq 2n - 1$ for all bonds (or binary open sets) B .
- $f_{\mathcal{C}^*, \emptyset^* \rightarrow \emptyset}^B$. [Binary circuit-open-set or cycle-open-set cryptomorphism] Binary open sets are subsets O such that $|O \cap C| \neq 2n - 1$ for all circuits (or binary cycles) C .
- $f_{\mathcal{C}^*, \emptyset \rightarrow \emptyset^*}^B$. [Binary bond-cycle or open-set-cycle cryptomorphism] Binary cycles are subsets C such that $|C \cap B| \neq 2n - 1$ for all bonds (or binary open sets) B .

¹⁶ Actually, a stronger statement can be made. If $\mathcal{C}$ is a nonempty clutter (i.e., a family of subsets of E that satisfies C0 and C1), we can apply the cryptomorphism $f_{\mathcal{C} \rightarrow \mathcal{B}}$, obtaining the family $\mathcal{B}$ of maximal subsets of E that contain no $C \in \mathcal{C}$. From $\mathcal{B}$, we use $f_{\mathcal{B} \rightarrow \mathcal{C}^*}$ to get the family $\mathcal{C}^*$ of minimal subsets that meet every member of $\mathcal{B}$. Then $\mathcal{C}$, $\mathcal{B}$, and $\mathcal{C}^*$ are the circuits, bases, and bonds, respectively, of a matroid (respectively binary matroid) if and only if no member of $\mathcal{C}$ intersects a member of $\mathcal{C}^*$ in a singleton (or in a set of odd cardinality, respectively).

Other binary axiomatizations that do not fall into the foregoing scheme but do characterize when a matroid is binary include the following:

- L3_B. In the geometric lattice L , no interval of height two has greater than five elements.
- R3_B. [Binary rank function] For all subsets Z and Y such that $|Y| = 4$, if $r(Z \cup Y) = r(Z) + 2$, then $r(Z \cup Y_2) = r(Z) + 1$ for some two-element subset $Y_2 \subseteq Y$.
- F3_B. No four closed sets, each covering the same set, can be covered by a common closed set.
- H2_B. [Binary hyperplane inclusion] If H_1 and H_2 are distinct hyperplanes, then $(H_1 \cap H_2) \cup [E - H_1) \cap (E - H_2)]$ is an intersection of hyperplanes: $H'_1 \cap H'_2 \cap \dots \cap H'_m$ such that for $i \neq j$, $H'_i \cup H'_j = E$.
- C2'_B. [Binary circuit (or bond) elimination] The symmetric difference of two circuits is the disjoint union of circuits.
- C2''_B. If $C - C' (\neq C)$ is minimal among all nonempty circuit differences, then the symmetric difference of C and C' is a circuit.
- O2_B. [Binary open-set (or cycle) elimination] Binary open sets are closed under symmetric difference.