C is realizable as the set of circuits of a hereditary system if and only if the elements of **C** are nonempty and no element of **C** contains another.

The characterization of rank functions is more subtle. It includes two properties (r1, r2 below) that we will need, plus an additional technical condition that forces r to be the rank function of the hereditary system M defined by $I_M = \{X \subseteq E: r(X) = |X|\}$.

8.2.17. Lemma. For the rank function r of a hereditary system on E,
(r1) $r(\emptyset) = 0$.
(r2) $r(X) \leq r(X+e) \leq r(X)+1$ whenever $X \subseteq E$ and $e \in E$.

Proof: From the definition $r(X) = \max\{|Y|: Y \subseteq X, Y \in \mathbf{I}\}$, we have $r(\emptyset) = 0$. Because $X + e$ contains every independent subset of X, also $r(X+e) \geq r(X)$. Because the independent subsets of $X + e$ not contained in X consist of e plus an independent subset of X, we have $r(X+e) \leq r(X)+1$. ■

PROPERTIES OF MATROIDS

We have remarked that many equivalent conditions on hereditary systems yield matroids. We can show that a hereditary system is a matroid by verifying any of them, after which we can employ them all without additional proof. We obtained the same benefit from equivalent characterizations of trees.

Adding an edge to a forest creates at most one cycle. More generally, adding one element to an independent set in a matroid creates at most one circuit. Our proof of the greedy algorithm for spanning trees (Theorem 2.3.3) used *only* this property of graphs. This "induced circuit" property is one of the conditions that characterize matroids, as is the effectiveness of the greedy algorithm itself! Both properties appear in our list.

Given weights on the elements of a matroid, the **greedy algorithm** is the process of iteratively including an element of largest nonnegative weight whose addition to the independent set already selected yields a larger independent set. Rado [1957] proved that matroids are precisely the hereditary systems for which the greedy algorithm selects a maximum-weighted independent set regardless of the choice of weights.

8.2.18. Definition. A hereditary system M on E is a **matroid** if it satisfies any of the following additional properties, where $\mathbf{I}, \mathbf{B}, \mathbf{C}$, and r are the independent sets, bases, circuits, and rank function of M.

I: **augmentation**—if $I_1, I_2 \in \mathbf{I}$ with $|I_2| > |I_1|$, then $I_1 + e \in \mathbf{I}$ for some $e \in I_2 - I_1$.
U: **uniformity**—for every $X \subseteq E$, the maximal subsets of X belonging to **I** have the same size.
B: **base exchange**—if $B_1, B_2 \in \mathbf{B}$, then for all $e \in B_1 - B_2$ there exists $f \in B_2 - B_1$ such that $B_1 - e + f \in \mathbf{B}$.
R: **submodularity**—$r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$ whenever $X, Y \subseteq E$.
A: **weak absorption**—$r(X) = r(X+e) = r(X+f)$ implies $r(X+e+f) = r(X)$ whenever $X \subseteq E$ and $e, f \in E$,

A′: **strong absorption**—if $X, Y \subseteq E$, and $r(X+e) = r(X)$ for all $e \in Y$, then $r(X \cup Y) = r(X)$.
C: **weak elimination**—for distinct circuits $C_1, C_2 \in \mathbf{C}$ and $x \in C_1 \cap C_2$, there is another member of $\mathbf{C}$ contained in $(C_1 \cup C_2) - x$.
J: **induced circuits**—if $I \in \mathbf{I}$, then $I + e$ contains at most one circuit.
G: **greedy algorithm**—for each nonnegative weight function on E, the greedy algorithm selects an independent set of maximum total weight.

The base exchange property implies that all bases have the same size: if $|B_1| < |B_2|$ for some $B_1, B_2 \in \mathbf{B}$, then we can iteratively replace elements of $B_1 - B_2$ by elements of $B_2 - B_1$ to obtain a base of size $|B_1|$ contained in B_2, but no base is contained in another.

8.2.19.* Remark. The rank of a set $X \subseteq E$ in a vectorial matroid is the dimension of the space spanned by X. Hence for vectorial matroids the submodularity inequality says that $\dim U \cap V + \dim U \oplus V \leq \dim U + \dim V$, where $U, V, U \oplus V$ are the spaces spanned by subsets $X, Y, X \cup Y$ of E, respectively. The usual proof of this is the vector space statement of our proof of U⇒R below. Exercise 10 obtains submodularity directly for cycle matroids.

Various of these properties (together with requirements for a hereditary system) have been used as the defining condition for matroids. Examples include I (Welsh [1976], Schrijver [to appear]), U (Edmonds [1965b,c], Bixby [1981], Nemhauser–Wolsey [1988]), A (Whitney [1935]), C (Tutte [1970]), G (Papadimitriou–Steiglitz [1982]), and others (van der Waerden [1937], Rota [1964], Crapo–Rota [1970], Aigner [1979]). ■

Many authors include basic properties of hereditary systems in the set of axioms characterizing some aspect of a matroid. This can distract from the special additional properties of matroids and lead to extra work. Starting with hereditary systems yields more concise proofs. All properties of hereditary systems are always available.

8.2.20. Theorem. For a hereditary system M, the conditions defining matroids in Definition 8.2.18 are equivalent.

Proof: U ⇒ B. By uniformity for $X = E$, all bases have the same size. We then apply uniformity to the set $(B_1 - e) \cup B_2$. This yields an augmentation of the independent set $B_1 - e$ from B_2 to reach size $|B_2|$.

B ⇒ I. Given independent sets $I_1, I_2 \in \mathbf{I}$ with $|I_2| > |I_1|$, choose $B_1, B_2 \in \mathbf{B}$ such that $I_1 \subseteq B_1$, $I_2 \subseteq B_2$. We use base exchange to replace elements of $B_1 - I_1$ outside B_2 with elements of B_2. Hence we may assume that $B_1 - I_1 \subseteq B_2$. If $B_1 - I_1 \subseteq B_2 - I_2$, then $|B_1| < |B_2|$, which is forbidden by the base exchange property as remarked above. Hence I_2 has an element in $B_1 - I_1$, and we use such an element to augment I_1.

