# Chapter 40

# The greedy algorithm and the independent set polytope

We now pass to algorithmic and polyhedral aspects of matroids. We show that the greedy algorithm characterizes matroids and that it implies a characterization of the independent set polytope (the convex hull of the incidence vectors of the independent sets).
Algorithmic and polyhedral aspects of the *intersection* of two matroids will be studied in Chapter 41.

## 40.1. The greedy algorithm

Let $\mathcal{I}$ be a nonempty collection of subsets of a finite set $S$ closed under taking subsets. For any weight function $w : S \to \mathbb{R}$ we want to find a set $I$ in $\mathcal{I}$ maximizing $w(I)$. The *greedy algorithm* consists of setting $I := \emptyset$, and next repeatedly choosing $y \in S \setminus I$ with $I \cup \{y\} \in \mathcal{I}$ and with $w(y)$ as large as possible. We stop if no such $y$ exists.

For general collections $\mathcal{I}$ of this kind this need not lead to an optimum solution. Indeed, matroids are precisely the structures where it always works, as the following theorem shows (Rado [1957] (necessity) and Gale [1968] and Edmonds [1971] (sufficiency)):

**Theorem 40.1.** *Let $\mathcal{I}$ be a nonempty collection of subsets of a set $S$, closed under taking subsets. Then the pair $(S,\mathcal{I})$ is a matroid if and only if for each weight function $w : S \to \mathbb{R}_+$, the greedy algorithm leads to a set $I$ in $\mathcal{I}$ of maximum weight $w(I)$.*

**Proof.** *Necessity.* Let $(S,\mathcal{I})$ be a matroid and let $w : S \to \mathbb{R}_+$ be any weight function on $S$. Call an independent set $I$ *good* if it is contained in a maximum-weight base. It suffices to show that if $I$ is good, and $y$ is an element in $S \setminus I$ with $I + y \in \mathcal{I}$ and with $w(y)$ as large as possible, then $I + y$ is good.

As $I$ is good, there exists a maximum-weight base $B \supseteq I$. If $y \in B$, then $I + y$ is good again. If $y \notin B$, then there exists a base $B'$ containing $I + y$ and contained in $B + y$. So $B' = B - z + y$ for some $z \in B \setminus I$. As $w(y)$ is chosen maximum and as $I + z \in \mathcal{I}$ since $I + z \subseteq B$, we know $w(y) \geq w(z)$.

Hence $w(B') \geq w(B)$, and therefore $B'$ is a maximum-weight base. So $I + y$ is good.

*Sufficiency.* Suppose that the greedy algorithm leads to an independent set of maximum weight for each weight function $w : S \to \mathbb{R}_+$. We show that $(S, \mathcal{I})$ is a matroid.

Condition (39.1)(i) is satisfied by assumption. To see condition (39.1)(ii), let $I, J \in \mathcal{I}$ with $|I| < |J|$. Suppose that $I + z \notin \mathcal{I}$ for each $z \in J \setminus I$.

Let $k := |I|$. Consider the following weight function $w$ on $S$:

$$w(s) := \begin{cases} k+2 & \text{if } s \in I, \\ k+1 & \text{if } s \in J \setminus I, \\ 0 & \text{if } s \in S \setminus (I \cup J). \end{cases} \tag{40.1}$$

Now in the first $k$ iterations of the greedy algorithm we find the $k$ elements in $I$. By assumption, at any further iteration, we cannot choose any element in $J \setminus I$. Hence any further element chosen, has weight 0. So the greedy algorithm yields an independent set of weight $k(k+2)$.

However, $J$ has weight at least $|J|(k+1) \geq (k+1)(k+1) > k(k+2)$. Hence the greedy algorithm does not give a maximum-weight independent set, contradicting our assumption. ∎

The theorem restricts $w$ to nonnegative weight functions. However, it is shown similarly that for matroids $M = (S, \mathcal{I})$ and arbitrary weight functions $w : S \to \mathbb{R}$, the greedy algorithm finds a maximum-weight base. By replacing 'as large as possible' in the greedy algorithm by 'as small as possible', one obtains an algorithm finding a *minimum*-weight base in a matroid. Moreover, by deleting elements of negative weight, the algorithm can be adapted to yield an independent set of maximum weight, for any weight function $w : S \to \mathbb{R}$.

