# 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

$$
\mathrm{CL} 2_{T} . \operatorname{cl}(A \cup B)=\operatorname{cl}(A) \cup \operatorname{cl}(B)
$$

(whereas the normalization axiom would be that $\bar{\varnothing}=\varnothing$ ).
Similarly, for the family $\mathscr{F}$ of closed sets, the topological axioms would be
$\mathrm{F0}_{T} . X$ and the empty set are closed.
$\mathrm{F}_{\boldsymbol{T}}$. 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 $\mathrm{B} 0, \mathrm{~B} 1, \mathrm{~B} 2$, as well as by $\mathrm{B} 0, \mathrm{~B} 1, \mathrm{~B}^{(5)}$, or by $\mathrm{B} 0, \mathrm{~B} 1^{\prime}, \mathrm{B} 2$.

Note that, for example, B1 and B1' are not equivalent per se, but among families of subsets of $X$ that obey B0 and B2, they describe the same subclass of families. (In other words, B0, B1, B2 together prove B1', and B0, B1', B2 prove B1.) Note that bases give the largest number of equivalent axiomatizations from the apparently modest $\mathbf{B} 2$ [basis exchange] to the apparently much stronger $\mathrm{B}^{2(2)}$ [symmetric subset exchange] to the (new) axiom $\mathrm{B} 2^{(9)}$ [algorithmic duality]. We remark that $\mathbf{B} 2$ and $\mathrm{B} 2^{(2)}$ 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 $f_{\mathcal{M} \rightarrow \boldsymbol{M}}$ that can be generalized to those that pair structures axiomatized by A0 and A1 with structures axiomatized by $\mathrm{A}^{\prime} 0$ and $\mathrm{A}^{\prime} 1$. Axiom A2 is then interpreted in $\mathscr{M}^{\prime}$ by axiom $\mathrm{A}^{\prime} 2$. 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 $f_{\mathrm{cL} \rightarrow r}$ would not, in general, be well defined if the closure system obeyed only axioms CL0 and CL1.

The reader is encouraged to show that primed axioms are equivalent to their unprimed counterparts or to prove that any of the cryptomorphism pairs $f_{\mathcal{M} \rightarrow \mathscr{M}^{\prime}}$ and $f_{\mathcal{M}^{\prime} \rightarrow \boldsymbol{M}}$ 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: $A \mapsto \mathrm{cl}(A) \cap \mathrm{cl}(X-A)]$.

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 $\mathrm{B} 2^{(7)}$. 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 $B \ni A$ means that the subset $B$ properly contains $A$. Further, $B$ covers $A$ in the family $\mathscr{M}$, denoted $B>A$ if $B \supsetneq A$, but for no member $C$ of $\mathscr{M}$ do we have that $B \supsetneq C \supsetneqq A$. 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: $f: E^{\prime} \rightarrow A(L)$

L0. fmaps a subset $E^{\prime}$ (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 $d^{\prime} \in L$ such that $d^{\prime} \vee d=e$ and $d^{\prime} \wedge d=c$.
L1" ${ }^{\prime \prime}$. 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 $\rho$ 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 $d$.
$\mathrm{L} 2^{\prime \prime}$. For all $b, c$, and $d$, if $c$ covers or equals $b$, then $c \vee d$ covers or equals $b \vee d$.
L2 ${ }^{\prime \prime \prime}$. [Atom modularity] If $a>0 \hat{0}$, then

$$
\rho(b)+\rho(a)=\rho(b \vee a)+\rho(b \wedge a) .^{1}
$$

(2) Closure operator: $\mathrm{cl}: 2^{E} \rightarrow 2^{E}$

CL1. [Closure axioms]
(a) [Increasing] $A \subseteq \operatorname{cl}(A)$.
(b) [Monotone] If $A \subseteq B$, then $\operatorname{cl}(A) \subseteq \operatorname{cl}(B)$.
(c) [Idempotent] $\mathrm{cl}[\mathrm{cl}(A)]=\operatorname{cl}(A)$.
$\mathrm{CL1}^{\prime}$. (a) $A \subseteq \operatorname{cl}(A)$.
(b) If $A \subseteq \operatorname{cl}(B)$, then $\operatorname{cl}(A) \subseteq \operatorname{cl}(B)$. $\mathrm{CL1}{ }^{\prime \prime}$. $A \cup \mathrm{cl}[\mathrm{cl}(A)] \subseteq \operatorname{cl}(A \cup B)$.
CL2. [MacLane-Steinitz exchange] If $x \in \operatorname{cl}(A \cup\{y\})-\operatorname{cl}(A)$, then $y \in \operatorname{cl}(A \cup\{x\})$.
$\mathrm{CL}^{\prime}$. If $\operatorname{cl}(A) \subsetneq B \subseteq \operatorname{cl}(A \cup\{x\})$, then $\operatorname{cl}(B)=\operatorname{cl}(A \cup\{x\})$.
(3) Rank function: $r: 2^{E} \rightarrow \mathbb{Z}$

