The reconstruction of matroids from their strong connectivity classes

Siaw-Lynn Ng

June 6, 2001

Abstract

In [1], it was shown that a connected matroid $\mathcal{M}$ on a finite set V decomposes into uniform matroids $\mathcal{U}_{k_1,n_1},\ldots,\mathcal{U}_{k_N,n_N}$ under strong connectivity. Here we examine the possibilities of reconstructing a matroid from its strongly connected components. This can be achieved for the small cases where $N=2$ and $N=3$. We approach the generalisation of these small cases by considering the sets of circuits (Section 3), bases (Section 4), and independent sets of the matroid (Section 6).

1 Introduction

Let $\mathcal{M}$ be a connected matroid on a finite set V with circuits $\mathcal{C}$. For each element $a \in V$, define Δ_a to be the set of circuits through a but excluding a:

$$\Delta_a = \{A\backslash a \mid a \in A \in \mathcal{C}\}.$$

Let $b \in V$ and define $\Delta_a(b)$ to be the set of subsets in Δ_a not containing b:

$$\Delta_a(b) = \{A \in \Delta_a \mid b \notin A\}.$$

For any a, $b \in V$, we say that a, b are strongly connected if and only if $\Delta_a(b) = \Delta_b(a)$, and in this case we write $a \sim b$.

In [1], it was shown that strong connectivity is an equivalence relation on V, and denoting the strong connectivity classes as $V_1,\ldots,V_N$, $\mathcal{M}|_{V_i}$ is a uniform matroid $\mathcal{U}_{k_i,n_i}$ when restricted to V_i. This raises the following question: If $\mathcal{M}$ is a matroid whose strong connectivity classes V_1, …, V_N are uniform matroids $\mathcal{U}_{k_1,n_1}$, …, $\mathcal{U}_{k_N,n_N}$ respectively, what are the possible sets of circuits of $\mathcal{M}$? In other words, if $\mathcal{M}$ and $\mathcal{N}$ are two matroids having the same strong connectivity classes $V_1,\ldots,V_N$, what differentiates $\mathcal{M}$ and $\mathcal{N}$?

This question is answered in [1] for the case when $N=2$. Using the following notation the result is quoted below: if $V = V_1 \cup V_2$, then we say that a subset X of V is a set of type (m,n) if $|X \cap V_1| = m$ and $|X \cap V_2| = n$.

Result 1.1 Let $\mathcal{M}$ be a connected matroid on V. If $\mathcal{M}$ has two strong connectivity classes V_1, V_2, with $\mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}$, $\mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}$, with $k_i \geq 1$, $n_i > k_i$ and without loss of generality, $k_1 \geq k_2$, then the circuits of $\mathcal{M}$ consists of

(a) all sets of type $(k_1+1, 0)$,

(b) all sets of type $(0, k_2+1)$, and

(c) all sets of type (m,n) for all m, n such that $m \leq k_1$, $n \leq k_2$, and $m+n=k$ for some constant k, where the parameter k satisfies

$$\begin{array}{ccccl} k_1+1 & \leq & k & \leq & k_1+k_2 \quad \text{if } k_1 > k_2, \\ k_1+1 & < & k & \leq & k_1+k_2 \quad \text{if } k_1 = k_2. \end{array}$$

Conversely, if a set V is the disjoint union of two sets V_1, V_2, $|V_1| = n_1$, $|V_2| = n_2$, and $\mathcal{C}$ is the collection of subsets of V consisting of the subsets described by (a), (b) and (c) above, then $\mathcal{C}$ is the set of circuits of a connected matroid on V with strong connectivity classes V_1 and V_2. □

There is a similar result for when one of the two components is a free matroid, while there is no connected matroid with two free components. We will concentrate on the case when none of the components is free.

In [2] it was shown that all connected matroids with two strongly connected components are representable over a finite field (and hence are secret sharing matroids). In this paper we investigate the problem of characterising matroids with more than two strongly connected components. As will be seen, the situation is much more complicated for $N > 2$. In the next section we introduce some notations and state a few generalisations of some results from [1]. In Section 3, we present a result on the circuit set of a matroid with three strongly connected components with a short explanation of the result and problems arising from it. We also describe the circuit set of a matroid with $N > 2$ strongly connected components.

2 Preliminaries

Let $\mathcal{M}$ be a connected matroid on V with N strongly connected components $\mathcal{U}_{k_1,n_1}, \ldots, \mathcal{U}_{k_N,n_N}$. Throughout this paper we will denote the strong connectivity classes as $V_1, \ldots, V_N$, so $\mathcal{M}|_{V_i} = \mathcal{U}_{k_i,n_i}$. We will also assume that $k_i < n_i$ for all $i = 1, \ldots N$.

Let C be a subset of V. Then we say that C is a set of type $(c_1, \ldots, c_N)$ if $|C \cap V_i| = c_i$ for $i = 1, \ldots, N$. If C is a set of type $(c_1, \ldots, c_N)$, then we define the weight $wt(C)$ of C and the support $supp(C)$ of C as follows:

$$\begin{aligned} wt(C) &= |\{i \mid c_i \neq 0\}|, \\ supp(C) &= \{i \mid c_i \neq 0\}. \end{aligned}$$

The size $|C|$ of C is $\sum_{i=1}^{N} c_i$.

The following facts are straightforward generalisations of some results in [1].

Result 2.1 (a) If $\mathcal{M}$ has a circuit of type $(c_1, \ldots, c_N)$ then all sets of type $(c_1, \ldots, c_N)$ are also circuits of $\mathcal{M}$.

(b) If C and C' are two circuits of $\mathcal{M}$ with identical supports then they are of the same size.

□

The converse of Result 2.1(b) is true for $N = 2$ but not for $N > 2$, that is, if C is a circuit of $\mathcal{M}$, not all sets X with $supp(X) = supp(C)$ and $|X| = |C|$ are circuits of $\mathcal{M}$. This is because $\mathcal{M}$ may have circuits of smaller weight which may be contained in some of these sets. We illustrate this in a small example:

Example 2.2 Let $\mathcal{M}$ be the connected matroid with four strongly connected components and circuits of the following types: $(3, 0, 0, 0)$, $(0, 3, 0, 0)$, $(0, 0, 4, 0)$, $(0, 0, 0, 5)$ and $(2, 2, 0, 0)$, $(0, 0, 3, 4)$, $(0, 2, 3, 3)$, $(0, 2, 2, 4)$, $(2, 0, 3, 3)$, $(2, 0, 2, 4)$. We see that there are circuits of weight 3, support $\{2, 3, 4\}$ and size 8, but not all sets of the same weight, size and support are circuits. For instance, the sets of type $(0, 1, 3, 4)$ has weight 3, support $\{2, 3, 4\}$ and size 8 but are not circuits because they contain circuits of type $(0, 0, 3, 4)$. □

This possibility somewhat complicates the situation for $N > 2$, as will be demonstrated in the following sections.

