A First Course in Combinatorial Optimization

JON LEE
IBM T.J. Watson Research Center, Yorktown Heights, New York

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne,VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2004

Printed in the United States of America

Typeface Times Roman 10/13 pt. *System* LaTeX 2ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication data available

ISBN 0 521 81151 1 hardback
ISBN 0 521 01012 8 paperback

Contents

1

Matroids and the Greedy Algorithm

Matroids are objects that generalize certain combinatorial aspects of linear dependence of finite sets of points in a vector space. A graph can be encoded by means of its 0/1-valued vertex-edge incidence matrix. It turns out that, when this matrix is viewed over **GF(2)**, each linearly independent set of columns corresponds to a forest in the underlying graph, and vice versa. Therefore, a fortiori, matroids generalize aspects of graphs. From this viewpoint, Hassler Whitney founded the subject of matroid theory in 1935.

In a natural sense, matroids turn out to yield the precise structure for which the most naïve "greedy" algorithm finds an optimal solution to combinatorial-optimization problems for all *weight* functions. Therefore, matroid theory is a natural starting point for studying combinatorial-optimization methods. Furthermore, matroids have algorithmic value well beyond the study of greedy algorithms (see, for example, Chapter 3).

In addition to the algorithmic importance of matroids, we also use matroids as a starting point for exploring the power of polytopes and linear-programming duality in combinatorial optimization.

1.1 Independence Axioms and Examples of Matroids

A *matroid* M is a finite set $E(M)$ together with a subset $\mathcal{I}(M)$ of $2^{E(M)}$ that satisfies the following properties:

<u>Independence Axioms</u>

I1. $\emptyset \in \mathcal{I}(M)$.
I2. $X \subset Y \in \mathcal{I}(M) \Longrightarrow X \in \mathcal{I}(M)$.
I3. $X \in \mathcal{I}(M), Y \in \mathcal{I}(M), |Y| > |X| \Longrightarrow \exists\ e \in Y \setminus X$ such that $X + e \in \mathcal{I}(M)$.

The set $\mathcal{I}(M)$ is called the set of *independent sets* of M. The set $E(M)$ is called the *ground set* of M. Property I3 is called the *exchange axiom*.

What follows are some examples that we will revisit as we proceed.

Example (Linear matroid). Let A be a matrix over a field $\mathbf{F}$, with columns indexed by the finite set $E(A)$. Let $E(M) := E(A)$, and let $\mathcal{I}(M)$ be the set of $X \subset E(M)$ such that the columns of A_X are linearly independent. In this case, we say that M is the *linear matroid* of A and that A is a *representation* of M over $\mathbf{F}$. It is very easy to see that properties I1 and I2 hold. To see how I3 holds, suppose that $X + e \notin \mathcal{I}(M)$ for every $e \in Y \setminus X$. Then the columns of A_Y are in c.s.(A_X) (the *column space* or *linear span* of A_X). Hence, c.s.(A_Y) is a subset of c.s.(A_X). Therefore, the dimension of c.s.(A_Y) is no more than that of c.s.(A_X). Therefore, we have $|Y| \leq |X|$. ♠

Let G be a graph with vertex set $V(G)$ and edge set $E(G)$. We denote the numbers of connected components of G (counting isolated vertices as components) by $\kappa(G)$. For $F \subset E(G)$, let $G.F$ (G *restricted to* F) denote the graph with $V(G.F) := V(G)$ and $E(G.F) := F$. A set of edges F of graph G is a *forest* if it contains no cycle.