I ⇒ A. Suppose that $r(X) = r(X+e) = r(X+f)$. If $r(X+e+f) > r(X)$, then let I_1, I_2 be maximum independent subsets of X and of $X+e+f$. Now $|I_2| > |I_1|$, and we can augment I_1 from I_2. Since I_1 is a maximum independent subset of

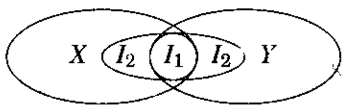
X, the augmentation can only add e or f, which contradicts the hypothesis that $r(X) = r(X+e) = r(X+f)$.

A $\Rightarrow$ A′. We use induction on $|Y - X|$. The statement is trivial when $|Y - X| = 1$. When $|Y - X| > 1$, choose $e, f \in Y - X$, and let $Y' = Y - e - f$. Applying the induction hypothesis to proper subsets of Y yields $r(X) = r(X \cup Y') = r(X \cup Y' + e) = r(X \cup Y' + f)$. Now weak absorption yields $r(X) = r(X \cup Y)$.

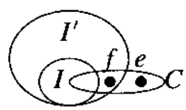
A′ $\Rightarrow$ U. If Y is a maximal independent subset of X, then $r(Y+e) = r(Y)$ for all $e \in X - Y$. By strong absorption, $r(X) = r(Y) = |Y|$. Hence all such Y have the same size.

U $\Rightarrow$ R. Given $X, Y \subseteq E$, choose a maximum independent set I_1 from $X \cap Y$. By uniformity, I_1 can be enlarged to a maximum independent subset of $X \cup Y$; call this I_2. Consider $I_2 \cap X$ and $I_2 \cap Y$, these are independent subsets of X and Y, and each includes I_1. Hence

$$r(X \cap Y) + r(X \cup Y) = |I_1| + |I_2| = |I_2 \cap X| + |I_2 \cap Y| \leq r(X) + r(Y).$$



U$\Rightarrow$R



J$\Rightarrow$G

R $\Rightarrow$ C. Consider distinct circuits $C_1, C_2 \in \mathbf{C}$ with $x \in C_1 \cap C_2$. We have $r(C_1) = |C_1| - 1$ and $r(C_2) = |C_2| - 1$. Also $r(C_1 \cap C_2) = |C_1 \cap C_2|$, since every proper subset of a circuit is independent. If $(C_1 \cup C_2) - x$ does not contain a circuit, then $r((C_1 \cup C_2) - x) = |C_1 \cup C_2| - 1$, and hence $r(C_1 \cup C_2) \geq |C_1 \cup C_2| - 1$. Applying submodularity to C_1 and C_2 yields the contradiction

$$|C_1 \cap C_2| + |C_1 \cup C_2| - 1 \leq |C_1| + |C_2| - 2.$$

C $\Rightarrow$ J. If $I + e$ contains $C_1, C_2 \in \mathbf{C}$ for some $I \in \mathbf{I}$, then C_1, C_2 both contain e. Now weak elimination guarantees a circuit in $(C_1 \cup C_2) - e$. On the other hand, $(C_1 \cup C_2) - e$ is independent, being contained in I.

J $\Rightarrow$ G. For weight function w, let I be the output of the greedy algorithm. Among the maximum-weight independent sets, let I^* be one having largest intersection with I. The algorithm cannot end with $I \subset I^*$. If $I \neq I^*$, then let e be the first element of $I - I^*$ chosen by the algorithm. By the choice of I^*, $I^* + e$ is dependent; hence it has a unique circuit C. Since $C \not\subseteq I$, we may choose $f \in C - I$. Since $I^* + e$ has no other circuit, $I^* + e - f \in \mathbf{I}$. The optimality of I^* yields $w(f) \geq w(e)$. Since f and the elements of I chosen earlier than e all lie in I^*, f does not complete a circuit with them. Thus f was available when the algorithm selected e, which yields $w(f) \leq w(e)$. Now $w(f) = w(e)$ and $w(I^* + e - f) = w(I^*)$. With $|I^* + e - f \cap I| > |I^* \cap I|$, this contradicts the choice of I^*. Thus $I^* = I$.

G $\Rightarrow$ I. Given $I_1, I_2 \in \mathbf{I}$ with $k = |I_1| < |I_2|$, we design a weight function for which the success of the greedy algorithm yields the desired augmentation. Let $w(e) = k + 2$ for $e \in I_1$, and let $w(e) = k + 1$ for $e \in I_2 - I_1$. Let $w(e) =$

0 for $e \notin I_1 \cup I_2$. Now $w(I_2) \ge (k+1)^2 > k(k+2) = w(I_1)$, so I_1 is not a maximum-weighted independent set. However, the greedy algorithm chooses every element of I_1 before any element of $I_2 - I_1$. Because it finds a maximum-weighted independent set, it continues after absorbing I_1 and adds an element $e \in I_2 - I_1$ such that $I_1 + e \in \mathbf{I}$. ■

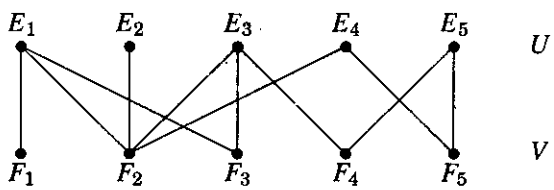
The property most often used to show that a hereditary system is a matroid is the augmentation property.

8.2.21. Example. The **uniform matroid** of rank k, denoted $U_{k,n}$ when $|E| = n$, is defined by $\mathbf{I} = \{X \subseteq E\colon |X| \le k\}$. This immediately satisfies the base exchange and augmentation properties. The **free matroid** is the uniform matroid of rank $|E|$. Uniform matroids are used in building more interesting matroids and in characterizing classes of matroids. Few uniform matroids are graphic, and few graphic matroids are uniform (Exercise 6). Neither $M(K_4 - e)$ nor $M(K_4)$ is a uniform matroid.