Lastly in this section we recall the circuit and base axioms:

Result 2.3 (Circuit axioms) A collection $\mathcal{C}$ of subsets of V is the set of circuits of a matroid on V if and only if conditions $(C1)$ and $(C2)$ are satisfied.

(C1) If $X \neq Y \in \mathcal{C}$ then $X \nsubseteq Y$. (Incomparability.)

(C2) If C_1, C_2 are distinct members of $\mathcal{C}$ and $z \in C_1 \cap C_2$ there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus z$. (Circuit elimination.)

□

Result 2.4 (Base axioms) A non-empty collection $\mathcal{B}$ of subsets of V is the set of bases of a matroid on V if and only if it satisfies the following condition:

(B1) If B_1, $B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there is an element $y \in B_2 \setminus B_1$ such that $(B_1 \cup y) \setminus x \in \mathcal{B}$. □

3 The circuit sets of matroids with more than two strongly connected component

We consider first connected matroids with three strongly connected components. Let $\mathcal{M}$ be a connected matroid with three strongly connected components $\mathcal{U}_{k_1,n_1}$, $\mathcal{U}_{k_2,n_2}$, $\mathcal{U}_{k_3,n_3}$. The following result describes the circuit sets of $\mathcal{M}$:

Theorem 3.1 If $\mathcal{U}_{k_1,n_1}$, $\mathcal{U}_{k_2,n_2}$, $\mathcal{U}_{k_3,n_3}$ are all connected, that is, $k_i < n_i$ for all $i = 1, 2, 3$, then, in addition to circuits of types $(k_1 + 1, 0, 0)$, $(0, k_2 + 1, 0)$, $(0, 0, k_3 + 1)$, $\mathcal{M}$ has circuits of one of the following types:

(a) (q_1, q_2, q_3) for all q_i with $1 \leq q_i \leq k_i$ and $q_1 + q_2 + q_3 = k_{123}$ for some constant k_{123} satisfying

$$\max(k_1 + k_2 + 1, k_1 + k_3 + 1, k_2 + k_3 + 1) \leq k_{123} \leq k_1 + k_2 + k_3.$$

(b) (q_1,q_2,q_3) and (m_1,m_2,m_3) for all q_i, $m_i \le k_i$ with exactly *one* fixed h such that $m_h = 0$, and

$$\begin{aligned} m_i + m_j &= k_{ij},\ i,j \neq h, \\ q_1 + q_2 + q_3 &= k_{123} \end{aligned}$$

for some constants k_{ij}, k_{123} satisfying

$$\begin{aligned} \max(k_i+1, k_j+1) \le \quad & k_{ij} & \le k_i + k_j, \\ \max(k_{ij}, k_i + k_h + 1, k_j + k_h + 1) \le \quad & k_{123} & \le (k_{ij} - 1) + k_h. \end{aligned}$$

In addition, for all circuits of type (q_1,q_2,q_3), we must have $q_i + q_j \le k_{ij} - 1$.

(c) (q_1,q_2,q_3), (m_1,m_2,m_3) and (r_1,r_2,r_3) for all q_i, m_i and r_i with exactly one fixed i and exactly one fixed j, $j \neq i$, such that $m_i = 0$ and $r_j = 0$, and

$$\begin{aligned} m_j + m_h &= k_{jh}, \\ r_i + r_h &= k_{ih}, \\ q_1 + q_2 + q_3 &= k_{123} \end{aligned}$$

for some constants k_{jh}, k_{ih} and k_{123} satisfying

$$\begin{aligned} \max(k_j+1, k_h+1) \le \quad & k_{jh} & \le k_j + k_h, \\ \max(k_i+1, k_h+1) \le \quad & k_{ih} & \le k_i + k_h, \\ \max(k_{jh}, k_{ih}, k_i + k_j + 1) \le \quad & k_{123} & \le k_{ih} + k_{jh} - (k_h + 1). \end{aligned}$$

In addition, for all circuits of type (q_1,q_2,q_3),

$$\begin{aligned} q_i + q_h &\le k_{ih} - 1, \\ q_j + q_h &\le k_{jh} - 1. \end{aligned}$$

(d) (q_1,q_2,q_3) and $(m_1,m_2,0)$, $(0,r_2,r_3)$, $(p_1,0,p_3)$ for all q_i, m_i, r_i and p_i such that $1 \le q_i, m_i, r_i, p_i \le k_i$ and

$$\begin{aligned} m_1 + m_2 &= k_{12}, \\ r_2 + r_3 &= k_{23}, \\ p_1 + p_3 &= k_{13}, \\ q_1 + q_2 + q_3 &= k_{123} \end{aligned}$$

for some constants k_{12}, k_{23}, k_{13}, k_{123} satisfying

$$\begin{aligned} \max(k_i+1, k_j+1) &\le k_{ij} \le k_i + k_j, i,j \in 1,2,3, \\ \max(k_{12}, k_{13}, k_{23}) &\le k_{123} \le \min(k_{12} + k_{23} - (k_2+1), k_{12} + k_{13} - (k_1+1), k_{13} + k_{23} - (k_3+1)), \end{aligned}$$

and for all $\{i,j,h\} = \{1,2,3\}$, not both equalities (1), (2) below holds:

$$k_{ij} = k_i + 1 = k_j + 1, \tag{1}$$
$$k_{123} = k_{ih} = k_{jh}. \tag{2}$$

In addition, for all circuits of type (q_1,q_2,q_3),

$$q_i + q_j \le k_{ij} - 1 \text{ for all } i,j = 1,2,3.$$

(e) $(k_1,k_2,0)$, $(0,k_2,k_3)$, $(k_1,0,k_3)$, provided not both $k_i = k_j = 1$ and $k_{ih} = k_{jh}$.