Throughout we assume that the matroid $M = (S, \mathcal{I})$ is given by an algorithm testing if a given subset of $S$ belongs to $\mathcal{I}$. We call this an *independence testing oracle*. So the full list of all independent sets is not given explicitly (such a list would increase the size of the input exponentially, making most complexity issues meaningless).

In explicit applications, the matroid usually can be described by such a polynomial-time algorithm (polynomial in $|S|$). For instance, we can test if a given set of edges of a graph $G = (V, E)$ is a forest in time polynomially bounded by $|V| + |E|$. So the matroid $(E, \mathcal{F})$ can be described by such an algorithm.

Under these assumptions we have:

**Corollary 40.1a.** *A maximum-weight independent set in a matroid can be found in strongly polynomial time.*

**Proof.** See above. ∎

Similarly, for minimum-weight bases:

**Corollary 40.1b.** *A minimum-weight base in a matroid can be found in strongly polynomial time.*

**Proof.** See above. ∎

## 40.2. The independent set polytope

The algorithmic results obtained in the previous section have interesting consequences for polyhedra associated with matroids, as was shown by Edmonds [1970b,1971,1979].

The *independent set polytope* $P_{\text{independent set}}(M)$ of a matroid $M = (S, \mathcal{I})$ is, by definition, the convex hull of the incidence vectors of the independent sets of $M$. So $P_{\text{independent set}}(M)$ is a polytope in $\mathbb{R}^S$.

Each vector $x$ in $P_{\text{independent set}}(M)$ satisfies the following linear inequalities:

$$\begin{aligned} &x_s \geq 0 && \text{for } s \in S, \\ &x(U) \leq r_M(U) && \text{for } U \subseteq S, \end{aligned} \tag{40.2}$$

because the incidence vector $\chi^I$ of any independent set $I$ of $M$ satisfies (40.2). Note that $x$ is an integer vector satisfying (40.2) if and only if $x$ is the incidence vector of some independent set of $M$.

Edmonds showed that system (40.2) fully determines the independent set polytope, by deriving it from the following formula (yielding a good characterization):

**Theorem 40.2.** *Let $M = (S, \mathcal{I})$ be a matroid, with rank function $r$. Then for any weight function $w : S \to \mathbb{R}_+$:*

$$\max\{w(I) \mid I \in \mathcal{I}\} = \sum_{i=1}^{n} \lambda_i r(U_i), \tag{40.3}$$

*where $U_1 \subset \cdots \subset U_n \subseteq S$ and where $\lambda_i \geq 0$ satisfy*

$$w = \sum_{i=1}^{n} \lambda_i \chi^{U_i}. \tag{40.4}$$

**Proof.** Order the elements of $S$ as $s_1, \ldots, s_n$ such that $w(s_1) \geq w(s_2) \geq \cdots \geq w(s_n)$. Define

$$U_i := \{s_1, \ldots, s_i\} \tag{40.5}$$

for $i = 0, \ldots, n$, and

$$I := \{s_i \mid r(U_i) > r(U_{i-1})\}. \tag{40.6}$$

So $I$ is the output of the greedy algorithm. Hence $I$ is a maximum-weight independent set.

Next let:

(40.7) $$\lambda_i := w(s_i) - w(s_{i+1}) \text{ for } i = 1, \ldots, n-1, \qquad \lambda_n := w(s_n).$$

This implies (40.3):

(40.8) $$w(I) = \sum_{s \in I} w(s) = \sum_{i=1}^{n} w(s_i)(r(U_i) - r(U_{i-1})) = w(s_n)r(U_n) + \sum_{i=1}^{n-1}(w(s_i) - w(s_{i+1}))r(U_i) = \sum_{i=1}^{n} \lambda_i r(U_i).$$

By taking any ordering of $S$ for which $w$ is nonincreasing, (40.5) gives any chain of subsets $U_i$ satisfying (40.4) for some $\lambda_i \geq 0$. Hence we have the theorem. ∎

This can be interpreted in terms of LP-duality. For any weight function $w : S \to \mathbb{R}$, consider the linear programming problem

(40.9) $$\begin{array}{lll} \text{maximize} & w^{\mathsf{T}}x, & \\ \text{subject to} & x_s \geq 0 & (s \in S), \\ & x(U) \leq r_M(U) & (U \subseteq S), \end{array}$$

and its dual:

(40.10) $$\begin{array}{lll} \text{minimize} & \sum_{U \subseteq S} y_U r_M(U), & \\ \text{subject to} & y_U \geq 0 & (U \subseteq S), \\ & \sum_{U \subseteq S} y_U \chi^U \geq w. & \end{array}$$

**Corollary 40.2a.** *If $w : S \to \mathbb{Z}$, then* (40.9) *and* (40.10) *have integer optimum solutions.*

**Proof.** We can assume that $w(s) \geq 0$ for each $s \in S$ (as neither the maximum nor the minimum changes by resetting $w(s)$ to 0 if negative). Then (40.4) implies that the $\lambda_i$ are integer. This gives integer optimum solutions of (40.9) and (40.10). ∎

In polyhedral terms, Theorem 40.2 implies:

**Corollary 40.2b.** *The independent set polytope is determined by* (40.2).

**Proof.** Immediately from Theorem 40.2 (with (40.10)). ∎

Moreover, in TDI terms:

**Corollary 40.2c.** *System* (40.2) *is totally dual integral.*

**Proof.** Immediately from Corollary 40.2a. ∎

Similar results hold for the base polytope. For any matroid $M$, let $P_{\text{base}}(M)$ be the *base polytope* of $M$, defined as the convex hull of the incidence vectors of bases of $M$. Then:

**Corollary 40.2d.** *The base polytope of a matroid* $M = (S, \mathcal{I})$ *is determined by*

(40.11) $$\begin{aligned} &x_s \geq 0 && \text{for } s \in S, \\ &x(U) \leq r_M(U) && \text{for } U \subseteq S, \\ &x(S) = r_M(S). \end{aligned}$$

**Proof.** This follows directly from Corollary 40.2b, since the base polytope is the intersection of the independent set polytope with the hyperplane $\{x \mid x(S) = r_M(S)\}$, as an independent set $I$ is a base if and only if $|I| \geq r_M(S)$. ∎

The corresponding TDI result reads:

**Corollary 40.2e.** *System* (40.11) *is totally dual integral.*

**Proof.** By Theorem 5.25 from Corollary 40.2c. ∎

One can similarly describe the *spanning set polytope* $P_{\text{spanning set}}(M)$ of $M$, which is, by definition, the convex hull of the incidence vectors of the spanning sets of $M$. It is determined by the system:

(40.12) $$\begin{aligned} &0 \leq x_s \leq 1 && \text{for } s \in S, \\ &x(U) \geq r_M(S) - r_M(S \setminus U) && \text{for } U \subseteq S. \end{aligned}$$

**Corollary 40.2f.** *The spanning set polytope is determined by* (40.12).

**Proof.** A subset $U$ of $S$ is spanning in $M$ if and only if $S \setminus U$ is independent in $M^*$. Hence for any $x \in \mathbb{R}^S$ we have:

(40.13) $$x \in P_{\text{spanning set}}(M) \iff \mathbf{1} - x \in P_{\text{independent set}}(M^*).$$

By Corollary 40.2b, $\mathbf{1} - x$ belongs to $P_{\text{independent set}}(M^*)$ if and only if $x$ satisfies:

(40.14) $$\begin{aligned} &1 - x_s \geq 0 && \text{for } s \in S, \\ &|U| - x(U) \leq r_{M^*}(U) && \text{for } U \subseteq S. \end{aligned}$$

Since $r_{M^*}(U) = |U| + r_M(S \setminus U) - r_M(S)$, the present corollary follows. ∎

Corollary 40.2c gives similarly the TDI result:

**Corollary 40.2g.** *System* (40.12) *is totally dual integral.*

**Proof.** By reduction to Corollary 40.2c, by a similar reduction as in the proof of the previous corollary. ∎

Note that

(40.15) $$P_{\text{base}}(M) = P_{\text{independent set}}(M) \cap P_{\text{spanning set}}(M),$$
$$P_{\text{independent set}}(M) = P^{\downarrow}_{\text{base}}(M) \cap [0,1]^S,$$
$$P_{\text{spanning set}}(M) = P^{\uparrow}_{\text{base}}(M) \cap [0,1]^S.$$

The following consequence on the intersection of the base polytope with a box was observed by Hell and Speer [1984]:

**Corollary 40.2h.** *Let $M = (S, \mathcal{I})$ be a matroid and let $l, u \in \mathbb{R}^S$ with $l \leq u$. Then there is an $x \in P_{\text{base}}(M)$ with $l \leq x \leq u$ if and only if $l \in P^{\downarrow}_{\text{base}}(M)$ and $u \in P^{\uparrow}_{\text{base}}(M)$.*

**Proof.** Necessity being trivial, we show sufficiency. We may assume that $l, u \in [0,1]^S$. So $l \in P_{\text{independent set}}(M)$ and $u \in P_{\text{spanning set}}(M)$. Choose $l', u'$ such that $l \leq l' \leq u' \leq u$, $l' \in P_{\text{independent set}}(M)$, $u' \in P_{\text{spanning set}}(M)$, and $\|u' - l'\|_1$ minimal.