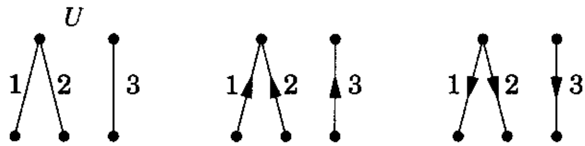
A linear matroid representable over the field $\mathbb{Z}_2$ or $\mathbb{Z}_3$ is **binary** or **ternary**, respectively. Every graphic matroid is binary (Exercise 43); $U_{2,4}$ is ternary (Exercise 44) but not binary (and hence not graphic). ■

8.2.22. Example. The **partition matroid** on E induced by a partition of E into blocks $E_1, \dots, E_k$ is defined by $\mathbf{I} = \{X \subseteq E\colon |X \cap E_i| \le 1 \text{ for all } i\}$. Since $\emptyset \in \mathbf{I}$, and since $X \in \mathbf{I}$ when its elements lie in distinct blocks, $\mathbf{I}$ is a hereditary family. Given $I_1, I_2 \in \mathbf{I}$ with $|I_2| > |I_1|$, the set I_2 must intersect more blocks than I_1; an element of I_2 in a block that I_1 misses yields the desired augmentation of I_1. Alternatively, $r(X)$ is the number of blocks having elements in X; this satisfies the absorption property. (Note: $M(K_4 - e)$ is *not* a partition matroid.)

Given a U, V-bigraph G, the incidences with $U = u_1, \dots, u_k$ define a partition matroid on $E(G)$ (this differs from the transversal matroid on U induced by G). The blocks are the sets $E_i = \{e \in E(G)\colon u_i \in e\}$. A set $X \subseteq E(G)$ is a matching in G if and only if X is independent in the partition matroid induced by U *and* in the partition matroid induced by V. This is the motivation for our later discussion of matroid intersection.



When G has an odd cycle, G has no set of vertices whose incident sets partition $E(G)$. In a digraph, however, each edge has a head and a tail, and we can define the **head partition matroid** and the **tail partition matroid** using the edge partitions induced by incidences with heads and by incidences with tails. (Example: The matroid of Example 8.2.3 arises as the partition matroid on E induced by U in the bipartite graph below, as the head partition matroid in the first digraph, and as the tail partition matroid in the second digraph.) ■



THE SPAN FUNCTION

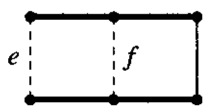
We next introduce several additional aspects of hereditary systems and matroid properties involving them. We use these aspects to illuminate matroid duality, which will lead to a characterization of planar graphs using matroids.

The algebraic concept of the space "spanned" by a set of vectors extends to hereditary systems. The definition is suggested by cycle matroids; a set spans itself and the elements that complete circuits with its subsets.

8.2.23. Definition. The **span function** of a hereditary system M is the function σ_M on the subsets of E defined by $\sigma_M(X) = X \cup \{e \in E\colon Y + e \in \mathbf{C}_M \text{ for some } Y \subseteq X\}$. If $e \in \sigma(X)$, then X **spans** e.

In a hereditary system, X is a dependent set if and only if it contains a circuit, which by Definition 8.2.23 holds if and only if $e \in \sigma(X - e)$ for some $e \in X$. We can therefore find the independent sets from the span function via $\mathbf{I} = \{X \subseteq E\colon (e \in X) \Rightarrow (e \notin \sigma(X - e))\}$. The properties of span functions that we use in studying matroids are (s1, s2, s3) below (an additional technical condition is needed to characterize the span functions of hereditary systems). First we illustrate property (s3) using graphs.

8.2.24. Example. In the cycle matroid $M(G)$, the meaning of $e \notin \sigma(X)$ is that X has no path between the endpoints of e. If also $e \in \sigma(X + f)$, then adding f completes such a path. The path completes a cycle with e, and hence also $f \in \sigma(X + e)$. In the figure below, X consists of the four bold edges. ■



8.2.25. Proposition. If σ is the span function of a hereditary system on E, and $X, Y \subseteq E$, then the following properties hold.

s1) $X \subseteq \sigma(X)$ (σ is **expansive**).

s2) $Y \subseteq X$ implies $\sigma(Y) \subseteq \sigma(X)$ (σ is **order-preserving**).

s3) $e \notin \sigma(X)$ and $e \in \sigma(X + f)$ imply $f \in \sigma(X + e)$ (**Steinitz exchange**).

Proof: Definition 8.2.23 implies immediately that σ is expansive and order-preserving. If $e \in \sigma(X+f)$, then e belongs to a circuit C in $X+f+e$. If also $e \notin \sigma(X)$, then $f \in C$. This circuit yields $f \in \sigma(X+e)$, and hence σ satisfies the Steinitz exchange property. ■

Properties of the span function lead to a short proof of a stronger form of the elimination property. The weak elimination property states that when $e \in C_1 \cap C_2$, there is a circuit in $(C_1 \cup C_2) - e$. Cycle matroids have the much stronger property that $C_1 \triangle C_2$ is an edge-disjoint union of cycles, since every vertex in $C_1 \triangle C_2$ has even degree. General matroids have the intermediate property that all elements of the symmetric difference belong to cycles in $(C_1 \cup C_2) - e$ when $e \in C_1 \cap C_2$ (Property C′ below).

We need a property relating rank and span in hereditary systems. The truth of the converse is our next characterization of matroids.

8.2.26.* Lemma. In a hereditary system, $[r(X+e) = r(X)] \Rightarrow e \in \sigma(X)$.

Proof: Let Y be a maximum independent subset of X. Since $|Y| = r(X) = r(X+e)$, also Y is a maximum independent subset of $X+e$. Hence e completes a circuit with some subset of X contained in Y, and $e \in \sigma(X)$. ■

8.2.27.* Theorem. If M is a hereditary system, then each condition below is necessary and sufficient for M to be a matroid.

P: **incorporation**—$r(\sigma(X)) = r(X)$ for all $X \subseteq E$.

S: **idempotence**—$\sigma^2(X) = \sigma(X)$ for all $X \subseteq E$.

T: **transitivity of dependence**—if $e \in \sigma(X)$ and $X \subseteq \sigma(Y)$, then $e \in \sigma(Y)$.

C′: **strong elimination**—whenever $C_1, C_2 \in \mathbf{C}$, $e \in C_1 \cap C_2$, and $f \in C_1 \triangle C_2$, there exists $C \in \mathbf{C}$ such that $f \in C \subseteq C_1 \cup C_2 - e$.

Proof: U $\Rightarrow$ P. Every element in $\sigma(X) - X$ completes a circuit with a subset of of X and thus lies in the span of every set between X and $\sigma(X)$. Thus it suffices to prove that $r(Y+e) = r(Y)$ when $e \in \sigma(Y)$. Let Z be a subset of Y such that $Z + e \in \mathbf{C}$. Augment Z to a maximal independent subset I of $Y+e$. By the uniformity property, $|I| = r(Y+e)$. Since $Z+e \in \mathbf{C}$, we have $e \notin I$. Thus $I \subseteq Y$, and we have $r(Y) \geq |I| = r(Y+e)$. (Absorption can be used instead.)