Conversely, if a set V is the disjoint union of three sets V_1, V_2, V_3, $|V_i| = n_i$, and $\mathcal{C}$ is the collection of subsets of V consisting of the subsets described in either (a), (b), (c), (d) or (e) above, as well as subsets of types $(k_1+1,0,0)$, $(0,k_2+1,0)$ and $(0,0,k_3+1)$, then $\mathcal{C}$ is the set of circuits of a connected matroid on V with strongly connected components $\mathcal{U}_{k_1,n_1}$, $\mathcal{U}_{k_2,n_2}$, $\mathcal{U}_{k_3,n_3}$. □

The proof of the above result is similar to that of the case when $\mathcal{M}$ decomposes into two strong connectivity classes. We give an informal explanation of some parts of the proof here.

Intuitively,

(a) The upper bound for k_{123} follows from the upper bounds for q_i, which is a direct consequence of the incomparability of circuits ((C1) of the axioms). The lower bound follows from (C2), so that if the elimination of an element of the intersection of two circuits of type (q_1, q_2, q_3) should result in a set of type $(0, *, *)$ or $(*, 0, *)$ or $(*, *, 0)$, it would still contain a circuit (of type $(*, 0, 0)$, $(0, *, 0)$ or $(0, 0, *)$).

(b) The upper and lower bounds for k_{ij} are derived as above. Similarly for the lower bound of k_{123}. The upper bound of $q_i + q_j$ follows from the fact that a circuit of weight three must not contain a circuit of weight two. The upper bound of k_{123} follows from that.

(c) The upper and lower bounds are obtained similarly. Furthermore, the upper bound of $q_i + q_h$ and $q_j + q_h$ also ensures that (taking $i = 3$, $j = 1$ for convenience) the union of a circuit of type $(m_1, m_2, 0)$ and a circuit of type $(0, r_2, r_3)$ with one element of the intersection removed will contain a circuit (of type (q_1, q_2, q_3)) when $m_2 = r_2$.

(d) The condition on the equalities (1), (2) is to prevent the merging of V_i, V_j as one strong connectivity class. For example, if both equalities hold, with

$$\begin{aligned} k_1 &= k_2 = 3, \\ k_{12} &= 4, \\ k_{123} &= k_{13} = k_{23} = 4, \end{aligned}$$

then we have circuits of types

$$\begin{aligned} &(4, 0, 0), (0, 4, 0), (0, 0, 2), (2, 2, 0), (3, 1, 0), (1, 3, 0), \\ &(0, 3, 1), (3, 0, 1), (2, 1, 1), (1, 2, 1), \end{aligned}$$

which means that $V_1 \cup V_2$ is in fact one strong connectivity class. The other upper and lower bounds follow from the same reasoning as in (a), (b), (c) above.

(e) This proof is relatively straightforward and can be generalised. The condition on the equalities again is to prevent merging of stongly connected components.

Proof: [Part (e) of Theorem 3.1] Suppose that $\mathcal{M}$ has circuits of types $(m_1, m_2, 0)$, $(0, r_2, r_3)$ and $(p_1, 0, p_3)$ in addition to circuits of types $(k_1 + 1, 0, 0)$, $(0, k_2 + 1, 0)$ and $(0, 0, k_3 + 1)$. It follows from Result 1.1 that all sets of type $(m_1, m_2, 0)$ with $m_1 + m_2 = k_{12}$ for some constant k_{12} satisfying

$$\max(k_1 + 1, k_2 + 1) \leq k_{12} \leq k_1 + k_2$$

are circuits of $\mathcal{M}$. Similarly all sets of type $(0, r_2, r_3)$ and $(p_1, 0, p_3)$ with $r_2 + r_3 = k_{23}$, $p_1 + p_3 = k_{13}$ are circuits, with

$$\begin{aligned} \max(k_2 + 1, k_3 + 1) &\leq k_{23} \leq k_2 + k_3, \\ \max(k_1 + 1, k_3 + 1) &\leq k_{13} \leq k_1 + k_3. \end{aligned}$$

Now, let

$$\begin{aligned} k_{12} &= k_1 + k_2 - \delta_1, \\ k_{13} &= k_1 + k_3 - \delta_2, \\ k_{23} &= k_2 + k_3 - \delta_3 \end{aligned}$$

for some δ_1, δ_2, $\delta_3 \geq 0$. We show that either all $\delta_i = 0$ or all $\delta_i > 0$. Suppose, without loss of generality, that $\delta_1 > 0$ and $\delta_2 = 0$. Then all sets of type $(k_1, 0, k_3)$ and type $(k_1, k_2 - \delta_1, 0)$ are circuits of $\mathcal{M}$. Let C_1 be a circuit of type $(k_1, 0, k_3)$ and C_2 a circuit of type $(k_1, k_2 - \delta_1, 0)$ such that $C_1 \cap V_1 = C_2 \cap V_1$. Then by (C2) of the circuit axioms, there must be a circuit contained in the set $X = C_1 \cup C_2 \backslash x$ for any $x \in C_1 \cap V_1$, which is a set of type $(k_1 - 1, k_2 - \delta_1, k_3)$. Clearly no circuit of type $(k_1, 0, k_3)$ can be contained in X. Since $k_1 - 1 + k_2 - \delta_1 < k_{12}$, no circuit of type $(m_1, m_2, 0)$ can be contained in X. Hence there must be a circuit of type $(0, r_2, r_3)$ contained in X and so we must have

$$k_2 + k_3 - \delta_3 \leq k_2 + k_3 - \delta_1,$$

that is, $\delta_3 \geq \delta_1 > 0$.

Now, consider circuits of types $(k_1 - \delta_1, k_2, 0)$ and $(0, k_2, k_3 - \delta_3)$. By the same argument as above, there must be a circuit contained in a set of type $(k_1 - \delta_1, k_2 - 1, k_3 - \delta_3)$. However, since $\delta_1 > 0$ and $\delta_3 > 0$, it is clear that none of the circuits can be contained in such a set, which contradicts (C2) of the circuit axioms. Hence we have proved that either all $\delta_i = 0$, or all $\delta_i > 0$.