Lemma (Forest components). *Let F be a forest of a graph G. Then $|F| = |V(G)| - \kappa(G.F)$.*

Proof. By induction of $|F|$. Clearly true for $|F| = 0$. For the inductive step, we just observe that, for $e \in F$, $\kappa(G.(F - e)) = \kappa(G.F) - 1$. ■

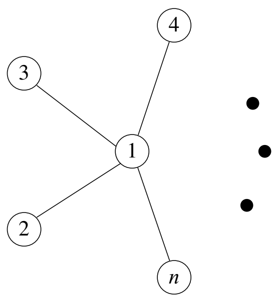
Example (Graphic matroid). Let G be a graph. Let $E(M) := E(G)$, and let $\mathcal{I}(M)$ be the set of forests of G. In this case, we say that M is the *graphic matroid* of G. It is easy to see that I1 and I2 hold. To see how I3 holds, suppose that X and Y are forests such that $X + e$ is not a forest for every $e \in Y \setminus X$. Then every edge in $Y \setminus X$ would have both ends in the same component of $G.X$. Hence, $\kappa(G.Y) \geq \kappa(G.X)$. Therefore, by the Lemma (Forest components), we have $|Y| \leq |X|$. ♠

Example (Uniform matroid). Let $E(M)$ be a finite set, and let r be an integer satisfying $0 \leq r \leq |E(M)|$. Let $\mathcal{I}(M) := \{X \subset E(M) : |X| \leq r\}$. In this case, we say that M is a *uniform matroid*. ♠

Example (Direct sum). Let M_1 and M_2 be matroids with $E(M_1) \cap E(M_2) = \emptyset$. Define M by $E(M) := E(M_1) \cup E(M_2)$, and $\mathcal{I}(M) := \{X_1 \cup X_2 : X_1 \in \mathcal{I}(M_1),\ X_2 \in \mathcal{I}(M_2)\}$. Then matroid M is the *direct sum* of M_1 and M_2. ♠

A system that respects I1 and I2 but not necessarily I3 is called an *independence system*. As the following example indicates, not every independence system is a matroid.

Example (Vertex packing on a star). Let G be a simple undirected graph. Define M by $E(M) := V(G)$, and let $\mathcal{I}(M)$ be the set of "vertex packings" of G – a *vertex packing* of G is just a set of vertices X with no edges of G between elements of X. Clearly M is an independence system. To see that M need not be a matroid consider the *n-star graph*:



with $n \geq 3$. The pair $X = \{1\}$, $Y = \{2, 3, \ldots, n\}$ violates I3. ♠

1.2 Circuit Properties

For any independence system, the elements of $2^{E(M)} \setminus \mathcal{I}(M)$ are called the *dependent sets* of M. We distinguish the dependent sets whose proper subsets are in $\mathcal{I}(M)$. We call these subsets the *circuits* of M, and we write the set of circuits of M as

$$\mathcal{C}(M) := \{X \subset E(M) \ : \ X \notin \mathcal{I}(M), \ X - e \in \mathcal{I}(M), \quad \forall\, e \in X\}.$$

For example, if M is the graphic matroid of a graph G, then the circuits of M are the cycles of G. Single-element circuits of a matroid are called *loops*; if M is the graphic matroid of a graph G, then the set of loops of M is precisely the set of loops of G.

Problem [Graphic $\Longrightarrow$ linear over GF(2)]. Show that if $A(G)$ is the vertex-edge incidence matrix of G, then the matroid represented by $A(G)$, with numbers of $A(G)$ interpreted in **GF(2)**, is precisely the graphic matroid of G.

If M is a matroid, then $\mathcal{C}(M)$ obeys the following properties:

Circuit Properties

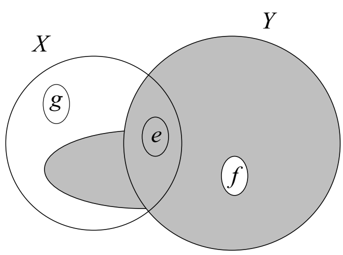
C1. $\emptyset \notin \mathcal{C}(M)$.
C2. $X \in \mathcal{C}(M)$, $Y \in \mathcal{C}(M)$, $X \subset Y \Longrightarrow X = Y$.
C3. $X \in \mathcal{C}(M)$, $Y \in \mathcal{C}(M)$, $X \neq Y$, $e \in X \cap Y \Longrightarrow \exists\ Z \subset (X \cup Y) - e$ such that $Z \in \mathcal{C}(M)$.

Properties C1 and C2 follow from I1 and I2 and the definition of $\mathcal{C}(M)$.