R0. [Normalization] $r(\varnothing)=0$.
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 $\mathrm{L} 2^{\prime \prime \prime}$ and obtain one axiom equivalent to both L 1 and L 2 :
$d \succ c$ if and only if $d=c \vee a$ for any element in the nonempty set of atoms $\{a: a \leq d, a \nmid c\}$.
${ }^{2} R 1$ is implied by $\mathrm{R} 0, \mathrm{R1} 1^{\prime}$, and R 2 ( 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 $\boldsymbol{E}$

(4) Closed sets or flats: $\mathscr{F}$

F0. $E \in \mathscr{F}$.
F1. [Closed-set family] If $F_{1}, F_{2} \in \mathscr{F}$, then $F_{1} \cap F_{2} \in \mathscr{F}$.
F2. If $F_{1}, \ldots, F_{k}$ is the family of closed sets that cover $F$ (i.e., each $F_{i}$ contains $F$ properly with no closed set between), then $F_{1}-F, \ldots, F_{k}-F$ partition $E-F$.
$\mathrm{F}^{\prime} . \quad \cup\left\{F^{\prime}: F^{\prime}>F\right\}=E$.
(5) Hyperplanes: $\mathscr{H}$

H0. $E \notin \mathscr{H}$.
H1. [Clutter; Incomparability] One hyperplane cannot properly contain another.
H2. [Weak inclusion] For all distinct $H_{1}, H_{2} \in \mathscr{H}$ and $x \in E$ there is a hyperplane $H$ such that $\left(H_{1} \cap H_{2}\right) \cup\{x\} \subseteq H$.
$\mathrm{H}^{2}$. [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 $H \in \mathscr{H}$ such that $\left(H_{1} \cap H_{2}\right) \cup\{x\} \subseteq H$ and $y \notin H$.
(6) Circuits: $\mathscr{C}$

C0. $\varnothing \nsubseteq \mathscr{C}$.
C1. [Incomparability] One circuit cannot properly contain another.
C2. [Weak elimination] $\left(C_{1} \cup C_{2}\right)-\{x\}$ 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) $A \cup{ }_{A}^{x}$ is labeled by $r(A \cup x)-r(A)$. R 1 is equivalent to having all squares labeled as follows:


R2 is equivalent to further eliminating

$\mathrm{C}^{\prime}$. If $I \subseteq E$ contains no circuit, then $I \cup\{x\}$ contains at most one circuit.
$C 2^{\prime \prime}$. [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 $C \subseteq\left(C_{1} \cup C_{2}\right)-\{x\} .{ }^{4}$
$C 2^{\prime \prime \prime}$. For all circuits $C_{1}, \ldots, C_{k}$ such that, for all $i, C_{1} \nsubseteq$ $W_{i=1}^{i=1} C_{j}$, and for all $E^{\prime} \subseteq E$ with $\left|E^{\prime}\right|<k$, there is a circuit $C$ such that $C \subseteq\left(\bigcup_{j=1}^{k} C_{j}\right)-E^{\prime} .{ }^{5}$
(7) Bonds: $\mathscr{C}^{*}$ are axiomatized the same as entry (6), Circuits.
(8) Open sets: $\mathcal{O}$

O0. $\varnothing \in \mathcal{O}$.
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

$$
\left(O_{1} \cup O_{2}\right)-\{x\} \supseteq O \supseteq\left(O_{1} \cup O_{2}\right)-\left(O_{1} \cap O_{2}\right) .
$$

$\mathrm{O}^{\prime}$. (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 $O \subseteq\left(O_{1} \cup O_{2}\right)-\{x\}^{6}{ }^{6}$
$\mathrm{O}^{\prime \prime}$. If $O_{1}, \ldots, O_{k}$ is the family of open sets covered by $O$ then $\bigcap_{j=1}^{k} O_{j}=\varnothing$.
(9) Cycles: $\mathcal{O}^{*}$ are axiomatized the same as entry (8), Open sets.
(10) Spanning sets: $\mathscr{S}$