Suppose that all $\delta_i > 0$. Consider circuits of types $(k_1 - \delta_1, k_2, 0)$ and $(0, k_2, k_3 - \delta_3)$. Then by the above argument, there must be a circuit C contained in a set of type $(k_1 - \delta_1, k_2 - 1, k_3 - \delta_3)$, which clearly cannot be of type $(m_1, m_2, 0)$ or type $(0, r_2, r_3)$. Hence C must be a circuit of type $(p_1, 0, p_3)$ and so we must have

$$(k_1 - \delta_1) + (k_3 - \delta_3) \geq k_1 + k_3 - \delta_2,$$

that is, $\delta_2 \geq \delta_1 + \delta_3$.

Next, consider circuits of types $(k_1, k_2 - \delta_1, 0)$ and $(k_1, 0, k_3 - \delta_2)$. By a similar argument as above, we must have $\delta_3 \geq \delta_1 + \delta_2$. However, this implies that $\delta_3 \geq \delta_1 + \delta_2 \geq \delta_1 + \delta_1 + \delta_3$, which gives $\delta_1 \leq 0$. This contradicts the assumption that all $\delta_i > 0$. So we must have $\delta_i = 0$ for all $i = 1, 2, 3$ and hence the result. □

Theorem 3.1 itemises all the possible circuit sets of a matroid with three strongly connected components. However, enumerating the combinations of the valid types of circuits implies that if a matroid $\mathcal{M}$ decomposes into N strong connectivity classes, then the number of possible circuit sets for $\mathcal{M}$ is of the order of 2^{2^N}. Hence it is infeasible to generalise the result in its present form and a better way of describing the circuits is needed. For example, in our result, the upper and lower bounds of k_{123} depends on whether there are circuits of types $(0, *, *)$, $(*, 0, *)$ or $(*, *, 0)$. If we don't list circuits there will have to be another way of expressing the bounds. Here we list the conditions that must be satisfied by the circuit set of a matroid with N strongly connected components.

Theorem 3.2 Suppose $\mathcal{M}$ has N strongly connected components $\mathcal{U}_{k_1,n_1}, \ldots, \mathcal{U}_{k_N,n_N}$, and circuit set $\mathcal{C}$. Let $\mathcal{C}$ be partitioned according to support:

$$\mathcal{C}_S = \{C \in \mathcal{C} \mid supp(C) = S\}, S \subseteq \{1, \ldots, N\}.$$

Then $\{\mathcal{C}_S \mid S \subseteq \{1, \ldots, N\}\}$ satisfies the following conditions:

(a) For any distinct $i, j \in \{1, \ldots, N\}$, there is an $S \subseteq \{1, \ldots, N\}$ such that $\{i, j\} \subseteq S$ and $\mathcal{C}_S \neq \emptyset$.

(b) For each $i = 1, \ldots, N$, successively define a constant σ_S associated with $\mathcal{C}_S$ for all $|S| = i$, as follows:

  (i) If $\mathcal{C}_S \neq \emptyset$ then let $\sigma_S = |C|$ for any circuit $C \in \mathcal{C}_S$.

  (ii) If $\mathcal{C}_S = \emptyset$ then let

$$\sigma_S = \min \left\{ 1 + \sum_{j=1}^{h} \left(\sigma_{S_j} - 1\right) \mid S_1, \ldots, S_h \text{ is a partition of } S \right\}.$$

  Then $\{\sigma_S \mid \mathcal{C}_S \neq \emptyset\}$ satisfies the following inequalities:

  (iii) For all $C \in \mathcal{C}_S$, if C is of type $(c_1, \ldots, c_N)$ then

$$\sum_{h \in S'} c_h < \sigma_{S'} \text{ for all } S' \subset S.$$

  (iv) For all $S' \subset S$, $|S'| = |S| - 1$, and for all disjoint subset $S_1, S_2 \subset S$, $S_1 \cup S_2 = S$,

$$\sigma_{S'} \leq \sigma_S \leq \sigma_{S_1} + \sigma_{S_2} - 2.$$

(c) For every $x, y \in \{1, \ldots, N\}$ such that

$$\sigma_{\{x,y\}} = \sigma_{\{x\}} = \sigma_{\{y\}},$$

there is a $\mathcal{C}_S$ with $x \in S$, $y \notin S$ and a $\mathcal{C}_{S'}$, $x \notin S$, $y \in S$ such that $\sigma_S \neq \sigma_{S'}$.

□

Briefly, the reasons for the necessary conditions on $\mathcal{C}$ are as follows:

(a) This is the condition for connectedness.

(b) (i) Any set of size σ_S and support S is either a circuit or contains a circuit.

  (ii) Any set of support S and size σ_S contains a circuit. In fact it is the smallest such set to guarantee to contain a circuit.

(iii) This follows from the fact that a circuit of support S must not contain a circuit of support $S' \subset S$.

(iv) The lower bound for σ_S is defined so that the elimination of an element from the intersection of two circuits of support S will still contain a circuit.

The upper bound follows from (iii) and the following fact:

If $S_1, \ldots, S_h$ is a partition of S and $T_1, \ldots, T_{h'}$ is a refinement of $S_1, \ldots, S_h$, then

$$\sum_{i=1}^{h} (\sigma_{S_i} - 1) \leq \sum_{i=1}^{h'} (\sigma_{T_i} - 1).$$

This is because if $\mathcal{C}_{S_i} \neq \emptyset$ then $\sigma_{S_i} - 1 \leq (\sigma_{T_{i_1}} - 1) + \cdots (\sigma_{T_{i_k}} - 1)$ where $T_{i_1} \cup \cdots T_{i_k} = S_i$, by (iii), while if $\mathcal{C}_{S_i} = \emptyset$ then $\sigma_{S_i} - 1$ is minimum by definition. Hence for the upper bound we need only to consider partitions of S with two parts.

(c) This is to make sure that two strongly connected components don't merge.