P $\Rightarrow$ S. Since σ is expansive, $\sigma^2(X) \supseteq \sigma(X)$, and we need only show that $e \in \sigma^2(X)$ implies $e \in \sigma(X)$. By the incorporation property, $r(\sigma(X)+e) = r(\sigma(X))$ and $r(\sigma(X)) = r(X)$. Since $X \subseteq \sigma(X)$, monotonicity of r yields $r(X) \leq r(X+e) \leq r(\sigma(X)+e) = r(X)$. Since equality holds throughout, Lemma 8.2.26 yields $e \in \sigma(X)$.

S $\Rightarrow$ T. If $X \subseteq \sigma(Y)$, then the order-preserving and idempotence properties of σ imply $\sigma(X) \subseteq \sigma^2(Y) = \sigma(Y)$.

T $\Rightarrow$ C′. Given distinct $C_1, C_2 \in \mathbf{C}$ with $e \in C_1 \cap C_2$ and $f \in C_1 - C_2$, we want $f \in \sigma(Y)$, where $Y =)C_1 \cup C_2) - e - f$. We have $f \in \sigma(X)$, where $X = C_1 - f$. By T, it suffices to show $X \subseteq \sigma(Y)$. Since $X - e \subseteq Y \subseteq \sigma(Y)$, we need only show $e \in \sigma(Y)$. Since σ is order-preserving, we have $e \in \sigma(C_2 - e) \subseteq \sigma(Y)$.

C′ $\Rightarrow$ C. C is a less restrictive statement than C′. ■

Like uniqueness of induced circuits (J), the incorporation property (P) relates two aspects of hereditary systems. These are well-known properties of matroids, and in the approach via hereditary systems they become characterizations. The equivalence of C and C′ was first proved by Lehman [1964].

Idempotence occurs naturally for graphic and linear matroids. The span of a set of vectors contains nothing additional in its span; similarly, every edge that can be added to the span of a set of edges joins two components. This suggests related aspects of hereditary systems.

8.2.28. Definition. The **spanning sets** of a hereditary system on E are the sets $X \subseteq E$ such that $\sigma(X) = E$. The **closed sets** are the sets $X \subseteq E$ such that $\sigma(X) = X$ (also called **flats** or **subspaces**). The **hyperplanes** are the maximal proper closed subsets of E.

8.2.29.* Remark. The span function of a matroid is also called its **closure function**. A **closure operator** is an expansive, order-preserving, idempotent function from the family of subsets of a set to itself. A closure operator is the span function of a matroid if and only if it has the Steinitz exchange property.

In every hereditary system, the span function satisfies Steinitz exchange. Thus treating matroids as hereditary systems with additional properties is not well suited for studying closure operators. The span function of a hereditary system M is a closure operator if and only if M is a matroid. Matroids are developed from lattice theory in MacLane [1936], Rota [1964], and Aigner [1979].

We have not considered all relationships among aspects of matroids. Brylawski [1986] presents a matrix describing the transformations among about a dozen aspects of matroids, calling these maps **cryptomorphisms**. ■

THE DUAL OF A MATROID

Duality in matroids generalizes the notion of duality for planar graphs. Every connected plane graph G has a natural dual graph G^* such that $(G^*)^* = G$. The dual is formed by associating a vertex of G^* with each face of G and including a dual edge e^* in G^* for each edge of G, such that the endpoints of the edge e^* are the vertices for the faces on the two sides of e.

A set of edges in a plane graph G forms a spanning tree in G if and only if the duals to the remaining edges form a spanning tree in G^* (Exercise 6.1.21). Hence the bases in the cycle matroid $M(G^*)$ are the complements of the bases in $M(G)$. We define duality for matroids and hereditary systems so that the properties of duality in planar graphs generalize.

8.2.30. Definition. The **dual** of a hereditary system M on E is the hereditary system M^* whose bases are the complements of the bases of M. The aspects $\mathbf{B}^*(\mathbf{B}_{M^*})$, $\mathbf{C}^*$, $\mathbf{I}^*$, r^*, σ^*, of M^* are the **cobases**, **cocircuits**, etc., of M.

The **supbases** $\mathbf{S}$ of M are the sets containing a base. The **hypobases** $\mathbf{H}$ are the maximal subsets containing no base. We write $\overline{X}$ for $E - X$.

8.2.31. Lemma. If M is a hereditary system, then
a) $\mathbf{B}^* = \{\overline{B}: B \in \mathbf{B}\}$ and $(M^*)^* = M$.
b) $\mathbf{I}^* = \{\overline{S}: S \in \mathbf{S}\}$ and $\mathbf{S}^* = \{\overline{I}: I \in \mathbf{I}\}$.
c) $\mathbf{C}^* = \{\overline{H}: H \in \mathbf{H}\}$ and $\mathbf{H}^* = \{\overline{C}: C \in \mathbf{C}\}$.

Proof: The statement about $\mathbf{B}^*$ is the definition of M^*. It immediately yields $(M^*)^* = M$ and both parts of (b). Also, X is a maximal (proper) subset of E containing no base (a hypobase of M) if and only if $\overline{X}$ is a minimal nonempty set contained in no cobase, which is a circuit of M^*. Similarly, the hypobases of M^* are the complements of the circuits of M. ■

We have chosen "supbase" and "hypobase" to share initials with "spanning" and "hyperplane", because for matroids the spanning sets and supbases are the same, and the hyperplanes and hypobases are the same.

8.2.32. Lemma. If M is a matroid, then the supbases are the spanning sets, and the hypobases are the hyperplanes.

Proof: A set X is spanning if and only if $\sigma(X) = E$. By the incorporation property, this is equivalent to $r(X) = r(E)$. By the uniformity property, this is equivalent to X containing a base. For hyperplanes, see Exercise 32.) ■

Consider $B_1, B_2 \subseteq E$. If neither of B_1, B_2 contains the other, then also neither of $\overline{B}_1, \overline{B}_2$ contains the other. Therefore, the dual of a hereditary system is a hereditary system. The notion of duality becomes useful when we prove that the dual of a matroid is a matroid. This follows easily from a dual version of the base exchange property.