S0. $E \in \mathscr{T}$ (or: $\mathrm{SO}^{\prime} . \mathscr{S} \neq \varnothing$ ).
S1. [Order filter] If $S \in \mathscr{S}$ and $S^{\prime} \supseteq S$, then $S^{\prime} \in \mathscr{\mathscr { S }}$.
S2. If $S$ and $S^{\prime}$ are spanning sets with $|S|=\left|S^{\prime}\right|+1$, then there is an element $x \in S-S^{\prime}$ such that $S-\{x\}$ spans. ${ }^{7}$
S2'. Minimal spanning sets containing a fixed subset $E^{\prime} \subseteq E$ are equicardinal.
Independent sets: $\mathscr{I}$
I0. $\varnothing \in \mathscr{I}$ (or: $\mathrm{I}^{\prime}$. $\mathscr{I} \neq \varnothing$ ).
${ }^{4}$ 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 $\mathbf{C} 2$ implies $\mathrm{C}^{\prime \prime}$. In particular, $\mathrm{C} 0, \mathrm{C} 1$, and $\mathbf{C} 2$ imply the independent-set axioms (using induction on $\left|I^{\prime}-I\right|$ to prove $\mathbf{I 2}$ ). 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 $\{\varnothing, x, y, x y, x y z\}$ shows that axiom $\mathrm{O}^{\prime}(\mathrm{b})$ alone does not imply O 2 .
${ }^{7}$ Complementing the family in footnote 8 , we see that we cannot remove the restriction that $x$ be not in $S^{\prime}$.

I1. [Order ideal; Simplicial complex] If $I \in \mathscr{I}$ and $I^{\prime} \subseteq \mathrm{I}$, then $I^{\prime} \in \mathscr{I}$.
I2. If $I$ and $I^{\prime}$ are independent sets, with $|I|=\left|I^{\prime}\right|+1$, then there is an element $x \in I-I^{\prime}$ such that $I^{\prime} \cup\{x\}$ is independent. ${ }^{8}$
I2 ${ }^{\prime}$. [Pure subcomplexes] For all $E^{\prime} \subseteq E$, the maximal independent subsets of $E^{\prime}$ are equicardinal.

Dependent sets: $\mathscr{D}$
D0. $\varnothing \notin \mathscr{D}$.
D1. [Order filter] If $D \in \mathscr{D}$ and $D^{\prime} \supseteq D$, then $D^{\prime} \in \mathscr{D}$.
D2. If $D_{1}$ and $D_{2}$ are dependent sets, then either $D_{1} \cap D_{2}$ is dependent or $\left(D_{1} \cup D_{2}\right)-\{x\}$ is dependent for all $x \in E$.
D2'. If $I \notin \mathscr{D}$ but $I \cup\{x\}$ and $I \cup\{y\}$ are both in $\mathscr{D}$, then all $(|I|+1)$-element subsets of $D=I \cup\{x, y\}$ are dependent. ${ }^{9}$

Bases: $\mathscr{B}$
B0. $\mathscr{B} \neq \varnothing$.
B1. [Incomparability] One basis cannot properly contain another.
B1'. [Equicardinality] All bases have the same size.
B2. [Weak exchange] For all bases $B$ and $B^{\prime}$ and $x \in B$, there is a $y \in B^{\prime}$ such that $(B-x) \cup\{y\}$ is a basis.
B2'. [Symmetric exchange] For all $B, B^{\prime} \in \mathscr{B}$ and $x \in B$, there is a $y \in B^{\prime}$ such that both $(B-x) \cup\{y\}$ and $\left(B^{\prime}-y\right) \cup\{x\}$ are bases. ${ }^{10}$
B2 ${ }^{(2)}$. [Symmetric-subset exchange; Matroidal Laplace expansion] For all $B, B^{\prime} \in \mathscr{B}$ and $A \subseteq B$, there is a subset $A^{\prime} \subseteq B^{\prime}$ such that $(B-A) \cup A^{\prime}$ and $\left(B^{\prime}-A^{\prime}\right) \cup A$ are both bases.
B2 ${ }^{(3)}$. [Bijective exchange] For all $B, B^{\prime} \in \mathscr{B}$, there is a bijection $f: B \rightarrow B^{\prime}$ such that $(B-x) \cup\{f(x)\}$ is a basis for all $x \in B .^{11}$
$B 2^{(4)}$. [Dual exchange] For all $B, B^{\prime} \in \mathscr{B}, y \in B^{\prime}-B$, there is an $x \in B-B^{\prime}$ such that $(B-x) \cup\{y\}$ is a basis. ${ }^{12}$