Theorem (Circuit elimination). *If M is a matroid, then $\mathcal{C}(M)$ satisfies C3.*

Proof. Suppose that X, Y, e satisfy the hypotheses of C3 but that $(X \cup Y) - e$ contains no element of $\mathcal{C}(M)$. By C2, $Y \setminus X \neq \emptyset$, so choose some $f \in Y \setminus X$. By the definition of $\mathcal{C}(M)$, $Y - f \in \mathcal{I}(M)$.

Let W be a subset of $X \cup Y$ that is maximal among all sets in $\mathcal{I}(M)$ that contain $Y - f$. Clearly $f \notin W$. Choose some $g \in X \setminus W$ [the set $X \setminus W$ is nonempty because X is a circuit and $W \in \mathcal{I}(M)$]. Clearly f and g are distinct because $f \in Y \setminus X$. In the following figure W is indicated by the shaded region.



Hence,

$$|W| \le |(X \cup Y) \setminus \{f, g\}| = |X \cup Y| - 2 < |(X \cup Y) - e|.$$

Now, applying I3 to W and $(X \cup Y) - e$, we see that there is an element $h \in ((X \cup Y) - e) \setminus W$, such that $W + h \in \mathcal{I}(M)$. This contradicts the maximality of W. ∎

Problem (Linear circuit elimination). Give a direct proof of C3 for linear matroids.

Problem (Graphic circuit elimination). Give a direct proof of C3 for graphic matroids.

Property C3 is called the *circuit-elimination* property. A system satisfying properties C1 and C2 but not necessarily C3 is called a *clutter*.

Example [Vertex packing on a star, continued (see p. 51)]. $X := \{1, i\}$ and $Y := \{1, j\}$ are distinct circuits for $1 \neq i \neq j \neq 1$, but $\{i, j\}$ contains no circuit. ♠

It should be clear that $\mathcal{C}(M)$ completely determines $\mathcal{I}(M)$ for any independence system. That is, given $E(M)$ and $\mathcal{C}(M)$ satisfying C1 and C2, there is precisely one choice of $\mathcal{I}(M)$ that has circuit set $\mathcal{C}(M)$ that will satisfy I1 and I2. That choice is

$$\mathcal{I}(M) := \{X \subset E(M) : \nexists\, Y \subset X,\ Y \in \mathcal{C}(M)\}.$$

Problem (Unique-circuit property). Let M be a matroid. Prove that if $X \in \mathcal{I}(M)$ and $X + e \notin \mathcal{I}(M)$, then $X + e$ contains a unique circuit of M. Give an example to show how this need not hold for a general independence system.

Problem (Linear unique circuit). Give a direct proof of the unique-circuit property for linear matroids.

Problem (Graphic unique circuit). Give a direct proof of the unique-circuit property for graphic matroids.

1.3 Representations

The *Fano matroid* is the matroid represented over **GF(2)** by the matrix

$$F = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}.$$

Exercise [Linear over GF(2) $\not\Longrightarrow$ graphic]. Prove that the Fano matroid is not graphic.

A linear matroid may have many representations. A *minimal representation* of M is a representation having linearly independent rows. If A and A' are $r \times n$ matrices over the same field, having full row rank, and there is a nonsingular matrix B and a nonsingular diagonal matrix D such that $A' = BAD$, then A and A' are *projectively equivalent*. It is easy to see that projective equivalence is an equivalence relation. If A and A' are projectively equivalent then they represent the same matroid; however, the converse is not generally true.