8.2.33. Lemma. If M is a matroid and $B_1, B_2 \in \mathbf{B}$, then for each $e \in B_1 - B_2$ there exists $f \in B_2$ such that $B_2 + e - f$ is a base.

Proof: Since B_2 is a base, $B_2 + e$ contains exactly one circuit C. Since B_1 is independent, C also contains an element $f \in B_2 - B_1$. Now $B_2 + e - f$ contains no circuit and has size $r(E)$. ■

8.2.34. Theorem. (Whitney [1935]) The dual of a matroid M on E is a matroid with rank function $r^*(X) = |X| - (r(E) - r(\overline{X}))$.

Proof: We have observed that M^* is a hereditary system; now we prove the base exchange property for M^*. If $\overline{B}_1, \overline{B}_2 \in \mathbf{B}^*$ and $e \in \overline{B}_1 - \overline{B}_2$, then $B_1, B_2 \in \mathbf{B}$, with $e \in B_2 - B_1$. By Lemma 8.2.33, there exists $f \in B_1 - B_2$ such that $B_1 + e - f \in \mathbf{B}$. Now $\overline{B}_1 - e + f \in \mathbf{B}^*$ is the desired exchange.

To compute $r^*(X)$, let Y be a maximal coindependent subset of X, so $r^*(X) = r^*(Y) = |Y|$. By Lemma 8.2.31, $\overline{Y}$ is a minimal superset of $\overline{X}$ that contains a base of M. Since $\overline{Y}$ arises from $\overline{X}$ by augmenting a maximal independent subset of $\overline{X}$ to become a base, we have $|\overline{Y}| - |\overline{X}| = r(E) - r(\overline{X})$. With $|\overline{Y}| - |\overline{X}| = |X| - |Y|$, this yields the desired formula

$$r^*(X) = |Y| = |X| - (|\overline{Y}| - |\overline{X}|) = |X| - (r(E) - r(\overline{X})).$$ ■

We can restate any matroid property using dual aspects. Exercises 33–34 request characterizations of hyperplanes and closed sets by this method. More subtle results involve relationships between a matroid and its dual.

8.2.35. Proposition. (Dual augmentation property) Let M be a matroid. If $X \in \mathbf{I}$ and $X' \in \mathbf{I}^*$ are disjoint, then there are disjoint $B \in \mathbf{B}$ and $B' \in \mathbf{B}^*$ such that $X \subseteq B$ and $X' \subseteq B'$.

Proof: Since X' is coindependent in M, $\overline{X'}$ is spanning in M. Hence every maximal independent subset of $\overline{X'}$ is a base; we augment $X \subseteq \overline{X'}$ to a base B contained in $\overline{X'}$. The cobase $B' = \overline{B}$ contains X'. ∎

We will use cycle matroids to characterize planar graphs. The next result enables us to describe the cocircuits of a cycle matroid.

8.2.36. Proposition. Cocircuits of a matroid are the minimal sets intersecting every base. Bases are the minimal sets intersecting every cocircuit.

Proof: The cocircuits are the minimal sets contained in no cobase. Because the cobases are the complements of the bases, a set is contained in no cobase if and only if it intersects every base. Similarly, the cobases are the maximal sets containing no cocircuit, so the complements of the cobases are the minimal sets intersecting every cocircuit. ∎

8.2.37. Corollary. The cocircuits of the cycle matroid $M(G)$ are the bonds of G.

Proof: By Proposition 8.2.36, the cocircuits are the minimal sets intersecting every maximal forest. Hence they are the minimal sets whose deletion increases the number of components; these are the bonds. ∎

8.2.38. Definition. The **bond matroid** or **cocycle matroid** of a graph G is the hereditary system whose circuits are the bonds of G.

By Corollary 8.2.37, the bond matroid of G is the the dual of the cycle matroid $M(G)$. Weak elimination now applies to bonds. Since a cycle must return to its starting point, it cannot intersect a bond in exactly one edge. This generalizes to matroids as another characterization of cocircuits.

8.2.39. Theorem. The cocircuits of a matroid M on E are the minimal nonempty sets $C^* \subseteq E$ such that $|C^* \cap C| \neq 1$ for every $C \in \mathbf{C}$.

Proof: To show that every cocircuit has this property, suppose that $C \in \mathbf{C}$, $C^* \in \mathbf{C}^*$, $C^* \cap C = e$. Then $C - e \in \mathbf{I}$ and $C^* - e \in \mathbf{I}^*$, and the dual augmentation property yields $B \in \mathbf{B}$ and $\overline{B} \in \mathbf{B}^*$ such that $C - e \subseteq B$ and $C^* - e \subseteq \overline{B}$. Since e must appear in B or B^*, we obtain $C \in \mathbf{I}$ or $C^* \in \mathbf{I}^*$.

For the converse, we show that every nonempty set in $\mathbf{I}*$ meets some $C \in \mathbf{C}$ in one element; since cocircuits do not, every *minimal* set that does not is a cocircuit. Choose $X^* \in \mathbf{I}^*$. Let B^* be a cobase containing X^*, and let $B = \overline{B^*}$. For each $e \in X^*$, $B + e$ contains a circuit C, and $X^* \cap C = \{e\}$. ∎

MATROID MINORS AND PLANAR DUALS

From a graph G we can obtain smaller graphs by repeatedly deleting and/or contracting edges. The resulting graphs are the **minors** of G. Wagner [1937] proved that G is planar if and only if it does not have K_5 or $K_{3,3}$ as a minor (Exercise 6.2.12). Hadwiger [1943] conjectured that G is k-colorable if G has no minor isomorphic to K_{k+1}. A simple graph is a forest if and only if it does not have C_3 as a minor.

To generalize these operations to matroids, we need to know how deletion and contraction affect cycle matroids. The acyclic subsets of $E(G-e)$ are precisely the acyclic subsets of $E(G)$ that omit e. The acylic subsets of $E(G \cdot e)$ are the subsets of $E(G)-e$ whose union with e is acyclic in G. A dual description of contraction is more convenient: X contains a spanning tree of each component of $G \cdot e$ if and only if $X+e$ contains a spanning tree of each component of G.

We also want the notation to extend in a natural way. This causes difficulty, because discussion of graph minors often emphasizes the edges removed, while discussion of matroid minors emphasizes the elements that remain. We compromise by using matroid notation for the matroid on the set that remains while extending graph notation to describe matroids obtained by deleting or contracting one element.