[^0]B2 ${ }^{(5)}$. [Basis interpolation or Middle basis axiom] For all $I \subseteq B^{\prime} \in \mathscr{B}$ and $S \supseteq B^{\prime \prime} \in \mathscr{B}$, with $I \subseteq S$, there is a basis $B$ such that $I \subseteq B \subseteq S$.
$B 2^{(6)}$. For any total order < on $E(|E|=n)$, associate the $n$-ary relation $\mathscr{B}^{<}$with the family $\mathscr{B}$, where $\left(x_{1}, x_{2}, \ldots, x_{k}\right.$, $\left.x_{k}, \ldots, x_{k}\right) \in \mathscr{B}<$ if $\left\{x_{1}, \ldots, x_{k}\right\} \in \mathscr{B}$ and $x_{i}>x_{i+1}$ for all $i$. Then the lexicographically maximum member of $\mathscr{B}<$ is also the componentwise maximum. ${ }^{13}$
B2 ${ }^{(7)}$. The "greedy algorithm" gives the optimal member of $\mathscr{\mathscr { O }}$ : If $w: E \rightarrow \mathbb{R}$ is any assignment of weights giving $w\left(x_{1}\right) \geq$ $w\left(x_{2}\right) \geq \cdots \geq w\left(x_{n}\right)$, and if we define $w(B)=\sum_{x \in B} w(x)$, then $w\left(I_{n}\right) \geq w(B)$ for all $B \in \mathscr{B}$, where $I_{0}=\varnothing$, and, for all $i$,

$$
I_{i}=\left\{\begin{array}{l}
I_{i-1} \cup\left\{x_{i}\right\} \quad \text { if this subset is contained in a basis, } \\
I_{i-1} \text { otherwise. }{ }^{14}
\end{array}\right.
$$

$\mathrm{B2}^{(8)}$. The "stingy algorithm" gives the optimal member of $\mathscr{O}$ : If $w: E \rightarrow \mathbb{R}$ is any assignment of weights giving $w\left(x_{1}\right) \geq$ $\cdots \geq w\left(x_{n}\right)$, then $w\left(S_{0}\right) \geq w(B)$ for all $B \in \mathscr{B}$, where $S_{n}=E$, and, for $i=n-1, n-2, \ldots, 0$,

$$
S_{i}=\left\{\begin{array}{l}
S_{i+1}-\left\{x_{i+1}\right\} \quad \text { if this subset contains a basis, } \\
S_{i+1} \text { otherwise. }
\end{array}\right.
$$

$\mathrm{B}^{(9)}$. [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 $\mathscr{M}$, we show how to get a structure that satisfies $\mathscr{M}^{\prime}$. Using this cryptomorphism we can prove the axioms for $\mathscr{M}^{\prime}$ from the axioms for $\mathscr{M}$. Often, but not always,
${ }^{13}\left(x_{1}, \ldots, x_{n}\right)<\left(x_{1}^{\prime}, \ldots, x_{n}^{\prime}\right)$ in the lexicographic order if for some $k(1 \leq k \leq n), x_{k}<x_{k}^{\prime}$, while $x_{i}=x_{i}^{\prime}$ for all $i<k .\left(x_{1}, \ldots, x_{n}\right)$ is a componentwise maximum if $x_{i} \geq x_{i}^{\prime}$ for all $\left(x_{1}^{\prime}, \ldots, x_{n}^{\prime}\right) \in$ $\mathscr{B}^{<}$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 $\mathrm{B1}^{\prime}$.
${ }^{14}$ If $w$ is allowed to take on negative values, $\mathrm{B} 2^{(7)}$ will imply B 1 as well as B 2 . An equivalent axiom would result if we considered only one-to-one weight functions, in which case we would have the conclusion that $w\left(I_{n}\right)>w(B)$ for all $B \in \mathscr{B}, B \neq I_{n}$. 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 $\mathrm{B}_{2}{ }^{(9)}$ is easily shown to imply the same axiom for the family $\mathscr{B} *$ of complementary subsets and is therefore a good way to prove matroid duality. Similar "self-dual" axioms are $\mathrm{B}^{\prime}$ and $\mathrm{B}^{(5)}$.
the $i$ th axiom for $\mathscr{M}^{\text {implies }}$ the $i$ th axiom for $\mathscr{M}^{\prime}(i=0,1,2)$. Sometimes. however, the axioms for $\mathscr{M}$ are used to make the cryptomorphism well defined, and once it is, the axioms for $\mathscr{M}^{\prime}$ 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 $\mathscr{F}$ by inclusion) or hyperplanes ( $L$ is the infimum subsemilattice of the Boolean algebra $2^{E}$ generated by $\mathscr{H}$ ).] 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 $\mathscr{M})^{\prime}$ " in the $\left(\mathscr{M}, \mathscr{M}^{\prime}\right.$ ) coordinate in Table A. 1 means that there is no natural way to go directly from $\mathscr{M}$ to $\mathscr{M}^{\prime}$ without using an intermediate cryptomorphism: $\mathscr{M} \rightarrow \overline{\mathcal{M}} \rightarrow \mathscr{M}^{\prime}$. The most straightforward dual cryptomorphisms are mentioned in brackets: [*...]. Hence, [*Dual set] in the $\left(7 . \mathscr{C}^{*}, 6 . \mathscr{C}^{\circ}\right)$ 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 $M^{\prime}$ over the field $F$, where $M^{\prime}$ has linearly independent rows. $\hat{F}$ is a sufficiently large extension field of $F$.