If $l' = u'$ we are done, so assume that there is an $s \in S$ with $l'(s) < u'(s)$. As we cannot increase $l'(s)$, there is a $T \subseteq S$ with $s \in T$ and $l'(T) = r(T)$. Similarly, as we cannot decrease $u'(s)$, there is a $U \subseteq S$ with $s \notin U$ and $u'(S \setminus U) = r(S) - r(U)$. Then we have the contradiction

(40.16) $$l'(T \cap U) + u'(T \cup U) \leq r(T \cap U) + u'(S) + r(T \cup U) - r(S)$$
$$\leq r(T) + r(U) + u'(S) - r(S) = l'(T) + u'(U)$$
$$< l'(T \cap U) + u'(T \cup U).$$

The last inequality follows from

(40.17) $$u'(T \cup U) - u'(U) = u'(T \setminus U) > l'(T \setminus U) = l'(T) - l'(T \cap U),$$

since $s \in T \setminus U$ and $u'(s) > l'(s)$. ∎

## 40.3. The most violated inequality

We now consider the problem to find, for any matroid $M = (S, \mathcal{I})$ and any $x \in \mathbb{R}^S_+$ not in the independent set polytope of $M$, an inequality among (40.2) most violated by $x$. That is, to find $U \subseteq S$ maximizing $x(U) - r_M(U)$.

The following theorem implies a min-max relation for this (Edmonds [1970b]):

**Theorem 40.3.** *Let $M = (S, \mathcal{I})$ be a matroid and let $x \in \mathbb{R}^S_+$. Then*

(40.18)
$$\max\{z(S) \mid z \in P_{\text{independent set}}(M), z \leq x\} \\ = \min\{r_M(U) + x(S \setminus U) \mid U \subseteq S\}.$$

**Proof.** The inequality $\leq$ in (40.18) follows from

(40.19)
$$z(S) = z(U) + z(S \setminus U) \leq r_M(U) + x(S \setminus U).$$

To see equality, let $z$ attain the maximum. Then for each $s \in S$ with $z_s < x_s$ there exists a $U \subseteq S$ with $s \in U$ and $z(U) = r_M(U)$ (otherwise we can increase $z_s$). Now the collection of sets $U \subseteq S$ satisfying $z(U) = r_M(U)$ is closed under taking unions (and intersections), since if $z(T) = r_M(T)$ and $z(U) = r_M(U)$, then

(40.20)
$$z(T \cup U) = z(T) + z(U) - z(T \cap U) \geq r_M(T) + r_M(U) - r_M(T \cap U) \\ \geq r_M(T \cup U).$$

Hence there exists a $U \subseteq S$ such that $z(U) = r_M(U)$ and such that $U$ contains each $s \in S$ with $z_s < x_s$. Hence:

(40.21)
$$z(S) = z(U) + z(S \setminus U) = r_M(U) + x(S \setminus U),$$

giving (40.18). ∎

Cunningham [1984] showed that from an independence testing oracle for a matroid one can derive a strongly polynomial time algorithm to find for any given vector $x$, a maximum violated inequality for the independent set polytope.

More strongly, Cunningham showed that one can solve the following problem in strongly polynomial time:

(40.22) given: a matroid $M = (S, \mathcal{I})$, by an independence testing oracle, and an $x \in \mathbb{Q}_+^S$;
find: a $z \in P_{\text{independent set}}(M)$ with $z \leq x$ maximizing $z(S)$, with a decomposition of $z$ as convex combination of incidence vectors of independent sets, and a subset $U$ of $S$ satisfying $z(S) = r_M(U) + x(S \setminus U)$.