Proposition (Fano representation). *The Fano matroid is representable over a field if and only if the field has characteristic 2. Moreover, F is the only minimal representation of the Fano matroid over every characteristic-2 field, up to projective equivalence.*

Proof. If the Fano matroid can be represented over a field $\mathbf{F}$, then it has a minimal representation over $\mathbf{F}$ of the form

$$A = \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} & a_{37} \end{pmatrix} \end{array}.$$

The first three columns of A must be linearly independent, so, by using elementary row operations, we can bring A into the form

$$A' = \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & a'_{14} & a'_{15} & a'_{16} & a'_{17} \\ 0 & 1 & 0 & a'_{24} & a'_{25} & a'_{26} & a'_{27} \\ 0 & 0 & 1 & a'_{34} & a'_{35} & a'_{36} & a'_{37} \end{pmatrix} \end{array}.$$

We have $a'_{14} = 0$, $a'_{24} \neq 0$, and $a'_{34} \neq 0$, as $\{2, 3, 4\}$ is a circuit. Similarly, $a'_{15} \neq 0$, $a'_{25} = 0$, $a'_{35} \neq 0$, and $a'_{16} \neq 0$, $a'_{26} \neq 0$, $a'_{36} = 0$. Finally, $a'_{17} \neq 0$, $a'_{27} \neq 0$, and $a'_{37} \neq 0$, as $\{1, 2, 3, 7\}$ is a circuit.

Therefore, any minimal representation of the Fano matroid over a field **F**, up to multiplication on the left by an invertible matrix, is of the form

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & a & b & c \\ 0 & 1 & 0 & d & 0 & e & f \\ 0 & 0 & 1 & g & h & 0 & i \end{pmatrix},$$

with the letters being nonzeros in the field **F**. We can bring the matrix into the form

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & q & 1 \\ 0 & 0 & 1 & r & s & 0 & 1 \end{pmatrix},$$

with the letters being nonzeros, by nonzero row and column scaling (multiply row 1 by c^{-1}, row 2 by f^{-1}, row 3 by i^{-1}, column 4 by $d^{-1}f$, column 5 by $a^{-1}c$, column 6 by $b^{-1}c$, column 1 by c, column 2 by f, and column 3 by i).

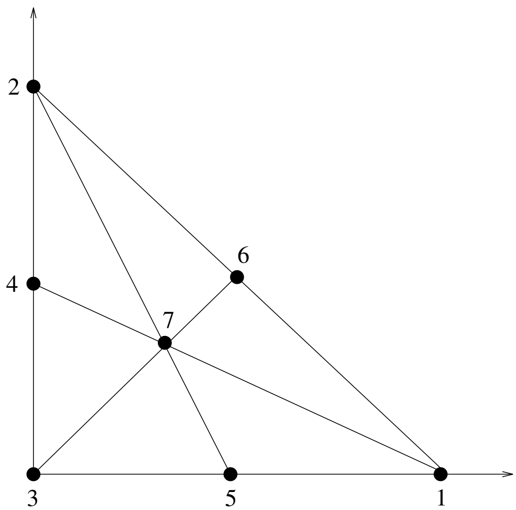
Now, columns 1, 4, and 7 should be dependent; calculating the determinant and setting it to 0, we get $r = 1$. Similarly, the required dependence of columns 2, 5, and 7 implies $s = 1$, and the dependence of columns 3, 6, and 7 implies $q = 1$. Therefore, over any field **F**, F is the only minimal representation of the Fano matroid, up to projective equivalence.

Finally, columns 4, 5, and 6 should be dependent, so we get $1 + 1 = 0$. Therefore, the field must have characteristic 2. ■

The *non-Fano matroid* arises when the **GF(2)** representation of the Fano matroid is used but the numbers are considered as rational. The representation F, viewed over **Q**, is projectively equivalent to the rational matrix

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$
$$F_{-} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1/2 & 1/2 & 1/3 \\ 0 & 1 & 0 & 1/2 & 0 & 1/2 & 1/3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Let F'_{-} be the matrix that we obtain by deleting the last row (of all 1's) of F_{-}. The *linear* dependencies among the columns of F_{-} are the same as the *affine* dependencies among the columns of the matrix F'_{-}. We can plot the columns of F'_{-} as points in the Euclidean plane and then visualize the independent sets of the non-Fano matroid as the sets of points that are affinely independent (in the plane, this means pairs of points that are not coincident and triples of points that do not lie on a straight line):



Exercise (Nonrepresentable matroids). First prove that the non-Fano matroid is representable over a field if and only if the characteristic of the field is not 2, and then prove that there are matroids representable over no field by taking the direct sum of the Fano matroid and the non-Fano matroid.