1. $L: L(M)$ is the supremum semilattice of $\operatorname{PG}(r-1, F)$ generated by the one-dimensional subspaces spanned by members of $E$.
$\rightarrow \checkmark$ 2. cl: Linear closure $\left[\mathbf{x} \in \operatorname{cl}(A)\right.$ if $\left.\mathbf{x}=\sum f_{i} \mathbf{a}_{i}, f_{i} \in F, \mathbf{a}_{i} \in A\right]$.
2. $r$ : Linear rank $[r(A)$ is the size of a largest square nonsingular submatrix contained in the submatrix $A$ ].
3. $\mathscr{F}$ : Linearly closed subsets; subspaces of $F^{r}$ intersected with $E$.

| To define: <br> In terms of: | 2. Closure operator <br> For all $A \subseteq E, c(A)=$ | 3. Rank function $r(A)=$ | 4. Closed sets $F \in \mathscr{F}$ if | 5. Hyperplanes $H \in \mathscr{H}$ if | 6. Circuits <br> $C \in \mathscr{C}$ if $C \neq \varnothing$ and |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 1. Lattice $L$ (with atoms $E$ ) | $\{x \in E: x \leq \vee\{y: y \in A\}\}$ | $\rho(\vee\{y: y \in A\})$, where $\rho$ is the lattice rank ( $=$ length of a maximal chain from 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 $A=B \cup\{x\}$, $r(B)+ \begin{cases}0 & x \in \operatorname{cl}(B) \\ 1 & \text { otherwise } .\end{cases}$ | $\mathrm{cl}(F)=F$ | $\begin{aligned} & H \neq E \text {, and } x \notin H \text { if and only if } \\ & \quad \operatorname{cl}(H \cup\{x\})=E \end{aligned}$ | $\begin{gathered} \text { For } C^{\prime} \subseteq C, \operatorname{cl}\left(C^{\prime}\right)=C \text { if and } \\ \text { only if }\left\|C-C^{\prime}\right\|=1 \end{gathered}$ |
| 3. Rank function $r$ | $\{x: r(A)=r(A \cup x)\}$ |  | $\begin{aligned} & r(F \cup\{x\})=r(F)+1 \text { for all } \\ & \quad x \notin F \end{aligned}$ | $\begin{aligned} & r(H)=r(E)-1=r(H \cup\{x\})-1 \\ & \text { for all } x \notin H \end{aligned}$ | $\begin{aligned} & r(C)=\|C\|-1=r(C-\{x\}) \\ & \text { for all } x \in C \end{aligned}$ |
| 4. Closed sets gF | $\cap\{F: F \supseteq A, F \in \mathscr{F}\}$ | Maximum size of chain of closed sets, all properly contained in A |  | $H$ is a maximal proper closed set | (Use cycles: add " $C$ is minimal such that" in $4 \rightarrow 9$ ) |
| 5. Hyperplanes $\mathscr{H}$ | $\cap\{H: H \supseteq A, H \in \mathscr{H}\}$ (where the empty intersection equals $E$ ) | $c(\varnothing)-c(A)$, where for $A \subseteq E$, <br> $c(A)=\max \{k$ : there exist <br> $H_{1}, \ldots, H_{k} \in \mathscr{H}$ where for all <br> $j, H_{j} \supseteq A$, and $\left.H_{j} \supseteq H_{1} \cap \ldots \cap H_{j-1}\right\}$ | $F$ is an intersection of hyperplanes |  | (Use cycles: add " $C$ is minimal such that" in $5 \rightarrow$ 9) <br> [*Dual complement] |
| 6. Circuits $\mathscr{C}$ | $\{x: x \in A$, or there is a $C \in \mathscr{C}$ with $x \in C \subseteq A \cup\{x\}\}$ | $\|A\|-\max \{k$ : there are $k$ circuits $C_{1}, \ldots, C_{k}$ such that for all $j, C_{j} \subseteq A$, and $\left.C_{i} \not \equiv C_{1} \cup \ldots \cup C_{1-1}\right\}$ | $\|C-F\| \neq 1$ for all $C \in \mathscr{C}$ | (Use closed sets) |  |
| 7. Bonds $\mathscr{C}^{*}$ | $E-\cup\left\{B: B \in \mathscr{C}^{*}, B \cap A=\varnothing\right\}$ | (Use hyperplanes) | (Use hyperplanes) | $H$ is the complement of a bond | (Use cycles: add " $C$ is minimal such that" in $7 \rightarrow 9$ ) <br> [*Dual set] |
| 9. Cycles $\mathcal{O}^{*}$ | $\left\{x: x \in A\right.$, or there is a $C \in \mathcal{O}^{*}$ with $x \in C \subseteq A \cup\{x\}\}$ | $\begin{aligned} & \|A\|-\max \{k: \\ & \left.\varnothing \subsetneq C_{1} \subsetneq C_{2} \subsetneq \ldots \subsetneq C_{k} \subseteq A\right\} \end{aligned}$ | $\begin{aligned} & \|C-F\| \neq 1 \text { for all } C \in \mathbb{O}^{*} \\ & \text { [*Dual complement] } \end{aligned}$ | (Use closed sets) | $C$ is a minimal cycle |