The converse of Theorem 3.2 is not true:

Example 3.3 Let $\mathcal{C}$ be a set subsets of $V_1 \cup V_2 \cup V_3 \cup V_4$, with

$$\begin{aligned}\mathcal{C} \;=\; &\{\text{sets of types } (5000), (0500), (0040), (0003), (4400), (4010), (3020), (2030),\\ &(4002), (0431), (0422), (0332)\}.\end{aligned}$$

Then

$$\begin{array}{lll}
\sigma_{\{1\}} = 5, & \sigma_{\{1,2\}} = 8, & \sigma_{\{1,2,3\}} = 9, \\
\sigma_{\{2\}} = 5, & \sigma_{\{1,3\}} = 5, & \sigma_{\{1,2,4\}} = 10, \\
\sigma_{\{3\}} = 4, & \sigma_{\{1,4\}} = 6, & \sigma_{\{1,3,4\}} = 7, \\
\sigma_{\{4\}} = 3, & \sigma_{\{2,3\}} = 8, & \sigma_{\{2,3,4\}} = 8, \\
 & \sigma_{\{2,4\}} = 7, & \sigma_{\{1,2,3,4\}} = 11, \\
 & \sigma_{\{3,4\}} = 6, &
\end{array}$$

satisfy conditions (a), (b) and (c) of Theorem 3.2. However $\mathcal{C}$ is not a set of circuits of a matroid: Let A be a set of type $(2,0,3,0)$ and B a set of type $(0,4,3,1)$. Then there should be a set contained in a set of type $(2,4,2,1)$ belonging to $\mathcal{C}$, but there isn't. □

It is not clear what the sufficient conditions are. The problem is that it is not clear which types of supports must occur in order for $\mathcal{C}$ to be the circuit set of a matroid. To understand this we should investigate further the following problem:

Problem 3.4 Let C_1 be a set of type $(c_1, \ldots, c_N)$ with support S_1 and C_2 a set of type $(d_1, \ldots, d_N)$ with support S_2. What are the conditions on c_i, d_i for C_1, C_2 to be circuits if $S_1 \neq S_2$? For example, if C_1 is of type $(c_1, c_2, 0, 0)$ and C_2 of type $(0, d_2, d_3, d_4)$ then either $c_2 \neq d_2$, or else there must be a circuit C contained in a set of type $(c_1, c_2 - 1, d_3, d_4)$. We may simply end up with a description:

Let $V = V_1 \cup V_2 \cup \ldots \cup V_N$ be a disjoint union of sets. Let $(c_1, \ldots c_N)$ denote the type of subsets c of V such that $|c \cap V_i| = c_i$. Let $\mathcal{C}$ be a collection of subsets of V and let $\bar{\mathcal{C}}$ be the types of the members of $\mathcal{C}$. Then

$$\begin{aligned}
\bar{\mathcal{C}} = \{c^1 &= (c^1_1, \ldots, c^1_N), \\
c^2 &= (c^2_1, \ldots, c^2_N), \\
&\ldots, \\
c^K &= (c^K_1, \ldots, c^K_N)\}
\end{aligned}$$

is the set of circuits of a matroid if and only if

(P1) $\bar{\mathcal{C}}$ is an antichain (any two elements are incomparable) in a poset $\{(x_1, \ldots, x_N) \mid 0 \leq x_i \leq |V_i|\}$ with partial order

$$(x_1, \ldots, x_N) \leq (y_1, \ldots, y_N) \text{ if and only if } x_i \leq y_i \text{ for all } i = 1, \ldots N.$$

(P2) for any $(c^i_1, \ldots, c^i_N) \neq (c^j_1, \ldots, c^j_N)$ in $\bar{\mathcal{C}}$, let $(c^{ij}_1, \ldots, c^{ij}_N)$ be defined as $c^{ij}_k = \max(c^i_k, c^j_k)$, and let $S_{ij} \subseteq \{1, \ldots, N\}$ be defined as $s \in S_{ij}$ if and only if $c^i_s c^j_s \neq 0$. Then for every $s \in S_{ij}$ there is a $c^h \in \bar{\mathcal{C}}$ such that

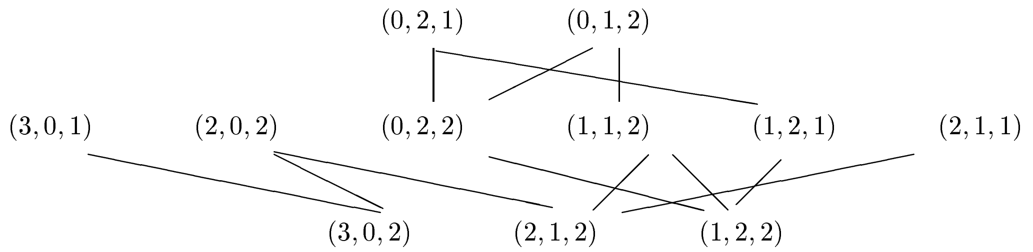
$$(c^h_1, \ldots, c^h_N) \leq (c^{ij}_1, \ldots, c^{ij}_s - 1, \ldots, c^{ij}_N).$$

For $(c^i_1, \ldots, c^i_N) = (c^j_1, \ldots, c^j_N)$, let S_{ij} be defined as $s \in S_{ij}$ if and only if $c^i_s \neq 0$. Then for every $s_1, s_2 \in S_{ij}$, there is a $c^h \in \bar{\mathcal{C}}$ such that

$$(c^h_1, \ldots, c^h_N) \leq (c^{ij}_1, \ldots, c^{ij}_{s_1} - 1, \ldots, c^{ij}_{s_2} + 1, \ldots, c^{ij}_N).$$

That the type of circuits of a matroid is a set of incomparable elements follows directly from axiom (C1). So if a set is picked as a circuit we know what other sets are *not* allowed. The problem is we don't know what to pick in the first place. Condition (P2) follows from (C2).

Example 3.5 Suppose $\mathcal{M}$ decomposes into $\mathcal{U}_{3,5}$ and $\mathcal{U}_{2,4}$ with circuits of types $(4,0)$, $(0,3)$, $(3,1)$ and $(2,2)$. Suppose $\mathcal{M}'$ decomposes into $\mathcal{U}_{3,5}$, $\mathcal{U}_{2,4}$ and $\mathcal{U}_{2,5}$ such that $\mathcal{M}'|_{V_1\cup V_2} = \mathcal{M}$. So $\mathcal{M}'$ has circuits of types $(4,0,0)$, $(0,3,0)$, $(0,0,3)$, $(3,1,0)$ and $(2,2,0)$. After eleminating all comparable elements, the possible additional circutis are of the following types:



However, it is not clear what combinations of these sets are valid. □

□

4 The set of bases of a matroid

We consider the set of bases of a matroid with N strongly connected components. Since the bases of a matroid have the same size, it is hoped that the description of a matroid in terms of its bases would be simpler than that in terms of its circuits.