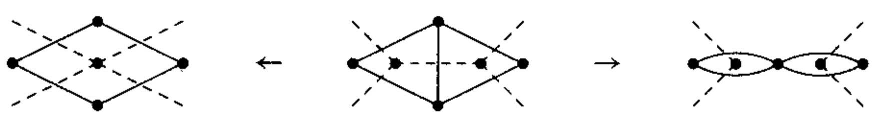
8.2.40. Definition. For a hereditary system M on E, the **restriction** *of* M *to* $F \subseteq E$, denoted $M|F$ and obtained by **deleting** $\overline{F}$, is the hereditary system defined by $\mathbf{I}_{M|F} = \{X \subseteq F\colon X \in \mathbf{I}_M\}$. The **contraction** *of* M *to* $F \subseteq E$, denoted $M.F$ and obtained by **contracting** $\overline{F}$, is the hereditary system defined by $\mathbf{S}_{M.F} = \{X \subseteq F\colon X \cup \overline{F} \in \mathbf{S}_M\}$. When $F = E - e$, we write $M - e = M|F$ and $M \cdot e = M.F$. The **minors** of M are the hereditary systems arising from M using deletions and contractions.

The definitions imply that $M|F$ and $M.F$ are hereditary systems. The operations of restriction and contraction commute (Exercise 41). The definition of contraction via supbases yields a natural duality between these operations.

8.2.41. Proposition. For hereditary systems, restriction and contraction are dual operations: $(M.F)^* = (M^*|F)$ and $(M|F)^* = (M^*.F)$.

Proof: $\mathbf{I}_{(M.F)^*} = \{X \subseteq F\colon F - X \in \mathbf{S}_{M.F}\} = \{X \subseteq F\colon (F-X) \cup \overline{F} \in \mathbf{S}_M\}$
$= \{X \subseteq F\colon \overline{X} \in \mathbf{S}_M\} = \{X \subseteq F\colon X \in \mathbf{I}_{M^*}\} = \mathbf{I}_{M^*|F}$.
For the second statement, apply the first to M^* and take duals. ■

The duality between deletion and contraction is most intuitive for plane graphs. Deleting an edge e in a plane graph G contracts the corresponding dual edge in G^*; contracting e deletes the edge in the dual.



8.2.42. Corollary. Under deletion or contraction of an edge e in a graph G, the cycle matroid and bond matroid behave as listed below.

$$M(G-e) = M(G) - e \quad M^*(G-e) = M^*(G)\cdot e$$
$$M(G\cdot e) = M(G)\cdot e \quad M^*(G\cdot e) = M^*(G) - e$$

Proof: Matroid deletion and contraction are defined so that the statements in the first column describe the behavior of cycle matroids. Using these and Proposition 8.2.41, we compute

$$M^*(G-e) = [M(G-e)]^* = [M(G)-e]^* = M^*(G)\cdot e, \text{ and}$$
$$M^*(G\cdot e) = [M(G\cdot e)]^* = [M(G)\cdot e]^* = M^*(G) - e. \qquad \blacksquare$$

As desired, restrictions and contractions of matroids are matroids.

8.2.43. Theorem. Given $F \subseteq E$ and a matroid M on E, both $M|F$ and $M.F$ are matroids on F. In terms of r_M, their rank functions are $r_{M|F}(X) = r_M(X)$ and $r_{M.F}(X) = r_M(X \cup \overline{F}) - r_M(\overline{F})$.

Proof: The augmentation property from M applies to any pair of sets in $\mathbf{I}_{M|F}$; thus $M|F$ satisfies the augmentation property and is a matroid. Using duality, $M.F = (M^*|F)^*$ is also a matroid. The rank function for $M|F$ follows from the definition of $\mathbf{I}_{M|F}$. This and repeated application of Theorem 8.2.34 to $(M^*|F)^*$ yields the rank function for $M.F$ (Exercise 42). $\blacksquare$

The formula for $r_{M.F}$ yields a description of the independent sets: $X \in \mathbf{I}_{M.F}$ if and only if adding X to $\overline{F}$ increases the rank by $|X|$.

A set of edges in a plane graph G forms a cycle if and only if the corresponding dual edges form a bond in G^* (Theorem 6.1.14). Using the natural bijection between edges and dual edges, this tells us that the cycle matroid of a plane graph G is (isomorphic to) the bond matroid of G^*. By Corollary 8.2.37, the bond matroid of a graph H is $[M(H)]^*$. Applying this to G and to G^* tells us that the bond matroid of G is (isomorphic to) the cycle matroid of G^*. Thus the bond matroid of a planar graph G is graphic. Using Kuratowski's Theorem, we will prove that this condition characterizes planarity.

Whitney [1933a] approached this by defining a non-geometric notion of dual. Changing his definition slightly, we say that H is an **abstract dual** of G if there is a bijection ϕ: $E(G) \to E(H)$ such that $X \subseteq E(G)$ is a bond in G if and only if $\phi(X)$ is the edge set of a cycle in H. With this definition, saying that G has an abstract dual is the same as saying that the bond matroid of G is graphic; the bijection ϕ establishes an isomorphism between $M^*(G)$ and $M(H)$.

8.2.44. Theorem. (Whitney [1933a]) A graph G is planar if and only if its bond matroid $M^*(G)$ is graphic.

Proof: We first prove that existence of an abstract dual is preserved under deletion and contraction of edges. Suppose that G has an abstract dual H, so that $M(H) \cong M^*(G)$. Let e' be the edge of H corresponding to e under the bijection. To prove that $H \cdot e'$ is an abstract dual of $G - e$ and that $H - e'$ is an abstract dual of $G \cdot e$, we use Corollary 8.2.42 to compute

$$M^*(G-e) = M^*(G) \cdot e \cong M(H) \cdot e' = M(H \cdot e'), \text{ and}$$
$$M^*(G \cdot e) = M^*(G) - e \cong M(H) - e' = M(H - e').$$

We have demonstrated that planar graphs have abstract duals. By Kuratowski's Theorem, a nonplanar graph contains a subdivision K_5 or $K_{3,3}$. Hence K_5 or $K_{3,3}$ is a minor of it. Since existence of abstract duals is preserved under deletion and contraction, showing that K_5 and $K_{3,3}$ have no abstract dual implies that every nonplanar graph has no abstract dual.