| 11. Independent sets $\mathscr{I}$ | $\begin{aligned} & E-\{x: x \notin A \text { and } I \cup\{x\} \in \mathscr{I} \\ & \text { for all } I \in \mathscr{I}, I \subseteq A\} \end{aligned}$ | $\boldsymbol{\operatorname { m a x }}\{\|I\|: I \in \mathscr{I}, I \subseteq A\}$ | $\begin{aligned} & I \cup\{x\} \in \mathscr{I} \text { whenever } I \subseteq F, \\ & I \in \mathscr{I} \text {, and } x \notin F \end{aligned}$ | (Use bases) | (Use dependent sets: add " $C$ is minimal such that" in $11 \rightarrow 12$ ) |
| 13. Bases采 | (Use independent sets) | $\boldsymbol{\operatorname { m a x } \{}\{\|B \cap A\|: B \in \mathscr{B}\}$ | (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 $B \in \mathscr{C}^{*}$ if $B \neq \varnothing$ and | 8. Open sels $O \in \mathbb{C}$ if | 9. Cycles $C \in \mathscr{C} *$ if $C=\varnothing$ or | 10. Spanning sets $S \in \mathscr{S}$ if | 11. Independent sets $I \in \mathscr{I}$ if | 12. Dependent sets $D \in \mathscr{O}$ if | 13. Bases $B \in \mathscr{B}$ if |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1. | (Use hyperplanes) | (Use closed sets) | $\begin{aligned} & x \leq \vee\{y: y \in C-\{x\}\} \\ & \text { for all } x \in C \end{aligned}$ | $\hat{1}=v\{x: x \in S\}$ | Suprema of subsets of 1 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 $\mathrm{cl}(E-B) \neq E$ | $\mathrm{dd}(E-O)=E-O$ | $\begin{aligned} & \operatorname{cl}(C-x)=\operatorname{cl}(C) \text { for } \\ & \quad \text { all } x \in C \end{aligned}$ | $\mathrm{cl}(\mathrm{S})=E$ | $\underset{x \in I}{x \notin \operatorname{cl}(I-\{x\}) \text { for all }}$ | $\begin{aligned} & x \in \operatorname{cl}(D-\{x\}) \text { for some } \\ & x \in D \end{aligned}$ | $\begin{aligned} & \operatorname{cl}(B)=E \neq \operatorname{cl}(B-x) \text { for } \\ & \text { all } x \in B \end{aligned}$ |
| 3. | $B$ is minimal such that $r(E-B)=r(E)-1$ | $\begin{aligned} & r(E-O)=r[E-O) \cup x]-1 \\ & \text { for all } x \in O \end{aligned}$ | $r(C-x)=r(C)$ 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 $F \in \mathscr{F}$ <br> [*Dual complement] | $S$ is contained in no proper closed set | $\begin{aligned} & \text { For every } x \in I, \\ & \begin{array}{l} I-F=\{x\} \text { for } \\ \text { some } F \in \mathscr{F} \end{array} \end{aligned}$ | There is an $x \in D$ such that $D-F \neq\{x\}$ for all $F \in \mathscr{F}$ | (Use spanning sets: add " $B$ minimal such that") |
| 5. | $B$ is a hyperplane complement | (Use bonds) | $\underset{H \in \mathscr{H}}{\|C-H\| \neq 1 \text { for all }}$ | $S$ is contained in no hyperplane | $\begin{aligned} & \text { For every } x \in I, \\ & \quad I-H=\{x\} \text { for } \\ & \text { some } H \in \mathscr{H} \end{aligned}$ | There is an $x \in D$ such that $D-H \neq\{x\}$ for all $H \in \mathscr{H}$ | (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 $C \in \mathscr{C}$ | $C$ is a union of circuits | $\begin{aligned} & \text { For all } x \notin S \text {, there is } \\ & \text { a circuit } C \text { such that } \\ & x \in C \subseteq S \cup\{x\} \end{aligned}$ | I contains no circuit | $D$ contains some circuit | (Use independent sets: add " $B$ maximal such that") |
| 7. |  | $O=\varnothing$, or $O$ is a union of bonds | $\|C \cap B\| \neq 1 \text { for all }$ $B \in \mathscr{C}^{*}$ | $S$ 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 $9 \rightarrow 8$ ) | $\begin{aligned} & \|O \cap C\| \neq 1 \text { for all } C \in \mathbb{C}^{*} \\ & \text { [*Dual set] } \end{aligned}$ |  | 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] |