Theorem 4.1 Let $\mathcal{M}$ be a connected matroid with N strongly connected components $\mathcal{U}_{k_1,n_1}$, $\mathcal{U}_{k_2,n_2}$, …, $\mathcal{U}_{k_N,n_N}$, $k_i < n_i$. Let r be the rank of $\mathcal{M}$. Then

$$\max(k_1, k_2, \ldots, k_N) \leq r \leq k_1 + k_2 + \cdots + k_N - 1.$$

These bounds are tight. □

Proof: Since there are independent sets of types $(k_1, 0, \ldots, 0)$, …, $(0, \ldots, 0, k_N)$, and a base B is a maximal independent set, we have $|B| > \max(k_1, k_2, \ldots, k_N)$.

Without loss of generality suppose that $k_1 \geq k_2 \geq \ldots \geq k_N$. Let $\mathcal{M}$ have circuits of all supports $S \subseteq \{1, \ldots, N\}$ with

$$k_S = \max_{i \in S}(k_i + 1).$$

Then $\mathcal{M}$ has rank k_1. Such a matroid exists: see Example 4.2.

The circuits of $\mathcal{M}$ has size at most $k_1 + \cdots + k_N$ and a circuit is of size $k_1 + \cdots + k_N$ if and only if it is of type $(k_1, k_2, \ldots, k_N)$. In this case $\mathcal{M}$ has rank $k_1 + k_2 + \cdots + k_N - 1$ and bases of types $(k_1 - 1, k_2, \ldots, k_N)$, $(k_1, k_2 - 1, \ldots, k_N)$, …, $(k_1, k_2, \ldots, k_N - 1)$ □

Example 4.2 Let $N = 4$, $k_1 = 4, k_2 = 3, k_3 = 2, k_4 = 1$. Then $\mathcal{M}$ has rank $r = k_1 = 4$, with circuit set $\mathcal{C}$ and base set $\mathcal{B}$ as follows:

The circuits of $\mathcal{M}$ consists of sets of the following types:

	$k_{12}=5$	$k_{13}=5$	$k_{14}=5$	$k_{23}=4$	$k_{24}=4$	$k_{34}=3$
(5000)	(4100)	(4010)	(4001)	(0310)	(0301)	(0021)
(0400)	(3200)	(3020)		(0220)		
(0030)	(2300)					
(0002)	$k_{123}=5$	$k_{124}=5$	$k_{134}=5$	$k_{234}=4$	$k_{1234}=5$	
	(3110)	(3101)	(3011)	(0211)	(2111)	
	(2210)	(2201)				
	(2120)					

The bases of $\mathcal{M}$ consists of sets of the following types:

$(*000)$	$(**00)$	$(*0*0)$	$(*00*)$	$(***0)$	$(**0*)$	$(*0**)$	$(****)$
(4000)	(3100)	(3010)	(3001)	(2110)	(2101)	(2011)	(1111)
	(2200)	(2020)		(1210)	(1201)		
	(1300)			(1120)			

□

The question now is: of what types are the bases? We would like to have a result of the following form:

Conjecture 4.3 Let $\mathcal{M}$ be a connected matroid which has N strong connectivity classes $\mathcal{U}_{k_1,n_1}, \mathcal{U}_{k_2,n_2}, \ldots, \mathcal{U}_{k_N,n_N}$, $k_i < n_i$ for all $i = 1, \ldots, N$. Let $\{\sigma_S \mid S \subseteq \{1, \ldots, N\}\}$ be a set of integers associated with $\mathcal{M}$ satisfying certain properties. Then the set $\mathcal{B}$ of bases of $\mathcal{M}$ is $\mathcal{B} = \bigcup_{S \subseteq \{1,\ldots,N\}} \mathcal{B}_S$, where $\mathcal{B}_S$ is determined by σ_S in some way. □

Now, if σ_S were to denote the sizes of circuits of with support S, then we have the following properties for $\{\sigma_S \mid S \subseteq \{1, \ldots, N\}\}$:

1. $\sigma_{\{i\}} = k_i + 1$.
2. σ_S satisfies the conditions of Theorem 3.2.
3. Suppose $\sigma_S = r + 1$ with $|S|$ maximum, that is, there are no circuits with support S' with $|S'| > |S|$. It is not clear how $\sigma_{S'}$ should be defined for $S' \neq S$, $|S'| = |S|$. Perhaps there is no need to define $\sigma_{S'}$ for any $|S'| > |S|$.
4. It is also possible that σ_S does not define circuit sets but does define bases:

Example 4.4 Consider Example 3.3 again:

$$\begin{array}{lll} \sigma_{\{1\}} = 5, & \sigma_{\{1,2\}} = 8, & \sigma_{\{1,2,3\}} = 9, \\ \sigma_{\{2\}} = 5, & \sigma_{\{1,3\}} = 5, & \sigma_{\{1,2,4\}} = 10, \\ \sigma_{\{3\}} = 4, & \sigma_{\{1,4\}} = 6, & \sigma_{\{1,3,4\}} = 7, \\ \sigma_{\{4\}} = 3, & \sigma_{\{2,3\}} = 8, & \sigma_{\{2,3,4\}} = 8, \\ & \sigma_{\{2,4\}} = 7, & \sigma_{\{1,2,3,4\}} = 11, \\ & \sigma_{\{3,4\}} = 6. & \end{array}$$

Take a set of cardinality $r = 7$ as a base unless forbidden: $\mathcal{B}_S = \emptyset$ if $\sigma_S \leq r$ and $\mathcal{B}_S = \{(b_1, b_2, b_3, b_4) \mid \sum_{i \in S} b_i = r, b_i \neq 0 \iff i \in S, \sum_{i \in S'} b_i < \sigma_{S'} \forall S' \subset S\}$ otherwise. Then $\mathcal{B}$ consists of the sets of the following types:

$(**00)$	$(0**0)$	$(0***)$	$(***0)$	$(**0*)$	$(****)$
(4300)	(0430)	(0421)	(3310)	(4201)	(3211)
(3400)		(0412)	(2410)	(4102)	(3112)
		(0331)	(2320)	(3301)	(2311)
		(0322)	(1420)	(3202)	(2221)
		(0232)	(1330)	(2401)	(2122)
				(2302)	(2212)
				(1402)	(1411)
					(1321)
					(1312)
					(1132)
					(1231)
					(1222)

The circuits $\mathcal{C}$ consists of sets of the following types:

	$(**00)$	$(*0*0)$	$(**0*)$	$(***0)$	$(0***)$	$(****)$
(5000)	(4400)	(4010)	(4301)	(3410)	(0431)	(1421)
(0500)		(3020)	(3401)	(1430)	(0422)	(1412)
(0040)		(2030)	(4202)	(2420)	(0332)	(1331)
(0003)			(3302)			(1322)
			(2402)			(1232)
						(3311)
						(3212)
						(2411)
						(2321)
						(2312)
						(2222)

It can be checked that $\mathcal{C}$ and $\mathcal{B}$ are indeed circuits and bases of a matroid. □

Base on these observations we propose the following conjecture:

Conjecture 4.5 Let $\mathcal{M}$ be a connected matroid of rank r with N strong connectivity classes $\mathcal{U}_{k_1,n_1}, \mathcal{U}_{k_2,n_2}, \ldots, \mathcal{U}_{k_N,n_N}$, $1 \leq k_i < n_i$ for all $i = 1, \ldots, N$. Then the set $\mathcal{B}$ of bases of $\mathcal{M}$ is

$$\mathcal{B} = \bigcup_{S \subseteq \{1,\ldots,N\}} \mathcal{B}_S,$$

where $\mathcal{B}_S = \emptyset$ if $\sigma_S \leq r$, otherwise,

$$\begin{aligned} \mathcal{B}_S \quad = \quad & \left\{ \text{sets of type } (b_1, b_2, \ldots, b_N) \mid b_i = 0 \Leftrightarrow i \notin S, \sum_{i \in S} b_i = r, \ 0 \leq b_i \leq k_i, \right. \\ & \left. \sum_{i \in S'} b_i < \sigma_{S'} \forall S' \subset S, \right\}, \end{aligned}$$

and $\{\sigma_S \mid S \subseteq \{1, \ldots, N\}\}$ is defined as follows: Let $\mathcal{P}^N$ be the set of all nonempty subsets of $\{1, \ldots, N\}$. Let $\mathcal{S} \neq \emptyset$ be a subset of $\mathcal{P}^N$ satisfying the following conditions:

1. $\{i\} \in \mathcal{S} \ \ \forall i \in \{1, 2, \ldots, N\}$;
2. $\forall \ i, j, \ \ \exists S \in \mathcal{S}$ such that $\{i, j\} \subseteq S$.

Let S_{max} be a member of $\mathcal{S}$ such that $|S_{max}| = \max\{|S| \mid S \in \mathcal{S}\}$. Then $r = \sigma_{S_{max}} - 1$.

The set of integers $\{\sigma_S \mid S \in \mathcal{P}^N\}$ is defined as follows:

1. $\sigma_{\{i\}} = k_i + 1$ for all $i = 1, \ldots, N$.
2. For all $S \notin \mathcal{S}$,

$$\begin{aligned} \sigma_S \quad &= \quad r + 1 \quad \text{if } |S| \geq |S_{max}|, \\ \sigma_S \quad &= \quad \min \left\{ 1 + \sum_{j=1}^{h} \left(\sigma_{S_j} - 1 \right) \ \mid S_1, \ldots, S_h \text{ is a partition of } S \right\} \quad \text{if } |S| < |S_{max}|. \end{aligned}$$

3. For all subset $S \in \mathcal{S}$,

$$\max_{\substack{S' \subset S \\ |S'| = |S| - 1}} \{\sigma_{S'}\} \leq \sigma_S \leq \min_{\substack{S_1, S_2 \subset S \\ S_1 \cup S_2 = S}} \{\sigma_{S_1} + \sigma_{S_2} - 2\}.$$

Conversely, if $\mathcal{B}$ is a set of subsets of $V_1 \cup V_2 \cup \cdots \cup V_N$ defined above, with $\{\sigma_S \mid S \in \mathcal{P}^N\}$ satisfying conditions 1, 2, 3 and 4 above, then $\mathcal{B}$ is the set of bases of a connected matroid $\mathcal{M}$ of rank r and N strong connectivity classes $\mathcal{U}_{k_1,n_1}, \mathcal{U}_{k_2,n_2}, \ldots, \mathcal{U}_{k_N,n_N}$, $k_i < n_i$ for all $i = 1, \ldots, N$. □

Conjecture 4.5 is true for the cases $N = 2$ and $N = 3$.

Example 4.6 Let $\mathcal{M}$ be a connected matroid of rank r which has $N = 2$ strong connectivity classes, $\mathcal{U}_{k_1,n_1}, \mathcal{U}_{k_2,n_2}$, $k_i < n_i$. By Theorem 4.1,

$$\max(k_1, k_2) \leq r \leq k_1 + k_2 - 1.$$

The set $\mathcal{S}$ is $\{\{1\}, \{2\}, \{1, 2\}\}$ and $S_{max} = \{1, 2\}$. The integers σ_S are defined as follows:

$$\begin{aligned} &\sigma_{\{1\}} = k_1 + 1, \\ &\sigma_{\{2\}} = k_2 + 1, \\ &\max(\sigma_{\{1\}}, \sigma_{\{2\}}) \leq \sigma_{\{1,2\}} = r + 1 \leq \sigma_{\{1\}} + \sigma_{\{2\}} - 2, \end{aligned}$$

that is, $\max(k_1 + 1, k_2 + 1) \leq \sigma_{\{1,2\}} = r + 1 \leq k_1 + k_2$. Consider the set $\mathcal{B}$:

$$\mathcal{B} = \bigcup_{S \subseteq \{1,\ldots,N\}} \mathcal{B}_S,$$

where $\mathcal{B}_S = \emptyset$ if $\sigma_S \leq r$, otherwise,

$$\mathcal{B}_S = \left\{ \text{ sets of type } (b_1, b_2) \mid b_i = 0 \Leftrightarrow i \notin S, \sum_{i \in S} b_i = r, \ 0 \leq b_i \leq k_i, \text{ and } \forall S' \subset S, \sum_{i \in S'} b_i < \sigma_{S'} \right\}.$$

Without loss of generality, let $\sigma_{\{1\}} \geq \sigma_{\{2\}}$. Then the only possibilities are:

1. $r \geq \sigma_{\{1\}}$, $r \geq \sigma_{\{2\}}$, $r < \sigma_{\{1,2\}}$.
2. $r < \sigma_{\{1\}}$, $r \geq \sigma_{\{2\}}$, $r < \sigma_{\{1,2\}}$.
3. $r < \sigma_{\{1\}}$, $r < \sigma_{\{2\}}$, $r < \sigma_{\{1,2\}}$.