If H is an abstract dual of G, then also G is an abstract dual of H, since $M^*(G) \cong M(H)$ if and only if $M(G) \cong M^*(H)$. If G has girth g, then bonds of H have size at least g, so $\delta(H) \geq g$. Also $e(H) = e(G)$, and the degree-sum formula yields $n(H) \leq \lfloor 2e(H)/\delta(H) \rfloor \leq \lfloor 2e(G)/g \rfloor$.

Let H be an abstract dual of K_5. Since K_5 has girth 3, $n(H) \leq \lfloor 20/3 \rfloor = 6$. Since all bonds of K_5 have four or six edges, all cycles of H have four or six edges, and thus H is a simple bipartite graph. However, no simple bipartite graph with at most six vertices has ten edges.

Let H be an abstract dual of $K_{3,3}$. Since $K_{3,3}$ has girth 4, $n(H) \leq \lfloor 18/4 \rfloor = 4$. Since all bonds of $K_{3,3}$ have at least three edges, all cycles of H have at least three edges, and thus H is a simple graph. However, no simple graph with at most four vertices has nine edges. ■

The argument that bond matroids of plane graphs are graphic shows that every "geometric" dual of a planar graph is an abstract dual. We have seen that the geometric dual need not be unique. Nevertheless, the cycle matroid of every graph dual to G must be $M^*(G)$; hence all geometric duals of G have the same cycle matroid. Whitney [1933b] determined when graphs have the same cycle matroid (see Exercise 45, also Kelmans [1980, 1987, 1988]).

Minors have many applications. They will soon help us prove the Matroid Intersection Theorem. They are used in characterizing classes of matroids by forbidden substructures; for example, a matroid is binary if and only if it does not have $U_{2,4}$ as a minor. Minors also are used to produce a winning strategy for a matroid generalization of Bridg-it (Theorem 2.1.17).

8.2.45.* Definition. Given $e \in E$ and a matroid M on E, the **Shannon Switching Game** (M, e) is played by the Spanner and the Cutter. The Cutter deletes elements of $E - e$ and the Spanner seizes them, one per move. The Spanner aims to seize a set that spans e, and the Cutter aims to prevent this. The Cutter moves first.

Having the Spanner move first can be simulated by adding an element e' such that $\{e, e'\}$ is a circuit; the Cutter must begin by deleting e' to avoid losing immediately. Bridg-it occurs by letting M be the cycle matroid of the graph in Theorem 2.1.17 with e the "auxiliary edge" and e' an extra auxiliary edge. The spanning tree strategy for the Spanner results from the following sufficient condition for a winning strategy. The condition is also necessary, but proving that requires the Matroid Union Theorem (Theorem 8.2.55).

8.2.46.* Theorem. (Lehman [1964]) In the Shannon Switching Game (M, e), the Spanner has a winning strategy if there are disjoint subsets X_1, X_2 of $E - e$ such that $e \in \sigma(X_1) = \sigma(X_2)$.

Proof: We use X_1, X_2 to produce a winning strategy. Let $X = \sigma(X_1) = \sigma(X_2)$. Since the Spanner can ignore deletions outside X and play in $M|(X+e)$, we may assume that X_1, X_2 are disjoint bases. If the Cutter plays g and the Spanner plays f, then g is no longer available and f cannot be deleted; the effect is deletion and contraction. Letting $M' = (M - g) \cdot f$, we have $e \in \sigma_{M'}(X)$ if and only if $g \notin X$ and $e \in \sigma_M(X + f)$. The Spanner wins if e is a loop in M', which is equivalent to $e \in \sigma_M(F)$, where F is the set seized by the Spanner.

If $|E| = 1$, then e is a loop and the Spanner wins; we proceed by induction on $|E|$. It suffices to provide an immediate answer f to g so that $M' = (M-g)\cdot f$ has two disjoint bases. If the Cutter deletes g not in X_1 or X_2, then the Spanner seizes an arbitrary f, and the two sets $X_1 - g - f$ and $X_2 - g - f$ are disjoint and spanning in M'. Hence we may assume that $g \in X_1$. The base exchange property yields $f \in X_2$ such that $X' = X_1 - g + f \in \mathbf{B}$. Now $X' - f$ and $X_2 - f$ are disjoint bases avoiding e in the game (M', e). ∎

MATROID INTERSECTION

Matroid theory took a great leap forward with the proof of the Matroid Intersection and Union Theorems by Edmonds. This provided a unified context for many well-known min-max relations, which became corollaries. We have proved some of these in earlier chapters. Yielding a simple unified proof for many important theorems, the Matroid Intersection Theorem can be considered among the most beautiful theorems of combinatorics.

The Matroid Intersection Theorem is a min-max relation for common independent sets in two matroids on the same ground set. We can view the intersection of two matroids as a hereditary system, but *not* as a matroid. For multiple matroids on a set E, we typically use subscripts to distinguish corresponding aspects, as in $\mathbf{B}_i$ for the bases of M_i, etc. We still use $\overline{X}$ to denote the complement of X within the ground set E.

8.2.47. Definition. Given hereditary systems M_1, M_2 on E, the **intersection** of M_1 and M_2 is the hereditary system whose independent sets are $\{X \subseteq E \colon X \in \mathbf{I}_1 \cap \mathbf{I}_2\}$.

For example, the intersection of the two natural partition matroids on the edges of a bipartite graph G has as its independent sets the matchings of G. These are generally not the independent sets of a matroid (see Exercises 1–2), and thus the greedy algorithm does not solve maximum-weighted matching.

Recall that a *loop* is an element forming a nonempty set of rank 0.

8.2.48. Theorem. (Matroid Intersection Theorem, Edmonds [1970]) For matroids M_1, M_2 on E, the size of a largest common independent set satisfies

$$\max\{|I| : I \in \mathbf{I}_1 \cap \mathbf{I}_2\} = \min_{X \subseteq E}\{r_1(X) + r_2(\overline{X})\}.$$

Proof: (Seymour [1976]) For weak duality, consider arbitrary $I \in \mathbf{I}_1 \cap \mathbf{I}_2$ and $X \subseteq E$. The sets $I \cap X$ and $I \cap \overline{X}$ are also common independent sets, and $|I| = |I \cap X| + \left|I \cap \overline{X}\right| \le r_1(X) + r_2(\overline{X})$.