1.4 The Greedy Algorithm

Associated with any independence system M is its *rank function* $r_M : 2^{E(M)} \mapsto \mathbf{R}$, defined by

$$r_M(X) := \max\{|Y| \ : \ Y \subset X, \ Y \in \mathcal{I}(M)\}.$$

We call $r_M(E(M))$ the *rank* of M. A set $S \subset E(M)$ such that $S \in \mathcal{I}(M)$ and $|S| = r_M(E(M))$ is a *base* of M. We write $\mathcal{B}(M)$ for the set of bases of M. It is a simple matter to find a base of the independence system M when M is a matroid, provided that we can easily recognize when a set is in $\mathcal{I}(M)$. We simply use a "greedy" algorithm:

Cardinality Greedy Algorithm

1. $S := \emptyset$. $U := E(M)$.
2. While $(U \neq \emptyset)$
   i. choose any $e \in U$; $U := U - e$;
   ii. if $S + e \in \mathcal{I}(M)$, then $S := S + e$.

Throughout execution of the algorithm, $S \subset E(M)$ and $S \in \mathcal{I}(M)$. At termination, $|S| = r_M(E(M))$ (convince yourself of this by using I2 and I3).

The algorithm need not find a base of M, if M is a general independence system.

Example [Vertex packing on a star, continued (see pp. 51, 53)]. If 1 is chosen as the first element to put in S, then no other element can be added, but the only base of M is $\{2, 3, \ldots, n\}$. ♠

With respect to a matroid M and weight function c, we consider the problem of finding maximum-weight independent sets S_k of cardinality k for all k satisfying $0 \leq k \leq r_M(E(M))$. This is an extension of the problem of determining the rank of M; in that case, $c(\{e\}) = 1, \forall\, e \in E(M)$, and we concern ourselves only with $k = r_M(E(M))$. A greedy algorithm for the present problem is as follows:

(Weighted) Greedy Algorithm

1. $S_0 := \emptyset$. $k := 1$. $U := E(M)$.
2. While $(U \neq \emptyset)$
   i. choose $s_k \in U$ of maximum weight; $U := U - s_k$;
   ii. if $S_{k-1} + s_k \in \mathcal{I}(M)$, then $S_k := S_{k-1} + s_k$ and $k := k + 1$.

Next we demonstrate that each time an S_k is assigned, S_k is a maximum-weight independent set of cardinality k.

Theorem (Greedy optimality for matroids). *The Greedy Algorithm finds maximum-weight independent sets of cardinality k for every k satisfying $1 \leq k \leq r_M(E(M))$.*

Proof. The proof is by contradiction. Note that $S_k = \{s_1, s_2, \ldots, s_k\}$ for $1 \le k \le r_M(E(M))$. Hence, $c(s_1) \ge c(s_2) \ge \cdots \ge c(s_k)$. Let $T_k = \{t_1^k, t_2^k, \ldots, t_k^k\}$ be any maximum-weight independent set of cardinality k, with the elements numbered so that $c(t_1^k) \ge c(t_2^k) \ge \cdots \ge c(t_k^k)$. Suppose that $c(T_k) > c(S_k)$; then there exists p, $1 \le p \le k$, such that $c(t_p^k) > c(s_p)$. Now, consider the sets

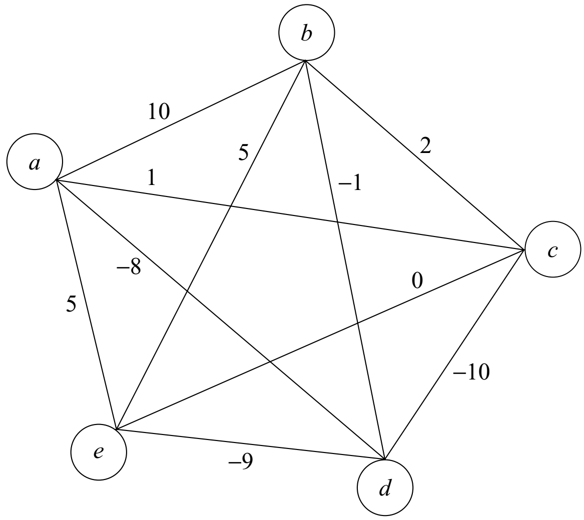
$$\{t_1^k, t_2^k, \ldots, t_{p-1}^k, t_p^k\},$$
$$\{s_1, s_2, \ldots, s_{p-1}\}.$$