[^0]:    ${ }^{8}$ Weakening the stipulation $x \in I-I^{\prime}$ in I2 by the statement $x \in I$ results in an axiom that does not imply 12 , as is shown by the family $\{\varnothing, w, x, y, z, w x, w y, w z, x y, x z, y z, w x y\}$.
    ${ }^{9} \mathrm{D} 2^{\prime}$ is D2 with the restriction on the hypothesis that $\left|D_{1}-D_{2}\right|=\left|D_{2}-D_{1}\right|=1$.
    ${ }^{10}$ For both B 2 and B 2 ', we get an equivalent axiom by replacing "...x $x \in B \ldots y \in B^{\prime}$..." with "... $x \in B-B^{\prime} \ldots y \in B^{\prime}-B \ldots$.
    ${ }^{11}$ Axiom $\mathrm{B} 2{ }^{(3)}$ is, in fact, equivalent to both B1 and B2. In general, we cannot combine B2 ${ }^{\prime}$ and $\mathrm{B} 2^{(3)}$ to get bijective symmetric exchange $\left\{\right.$ where both $(B-x) \cup\{f(x)\}$ and $\left[B^{\prime}-f(x)\right] \cup$ $\{x\}$ 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 $\mathrm{B}^{2(2)}$ and $\mathrm{B2}^{(3)}$ : bijective subset exchange, where there exists a bijection $f: B \rightarrow B^{\prime}$ such that $(B-A) \cup f(A)$ is a basis for all $A \subseteq B$.
    ${ }^{12}$ Axiom $\mathbf{B 2}^{(4)}$, with "...y $\boldsymbol{y} B^{\prime}-B \ldots x \in B-B^{\prime} \ldots$ " replaced by $\overline{B_{2}{ }^{(4)}}$ ("...y $y \in B^{\prime} \ldots x \in$ $B \ldots$.$) is too weak. For example, the equicardinal family \{x y u, x y v, x y w, u v x, u v y, u v w\}$ satisfies $\mathrm{B}^{2(4)}$ but not B 2 .