To achieve equality, we use induction on $|E|$; when $|E| = 0$ both sides are 0. If every element of E is a loop in M_1 or in M_2, then $\max |I| = 0 = r_1(X) + r_2(\overline{X})$, where X consists of all loops in M_1. Hence we may assume that $|E| > 0$ and that some $e \in E$ is a non-loop in both matroids. Let $F = E - e$, and consider the matroids $M_1|F$, $M_2|F$, $M_1.F$, and $M_2.F$.

Let $k = \min_{X \subseteq E}\{r_1(X) + r_2(\overline{X})\}$; we seek a common independent k-set in M_1 and M_2. If there is none, then $M_1|F$ and $M_2|F$ have no common independent k-set, and $M_1.F$ and $M_2.F$ have no common independent $k-1$-set. The induction hypothesis and rank formulas (Theorem 8.2.43) yield

$$\begin{aligned} r_1(X) + r_2(F - X) &\le k - 1 \qquad \text{for some } X \subseteq F, \text{ and} \\ r_1(Y + e) - 1 + r_2(F - Y + e) - 1 &\le k - 2 \qquad \text{for some } Y \subseteq F. \end{aligned}$$

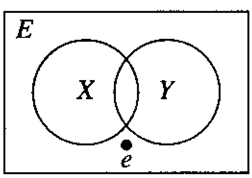
We use $(F - Y) + e = \overline{Y}$ and $F - X = \overline{X + e}$ and sum the two inequalities:

$$r_1(X) + r_2(\bar{X} + e) + r_1(Y + e) + r_2(\overline{Y}) \le 2k - 1.$$

Now we apply submodularity of r_1 to X and $Y + e$ and submodularity of r_2 to $\overline{Y}$ and $\overline{X + e}$. For clarity, write $U = X + e$ and $V = Y + e$. Applying this to the preceding inequality yields

$$r_1(X \cup V) + r_1(X \cap V) + r_2(\overline{Y} \cup \overline{U}) + r_2(\overline{Y} \cap \overline{U}) \le 2k - 1.$$

Since $\overline{Y} \cap \overline{U} = \overline{X \cup V}$ and $\overline{Y} \cup \overline{U} = \overline{X \cap V}$, the left side sums two instances of $r_1(Z) + r_2(\overline{Z})$, and the hypothesis $k \le r_1(Z) + r_2(\overline{Z})$ for all $Z \subseteq E$ yields $2k \le 2k - 1$. Hence M_1 and M_2 do have a common independent k-set. ■



It can be helpful to restrict the range of the minimization.

8.2.49. Corollary. The maximum size of a common independent set in matroids M_1, M_2 on E is the minimum of $r_1(X_1) + r_2(X_2)$ over sets X_1, X_2 such that $X_1 \cup X_2 = E$ and each X_i is closed in M_i.

Proof: The incorporation property implies that $r_i(\sigma_i(X)) = r_i(X)$. ■

We have proved special cases of the Matroid Intersection Theorem by other means. We proved the König–Egerváry Theorem in various ways, and we proved the Ford–Fulkerson characterization of CSDRs from Menger's Theorem in Theorem 4.2.25. Whenever we have two matroids on the same set, the Matroid Intersection Theorem tells us that there must be a min-max relation for the maximum size of a common independent set, tells us what the result should be, and provides a proof.

8.2.50. Corollary. (König [1931], Egerváry [1931]) In a bipartite graph, the largest matching and smallest vertex cover have equal size.

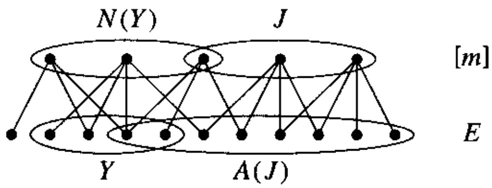
Proof: When M_1 and M_2 are the partition matroids on $E(G)$ induced by the partite sets U_1, U_2 of G, the matchings are the common independent sets. For $X_1, X_2 \subseteq E$, the rank $r_i(X_i)$ counts the vertices of U_i incident to edges in X_i. Hence if $X_1 \cup X_2 = E$, then G has a vertex cover of size $r_1(X_1) + r_2(X_2)$, using vertices of U_i to cover X_i. Conversely, if $T_1 \cup T_2$ is a vertex cover with $T_i \subseteq U_i$, let X_i be the set of edges incident to T_i; we have $X_1 \cup X_2 = E$ with X_i closed in M_i and $r_1(X_1) + r_2(X_2) = |T_1| + |T_2|$. We conclude that

$$\alpha'(G) = \max\{|I| : I \in \mathbf{I}_1 \cap \mathbf{I}_2\} = \min\{r_1(X_1) + r_2(X_2)\} = \beta(G). \qquad \blacksquare$$

The next corollary uses the rank function for transversal matroids.

8.2.51. Example. *Transversal matroids* (see Example 8.2.13). Suppose that $A_1 \cup \cdots \cup A_m = E$, and let G be the corresponding incidence graph with partite sets E and $[m]$. Consider $X \subseteq E$. If $|N(Y)| < |Y|$ for some $Y \subseteq X$, then Y forces at least $|Y| - |N(Y)|$ unsaturated elements in X. Hall's Condition applied to X yields $r(X) = \min\{|X| - (|Y| - |N(Y)|)\colon Y \subseteq X\}$ (Exercise 51).

We obtain another expression for $r(X)$ (see Ore [1955]). Let $A(J) = \bigcup_{i \in J} A_i$; in terms of the graph, $A(J) = N(J)$. By applying Hall's Condition to $[m]$ instead of E, we can write the maximum size of a matching as $r(M) = \min\{m - (|J| - |A(J)|)\colon J \subseteq [m]\}$. To determine the maximum number of elements in $X \subseteq E$ that can be matched, we discard the elements of $E - X$, obtaining $r(X) = \min_{J \subseteq [m]}\{|A(J) \cap X| - |J| + m\}$.



The first formula for $r(X)$ uses neighborhoods of subsets of E; the second uses neighborhoods of subsets of $[m]$. Exercise 53 shows directly that the second rank formula is the rank function of a matroid, without relying on results from bipartite matching. Further material on transversals appears in Mirsky [1971] and in Lovász–Plummer [1986]. $\blacksquare$