Property I3 implies that there is some i, $1 \le i \le p$, such that

$$t_i^k \notin \{s_1, s_2, \ldots, s_{p-1}\},$$
$$\{s_1, s_2, \ldots, s_{p-1}\} + t_i^k \in \mathcal{I}(M).$$

Now $c(t_i^k) \ge c(t_{i+1}^k) \ge \cdots \ge c(t_p^k) > c(s_p)$; therefore, t_i^k should have been chosen in preference to s_p by the Greedy Algorithm. ■

Exercise (Maximum-weight spanning tree). Use the Greedy Algorithm, with respect to the graphic matroid of the following edge-weighted graph, to find a maximum-weight spanning tree.



The Greedy Algorithm can be used to find a maximum-weight independent set (with no restriction on the cardinality) by stopping once all positive-weight elements have been considered in Step 2.i.

Problem (Scheduling). Jobs labeled $1, 2, \ldots, n$ are to be processed by a single machine. All jobs require the same processing time. Each job j has a deadline d_j and a profit c_j, which will be earned if the job is completed by its deadline. The problem is to find the ordering of the jobs that maximizes total profit. First, prove that if a subset of the jobs can be completed on time, then they will be completed on time if they are ordered by deadline. Next, let $E(M) := \{1, 2, \ldots, n\}$, and

$$\mathcal{I}(M) := \{J \subset E(M) \; : \; \text{the jobs in } J \text{ are completed on time}\}.$$

Prove that M is a matroid by verifying that I1–I3 hold for $\mathcal{I}(M)$, and describe a method for finding an optimal order for processing the jobs.

Exercise (Scheduling). Solve the scheduling problem with the following data. The machine is available at 12:00 noon, and each job requires one hour of processing time.

Job j	c_j	d_j
1	20	3:00 P.M.
2	15	1:00 P.M.
3	10	2:00 P.M.
4	10	1:00 P.M.
5	6	2:00 P.M.
6	4	5:00 P.M.
7	3	5:00 P.M.
8	2	4:00 P.M.
9	2	2:00 P.M.
10	1	6:00 P.M.

It is natural to wonder whether some class of independence systems, more general than matroids, might permit the Greedy Algorithm to always find maximum-weight independent sets of all cardinalities. The following result ends such speculation.

Theorem (Greedy characterization of matroids). *Let M be an independence system. If the Greedy Algorithm produces maximum-weight independent sets of all cardinalities for every (nonnegative) weight function, then M is a matroid.*

Proof. We must prove that $\mathcal{I}(M)$ satisfies I3. The proof is by contradiction. Choose Y and X so that I3 fails. We assign weights as follows:

$$c(e) := \begin{cases} 1+\epsilon, & \text{if } e \in X \\ 1, & \text{if } e \in Y \setminus X \\ 0, & \text{if } e \in E(M) \setminus (X \cup Y) \end{cases},$$

with $\epsilon > 0$ to be determined. Because Y is in $\mathcal{I}(M)$, the Greedy Algorithm should find a maximum-weight independent set of cardinality $|Y|$. With just $|X|$ steps, the Greedy Algorithm chooses all of X, and then it completes X to an independent set X' of cardinality $|Y|$ by using 0-weight elements, for a total weight of $|X|(1+\epsilon)$. Now we just take care to choose $\epsilon < 1/|E(M)|$, so that $c(X') < c(Y)$. This is a contradiction. ■

Problem (Swapping Algorithm)

Swapping Algorithm

1. Choose any $S \in \mathcal{I}(M)$, such that $|S| = k$.
2. While ($\exists\, S' \in \mathcal{I}(M)$ with $|S'| = k$, $|S \Delta S'| = 2$ and $c(S') > c(S)$): Let $S := S'$.