By (40.18), the set $U$ certifies that $z$ maximizes $z(S)$. In the algorithm for (40.22), Cunningham utilized the 'consistent breadth-first search' based on lexicographic order, given by Schönsleben [1980] and Lawler and Martel [1982a].

To prove Cunningham's result, we first show two lemmas. The first lemma is used only to prove the second lemma. As in Section 39.9, we define for any independent set $I$ of a matroid $M = (S, \mathcal{I})$:

(40.23)
$$A(I) := \{(y, z) \mid y \in I, z \in S \setminus I, I - y + z \in \mathcal{I}\}.$$

**Lemma 40.4α.** *Let $M = (S, \mathcal{I})$ be a matroid and let $I \in \mathcal{I}$. Let $(s, t) \in A(I)$, define $I' := I - s + t$, and let $(u, v) \in A(I') \setminus A(I)$. Then $t = u$ or $(u, t) \in A(I)$, and $s = v$ or $(s, v) \in A(I)$.*

**Proof.** By symmetry, it suffices to show that $t = u$ or $(u,t) \in A(I)$ (as we may assume that $I$ is a base, and hence the second part follows by duality). We can assume that $t \neq u$. Then $t \neq v$, since $v \notin I' = I - s + t$, as $(u,v) \in A(I')$.

If $v = s$, then $I - u + t = I - u - s + t + v = I' - u + v \in \mathcal{I}$ and hence $(u,t) \in A(I)$. If $v \neq s$, then $I - u \in \mathcal{I}$ and $I - u - s + t + v \in \mathcal{I}$, and therefore $I - u + t \in \mathcal{I}$ or $I - u + v \in \mathcal{I}$; that is, $(u,v) \in A(I)$ or $(u,t) \in A(I)$. ∎

**Lemma 40.4$\beta$.** *Let $M = (S, \mathcal{I})$ be a matroid and let $q$ be a new element. For any $I \in \mathcal{I}$, define*

(40.24) $$\widetilde{A}(I) := \{(u,v) \mid u \in I + q, v \in S \setminus I, I - u + v \in \mathcal{I}\}.$$

*Let $(s,t) \in A(I)$, define $I' := I - s + t$, and let $(u,v) \in \widetilde{A}(I') \setminus \widetilde{A}(I)$. Then $t = u$ or $(u,t) \in \widetilde{A}(I)$, and $s = v$ or $(s,v) \in \widetilde{A}(I)$.*

**Proof.** Let $\widetilde{\mathcal{I}} := \{J \subseteq S + q \mid J - q \in \mathcal{I}\}$. Then the present lemma follows from Lemma 40.4$\alpha$ applied to the matroid $(S + q, \widetilde{\mathcal{I}})$. ∎

Now we can derive Cunningham's result:

**Theorem 40.4.** *Problem* (40.22) *is solvable in strongly polynomial time.*

**Proof.** We keep a vector $z \leq x$ in the independent set polytope of $M$ and a decomposition

(40.25) $$z = \sum_{i=1}^{k} \lambda_i \chi^{I_i},$$

with $I_1, \ldots, I_k \in \mathcal{I}$, $\lambda_1, \ldots, \lambda_k > 0$, and $\sum_i \lambda_i = 1$. Initially $z := \mathbf{0}$, $k := 1$, $I_1 := \emptyset$, $\lambda_1 := 1$.

Let

(40.26) $$T := \{s \in S \mid z_s < x_s\}.$$

Let $q$ be a new element. For each $i$, define $\widetilde{A}(I_i)$ as in (40.24), and let $D = (S + q, A)$ be the directed graph with

(40.27) $$A := \widetilde{A}(I_1) \cup \cdots \cup \widetilde{A}(I_k).$$

Fix an arbitrary linear order of the elements of $S + q$, by setting $S + q = \{1, \ldots, n\}$.

**Case 1: $D$ has no $q - T$ path.** Let $U$ be the set of $s \in S$ for which $D$ has an $s - T$ path. As $T \subseteq U$, we know $z(S \setminus U) = x(S \setminus U)$. Also, as no arc of $D$ enters $U$, we have $|U \cap I_i| = r_M(U)$ for all $i$, implying

(40.28) $$z(U) = \sum_{i=1}^{k} \lambda_i |U \cap I_i| = \sum_{i=1}^{k} \lambda_i r_M(U) = r_M(U).$$

Hence $z(S) = r_M(U) + x(S \setminus U)$ as required.

**Case 2: $D$ has a $q-T$ path.** For each $v \in S+q$, let $d(v)$ denote the distance in $D$ from $q$ to $v$ (set to $\infty$ if no $q-v$ path exists). Choose a $t \in T$ with $d(t)$ finite and maximal, and among these $t$ we choose the largest $t$. Let $(s,t) \in A$, with $d(s) = d(t) - 1$, and $s$ largest. We can assume that $(s,t) \in \widetilde{A}(I_1)$. Let

(40.29) $\alpha := \min\{x_t - z_t, \lambda_1\}$

and define $z'$ by

(40.30) $z' := z + \alpha(\chi^t - \chi^s)$ if $s \neq q$, and $z' := z + \alpha\chi^t$ if $s = q$.

Let $I_1' := I_1 - s + t$ (so $I_1' = I_1 + t$ if $s = q$).

Then

(40.31) $$z' = \alpha\chi^{I_1'} + (\lambda_1 - \alpha)\chi^{I_1} + \sum_{i=2}^{k} \lambda_i \chi^{I_i}.$$

If $\alpha = \lambda_1$, we delete the second term. We obtain a decomposition of $z'$ as a convex combination of at most $k+1$ independent sets, and we can iterate.

*Running time.* We show that the number of iterations is at most $|S|^9$. Consider any iteration. Let $d'$ and $A'$ be the objects $d$ and $A$ of the next iteration. We first show:

(40.32) for each $v \in S+q$: $d'(v) \geq d(v)$.

To show this, we can assume that $d'(v) < \infty$. We show (40.32) by induction on $d'(v)$, the case $d'(v) = 0$ being trivial (as it means $v = q$). Assume $d'(v) > 0$. Let $u$ be such that $(u,v) \in A'$ and $d'(u) = d'(v) - 1$. By induction we know $d'(u) \geq d(u)$.

If $(u,v) \in A$, then $d(v) \leq d(u) + 1 \leq d'(u) + 1 = d'(v)$, as required. If $(u,v) \notin A$, then $(u,v) \in \widetilde{A}(I_1')$ and $(u,v) \notin \widetilde{A}(I_1)$. By Lemma 40.4$\beta$, $t = u$ or $(u,t) \in \widetilde{A}(I_1)$, and $s = v$ or $(s,v) \in \widetilde{A}(I_1)$. Hence

(40.33) $d(v) \leq d(s) + 1 = d(t) \leq d(u) + 1 \leq d'(u) + 1 = d'(v)$.

So $d(v) \leq d'(v)$. This shows (40.32).

Let $\beta$ be the number of $j = 1, \ldots, k$ with $(s,t) \in \widetilde{A}(I_j)$. Let $T'$, $t'$, $s'$, and $\beta'$ be the objects $T$, $t$, $s$, $\beta$ in the next iteration. We show:

(40.34) if $d'(v) = d(v)$ for each $v \in S+q$, then $(d'(t'), t', s', \beta')$ is lexicographically less than $(d(t), t, s, \beta)$.

Indeed, if $\alpha = x_t - z_t$, then $T' = T - t + s$ or $T' = T - t$. So $d'(t') < d(t)$, or $d'(t') = d(t)$ and $t' < t$. If $\alpha < x_t - z_t$, then $T' = T + s$ or $T' = T$. Moreover, $\alpha = \lambda_1$, so $I_1$ has been omitted from the convex combination. So, as $t \in T'$ and $d(s) < d(t)$, we know that $t' = t$ and $d'(t') = d(t)$. As $t \in I_1'$, we know $(s',t) \notin \widetilde{A}(I_1')$. Hence, as $(s',t) \in A'$, we have $(s',t) \in \widetilde{A}(I_j)$ for some $j = 2, \ldots, k$. Hence $(s',t) \in A$. By the choice of $s$, we know $s' \leq s$. If $s' < s$, we have (40.34), so assume $s' = s$. Then $\beta' = \beta - 1$, as $(s,t) \notin \widetilde{A}(I'_1)$. This proves (40.34).

The number $k$ of independent sets in the decomposition grows by 1 if $\alpha = x_t - z_t < \lambda_1$. In that case, $d'(v) = d(v)$ for each $v \in S + q$ (by (40.32), as $A' \supseteq A$). Moreover, $d'(t') < d(t)$ or $t' < t$ (since $T' \subseteq T - t + s$). So $k$ does not exceed $|S|^4$, and hence $\beta$ is at most $|S|^4$. Concluding, the number of iterations is at most $|S|^9$. ∎

With Gaussian elimination, we can reduce the number $k$ in each iteration to at most $|S|$ (by Carathéodory's theorem). Incorporating this reduces the number of iterations to $|S|^6$.