Prove that if M is a matroid, then the Swapping Algorithm finds a maximum-weight independent set of cardinality k.

Exercise [Maximum-weight spanning tree, continued (see p. 58)]. Apply the Swapping Algorithm to calculate a maximum-weight spanning tree for the edge-weighted graph of the Maximum-weight spanning tree Exercise.

1.5 Rank Properties

Let E be a finite set, and let M be a matroid with $E(M) = E$. If $r := r_M$, then r satisfies the following useful properties:

Rank Properties

R1. $0 \le r(X) \le |X|$, and integer valued, $\forall\ X \subset E$.
R2. $X \subset Y \Longrightarrow r(X) \le r(Y), \forall\ X, Y \subset E$.
R3. $r(X \cup Y) + r(X \cap Y) \le r(X) + r(Y), \forall\ X, Y \subset E$.

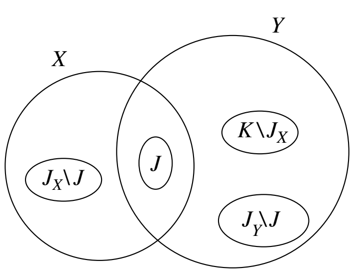
Property R3 is called *submodularity*. The rank function of a general independence system M need only satisfy R1 and R2 and the weaker property of *subadditivity*: $r_M(X \cup Y) \le r_M(X) + r_M(Y)$.

Example [Vertex packing on a star, continued (see pp. 51, 53, 57)]. For $X := \{1, i\}$ and $Y := \{1, j\}$, with $i \ne j$, we have $r_M(X) = 1$, $r_M(Y) = 1$, $r_M(X \cup Y) = 2$, and $r_M(X \cap Y) = 1$. ♠

Problem (Cuts). Let G be a graph, let $E := V(G)$, let c be a nonnegative-weight function on $E(G)$, and define $r(X) := \sum_{e \in \delta_G(X)} c(e)$, for $X \subset E$. Show that r always satisfies R3, but need not satisfy R1 and R2 [even when $c(e) = 1$, for all $e \in E(G)$].

Theorem (Submodularity of matroid rank function). *If M is a matroid, then r_M satisfies R3.*

Proof. Let J be a maximal independent subset of $X \cap Y$. Extend J to J_X (J_Y), a maximal independent subset of X (Y, respectively). We have $r_M(X \cap Y) = |J| = |J_X \cap J_Y|$. If we can show that $r_M(X \cup Y) \le |J_X \cup J_Y|$, then R3 follows, because $|J_X \cup J_Y| + |J_X \cap J_Y| = |J_X| + |J_Y|$. Extend J_X to a maximal independent subset K of $X \cup Y$.



Suppose that $|K| > |J_X \cup J_Y|$. Because $J_X \setminus J$ is contained in both K and $J_X \cup J_Y$, we have $|K \setminus (J_X \setminus J)| > |J_Y|$. Now, by the choice of J_X, we have that $K \setminus (J_X \setminus J)$ is an independent subset of Y. This contradicts the choice of J_Y. ■

Our next goal is to show that R1–R3 characterize the rank functions of matroids. That is, for every E and r satisfying R1–R3, there is a matroid M with $E(M) = E$ and $r_M = r$. First, we establish a useful lemma.