Theorem 40.4 immediately implies that one can test if a given vector belongs to the independent set polytope of a matroid:

**Corollary 40.4a.** *Given a matroid $M = (S, \mathcal{I})$ by an independence testing oracle and an $x \in \mathbb{Q}^S$, one can test in strongly polynomial time if $x$ belongs to $P_{\text{independent set}}(M)$, and if so, decompose $x$ as a convex combination of incidence vectors of independent sets.*

**Proof.** Directly from Theorem 40.4. ∎

One can derive a similar result for the spanning set polytope:

**Corollary 40.4b.** *Given a matroid $M = (S, \mathcal{I})$ by an independence testing oracle and an $x \in \mathbb{Q}^S$, one can test in strongly polynomial time if $x$ belongs to $P_{\text{spanning set}}(M)$, and if so, decompose $x$ as a convex combination of incidence vectors of spanning sets.*

**Proof.** $x$ belongs to the spanning set polytope of $M$ if and only if $\mathbf{1} - x$ belongs to the independent set polytope of the dual matroid $M^*$. Also convex combinations of spanning sets of $M$ and independent sets of $M^*$ transfer to each other by this operation. Since $r_{M^*}(U) = |U| + r_M(S \setminus U) - r_M(S)$ for each $U \subseteq S$, also an independence testing oracle for $M^*$ is easily obtained from one for $M$. ∎

The theorem also implies that the following *most violated inequality problem* can be solved in strongly polynomial time:

(40.35) given: a matroid $M = (S, \mathcal{I})$ by an independence testing oracle, and a vector $x \in \mathbb{Q}^S$;
find: a subset $U$ of $S$ minimizing $r_M(U) - x(U)$.

**Corollary 40.4c.** *The most violated inequality problem can be solved in strongly polynomial time.*

**Proof.** Any negative component of $x$ can be reset to 0, as this does not change the problem. So we can assume that $x \geq \mathbf{0}$. Then by Theorem 40.4 we can find a $U \subseteq S$ minimizing $r_M(U) + x(S \setminus U)$ in strongly polynomial time. This $U$ is as required. ∎

### 40.3a. Facets and adjacency on the independent set polytope

Let $M = (S, \mathcal{I})$ be a matroid, with rank function $r$. Trivially, the independent set polytope $P$ of $M$ is full-dimensional if and only if $M$ has no loops. If $P$ is full-dimensional there is a unique minimal collection of linear inequalities defining $P$ (up to scalar multiplication), which corresponds to the facets of $P$. Edmonds [1970b] found that this collection is given by the following theorem. Recall that a subset $F$ of $S$ is called a *flat* if for all $s$ in $S \setminus F$ one has $r(F + s) > r(F)$. A subset $F$ is called *inseparable* if there is no partition of $F$ into nonempty sets $F_1$ and $F_2$ with $r(F) = r(F_1) + r(F_2)$. Then:

**Theorem 40.5.** *If $M$ is loopless, the following is a minimal system for the independent set polytope of $M$:*

(40.36)
(i) $x_s \geq 0$ $(s \in S)$,
(ii) $x(F) \leq r(F)$ ($F$ is a nonempty inseparable flat).

**Proof.** As $M$ is loopless, the independent set polytope of $M$ is full-dimensional. It is easy to see that (40.36) determines the independent set polytope, as any other inequality $x(U) \leq r(U)$ is implied by the inequalities $x(F_i) \leq r(F_i)$, where $F_1, \ldots, F_t$ is a maximal partition of $F := \mathrm{span}_M(U)$ such that $r(F_1) + \cdots + r(F_t) = r(F)$.

The irredundancy of collection (40.36) can be seen as follows. Each inequality $x_s \geq 0$ is irredundant, since the vector $-\chi^s$ satisfies all other inequalities.

We show that also the inequalities (40.36)(ii) are irredundant, by showing that for any two nonempty nonseparable flats $T, U$ there exists a base $I$ of $T$ with $|I \cap U| < r(U)$ (implying that the face determined by $T$ is contained in no (other) facet).