Lemma (Closure). *Suppose that $r : 2^E \mapsto \mathbf{R}$ satisfies R2 and R3. If X and Y are arbitrary subsets of E with the property that $r(X + e) = r(X)$, $\forall\, e \in Y \setminus X$, then $r(X \cup Y) = r(X)$.*

Proof. The proof is by induction on $k = |Y \setminus X|$. For $k = 1$ there is nothing to show. For $k > 1$, choose $e \in Y \setminus X$.

$$
\begin{aligned}
2r(X) &= r(X \cup ((Y \setminus X) - e)) + r(X + e) \quad \text{(by the inductive hypothesis)}\\
&\geq r(X \cup Y) + r(X) \quad \text{(by R3)}\\
&\geq 2r(X) \quad \text{(by R2)}.
\end{aligned}
$$

Therefore, equality must hold throughout, and we conclude that $r(X \cup Y) = r(X)$. ■

Theorem (Rank characterization of matroids). *Let E be a finite set, and suppose that $r : 2^E \mapsto \mathbf{R}$ satisfies R1–R3. Then*

$$\mathcal{I}(M) := \{Y \subset E(M) \ : |Y| = r(Y)\}.$$

defines a matroid M with $E(M) := E$ and $r_M = r$.

Proof. We show that the choice of $\mathcal{I}(M)$ in the statement of the theorem satisfies I1–I3, and then show that r is indeed the rank function of M.

R1 implies that $r(\emptyset) = 0$; therefore, $\emptyset \in \mathcal{I}(M)$, and I1 holds for $\mathcal{I}(M)$.

Now, suppose that $X \subset Y \in \mathcal{I}(M)$. Therefore, $r(Y) = |Y|$. R3 implies that

$$r(X \cup (Y \setminus X)) + r(X \cap (Y \setminus X)) \leq r(X) + r(Y \setminus X),$$

which reduces to

$$r(Y) \leq r(X) + r(Y \setminus X).$$

Using the facts that $r(Y) = |Y|$, $r(Y \setminus X) \le |Y \setminus X|$, and $r(X) \le |X|$, we can conclude that $r(X) = |X|$. Therefore, $X \in \mathcal{I}(M)$, and I2 holds for $\mathcal{I}(M)$.

Next, choose arbitrary $X, Y \in \mathcal{I}(M)$, such that $|Y| > |X|$. We prove I3 by contradiction. If I3 fails, then $r(X + e) = r(X)$ for all $e \in Y \setminus X$. Applying the Closure Lemma, we have $r(X \cup Y) = r(X)$. However, $r(X) = |X|$ and $r(X \cup Y) \ge r(Y) = |Y|$ implies $|Y| \le |X|$. Therefore, I3 holds for $\mathcal{I}(M)$.

We conclude that M is a matroid on E. Because M is a matroid, it has a well-defined rank function r_M which satisfies

$$r_M(Y) = \max\{|X| \ : X \subset Y,\ |X| = r(X)\}.$$

R2 for r implies that

$$\max\{|X| \ : X \subset Y,\ |X| = r(X)\} \le r(Y).$$

Therefore, we need show only that Y contains a set X with $|X| = r(X) = r(Y)$. Let X be a maximal independent subset of Y. Because $X + e \notin \mathcal{I}(M)$, $\forall\, e \in Y \setminus X$, we have $r(X + e) = r(X)$, $\forall\, e \in Y \setminus X$. By the Closure Lemma, we can conclude that $r(Y) = r(X) = |X|$, and we are done. ■

1.6 Duality

Every matroid M has a natural *dual* M^* with $E(M^*) := E(M)$ and

$$\mathcal{I}(M^*) := \{X \subset E(M) \ : \ E(M) \setminus X \text{ contains a base of } M\}.$$

Theorem (Matroid duality). *The dual of a matroid is a matroid.*

Proof. Clearly M^* is an independence system. Therefore, it possesses a well-defined rank function r_{M^*}. First we demonstrate that

$$r_{M^*}(X) = |X| + r_M(E(M) \setminus X) - r_M(E(M)), \quad \forall\, X \subset E(M^*).$$

Let Y be a subset of X that is in $\mathcal{I}(M^*)$. By the definition of $\mathcal{I}(M^*)$, $E(M) \setminus Y$ contains a base B of M. If Y is a (setwise) maximal subset of X that is in $\mathcal{I}(M^*)$, then $(X \setminus B) \setminus Y$ is empty (otherwise we could append such elements to Y to get a larger set). Therefore, a maximal such Y is of the form $X \setminus B$ for some base B of M. Now, if $Y = X \setminus B$ is a maximum cardinality such set, then