To show this, let $I$ be a base of $T$ with $|I \cap (T \setminus U)| = r(T \setminus U)$. Suppose $|I \cap U| = r(U)$. Then

$$r(U) \geq r(T \cap U) \geq r(T) - r(T \setminus U) = |I \cap U| = r(U). \tag{40.37}$$

Hence we have equality throughout. This implies (as $T$ is inseparable) that $T \setminus U = \emptyset$ or $T \cap U = \emptyset$, and that $r(U) = r(T \cap U)$. If $T \setminus U = \emptyset$, then $T \subset U$, and hence (as $T$ is a flat) $r(U) > r(T) \geq r(T \cap U)$, a contradiction. If $T \cap U = \emptyset$, then $r(U) = r(T \cap U) = 0$, implying that $U = \emptyset$ (as $M$ has no loops), again a contradiction. ∎

It follows that the base polytope, which is the face $\{x \in P \mid x(S) = r(S)\}$ of $P$, has dimension $|S| - 1$ if and only if $S$ is inseparable (that is, the matroid is *connected*).

As for adjacency of vertices of the independent set polytope, we have:

**Theorem 40.6.** *Let $M = (S, \mathcal{I})$ be a loopless matroid and let $I$ and $J$ be distinct independent sets. Then $\chi^I$ and $\chi^J$ are adjacent vertices of the independent set* *polytope of* $M$ *if and only if* $|I \triangle J| = 1$*, or* $|I \setminus J| = |J \setminus I| = 1$ *and* $r_M(I \cup J) = |I| = |J|$.

**Proof.** To see sufficiency, note that the condition implies that $I$ and $J$ are the only two independent sets with incidence vector $x$ satisfying $x(I \cap J) = r_M(I \cap J)$, $x_s = 0$ for $s \notin I \cup J$, and (if $|I \triangle J| = 2$) $x(I \cup J) = r_M(I \cup J)$. Hence $I$ and $J$ are adjacent.

To see necessity, assume that $\chi^I$ and $\chi^J$ are adjacent. If $I$ is not a base of $I \cup J$, then $I + j$ is independent for some $j \in J \setminus I$. Hence

(40.38) $$\tfrac{1}{2}(\chi^I + \chi^J) = \tfrac{1}{2}(\chi^{I+j} + \chi^{J-j}),$$

implying (as $\chi^I$ and $\chi^J$ are adjacent) that $I+j = J$ and $J-j = I$, that is $|I \triangle J| = 1$.

So we can assume that $I$ and $J$ are bases of $I \cup J$. Choose $i \in I \setminus J$. By Theorem 39.12, there is a $j \in J \setminus I$ such that $I - i + j$ and $J - j + i$ are bases of $I \cup J$. Then

(40.39) $$\tfrac{1}{2}(\chi^I + \chi^J) = \tfrac{1}{2}(\chi^{I-i+j} + \chi^{J-j+i}),$$

implying (as $\chi^I$ and $\chi^J$ are adjacent) that $I - i + j = J$ and $J - j + i = I$, that is we have the second alternative in the condition. ∎

More on the combinatorial structure of the independent set polytope can be found in Naddef and Pulleyblank [1981a].

## 40.3b. Further notes

Prodon [1984] showed that the separation problem for the independent set polytope of a matching matroid can be solved by finding a minimum-capacity cut in an auxiliary directed graph.

Frederickson and Solis-Oba [1997,1998] gave strongly polynomial-time algorithm for measuring the sensitivity of the minimum weight of a base under perturbing the weight. (Related analysis was given by Libura [1991].)

Narayanan [1995] described a rounding technique for the independent set polytope membership problem, leading to an $O(n^3r^2)$-time algorithm, where $n$ is the size of the underlying set of the matroid and $r$ is the rank of the matroid.

A strongly polynomial-time algorithm maximizing certain convex objective functions over the bases was given by Hassin and Tamir [1989].

For studies of structures where the greedy algorithm applies if condition (39.1)(i) is deleted, see Faigle [1979,1984b], Hausmann, Korte, and Jenkyns [1980], Korte and Lovász [1983,1984a,1984b,1984c,1985a,1985b,1989], Bouchet [1987a], Goecke [1988], Dress and Wenzel [1990], Korte, Lovász, and Schrader [1991], Helman, Moret, and Shapiro [1993], and Faigle and Kern [1996].