In all cases, $\mathcal{B}$ consists of the sets of types

$$\begin{gathered}(k_1, r-k_1)\\ (k_1-1, r-k_1+1)\\ \vdots\\ (r-k_2, k_2).\end{gathered}$$

(Note however that in the last case $\mathcal{M}$ becomes a uniform matroid. Hence there is need for further conditions on σ_S to ensure that strongly connected components do not merge.) □

However, there is a counter example:

Example 4.7 Let $\mathcal{S} = \{\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$, so $S_{max} = \{2,3,4\}$. We have, according to Conjecture 4.5

$$\begin{array}{lll}
\sigma_{\{i\}} = k_i + 1: & S \notin \mathcal{S}: & S \in \mathcal{S}: \\
\sigma_{\{1\}} = 5, & \sigma_{\{2,3\}} = 8, & 5 \leq \sigma_{\{1,2\}} \leq 8, \\
\sigma_{\{2\}} = 5, & \sigma_{\{2,4\}} = 7, & 5 \leq \sigma_{\{1,3\}} \leq 7, \\
\sigma_{\{3\}} = 4, & \sigma_{\{3,4\}} = 6, & 5 \leq \sigma_{\{1,4\}} \leq 6, \\
\sigma_{\{4\}} = 3, & \sigma_{\{1,2,3\}} = r+1, & 8 \leq \sigma_{\{2,3,4\}} = r+1 \leq 9, \\
 & \sigma_{\{1,2,4\}} = r+1, & \\
 & \sigma_{\{1,3,4\}} = r+1, & \\
 & \sigma_{\{1,2,3,4\}} = r+1. &
\end{array}$$

Take $\sigma_{\{1,2\}} = 8$, $\sigma_{\{1,3\}} = 5$, $\sigma_{\{1,4\}} = 6$. Taking $r = 7$, we have Example 4.4. Taking $r = 8$ however, we have $\mathcal{B}$ consisting of sets of the following types:

$(**\,*0)$	$(**\,0*)$	$(0\,***)$	$(****)$	
(3410)	(4301)	(0431)	(3311)	(1421)
(2420)	(3401)	(0422)	(3212)	(1412)
(1430)	(3302)	(0332)	(2411)	(1331)
	(2402)		(2321)	(1322)
			(2312)	(1232)

Let $B_1 = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, d_1\}$ be a set of type $(4,3,0,1)$, $B_2 = \{a_1, a_2, a_3, b_1, b_2, b_3, b_4, c_1\}$ a set of type $(3,4,1,0)$, where $a_i \in V_1$, $b_i \in V_2$, $c_i \in V_3$, $d_i \in V_4$. Then $d_1 \in B_1 \setminus B_2$ while $B_2 \setminus B_1 = \{b_4, c_1\}$. However $(B_1 \cup c_1) \setminus d_1$ is a set of type $(4,3,1,0)$ and $(B_1 \cup b_4) \setminus d_1$ is a set of type $(4,4,0,0)$, neither of which is in $\mathcal{B}$. Hence $\mathcal{B}$ is not the set of bases of a matroid despite satisfying the conditions of the conjecture. □

The case $N = 3$ is analysed in the next section.

5 Conjecture 4.5 for $N = 3$

We consider the case $N = 3$. Let $\mathcal{B}$ and $\mathcal{S}$ satisfy the hypothesis of Conjecture 4.5. We consider the necessary conditions for $\mathcal{B}$ to be the set of bases of a matroid.

Let B_1 , $B_2 \in \mathcal{B}$. Let B_1 be of type (a_1, a_2, a_3) with support S_1 and B_2 of type (b_1, b_2, b_3) with support S_2. The possibilities are

(a) $S_1 = S_2$:
  - (i) $a_i = b_i$ for all i,
  - (ii) $a_i \neq b_i$ for some i.

(b) $S_1 \neq S_2$:
  - (a) $S_1 \cap S_2 = \emptyset$,
  - (b) $S_1 \subset S_2$,
  - (c) $S_1 \supset S_2$,
  - (d) $|S_1 \cap S_2| = 1$.

We consider all possibilities. We require that if $x \in B_1 \setminus B_2$ then there must be a $y \in (B_2 \setminus B_1)$ such that $(B_1 \cup y) \setminus x \in \mathcal{B}$.

(a) $S_1 = S_2$:

(i) $a_i = b_i$ for all i: If there is an $x \in B_1 \setminus B_2$, say $x \in V_1$, then since $a_1 = b_1$ there must be a $y \in (B_2 \setminus B_1) \cap V_1$. The set $(B_1 \cup y) \setminus x$ is a set of type (a_1, a_2, a_3) and hence is a base.

(ii) $a_i \neq b_i$ for some i: Suppose $x \in B_1 \setminus B_2$, $x \in V_1$. If $a_1 \leq b_1$ then there is a $y \in (B_2 \setminus B_1) \cap V_1$ such that $(B_1 \cup y) \setminus x$ is again a set of type (a_1, a_2, a_3) and hence is a base.

If $a_1 > b_1$ then, since $a_1 + a_2 + a_3 = b_1 + b_2 + b_3$, there must be a b_i such that $b_i > a_i$, $i = 2$ or 3. Say $i = 2$. There there is a $y \in (B_2 \setminus B_1) \cap V_2$. Consider the set $B = (B_1 \cup y) \setminus x$, which is of type $(d_1, d_2, d_3) = (a_1 - 1, a_2 + 1, a_3)$. We verify that B is a base:

- $d_1 + d_2 + d_3 = a_1 + a_2 + a_3 = r$.
- Since $S_1 = S_2$, $a_1 > b_1 > 0$, we have $d_1 = a_1 - 1 > 0$. Also $d_2 = a_2 + 1 > 0$, so B is of type $S_1 = S_2$ and by definition $\sigma_{S_1} > r$. So $d_i \neq 0 \iff i \in S_1$ and $\sigma_{S_1} > r$.
- We verify that $\sum_{i \in S'} d_i < \sigma_{S'}$ for all $S' \subset S_1$:
  If $1 \in S'$ and $2 \notin S'$ then $\sum_{i \in S'} d_i = \left(\sum_{i \in S'} a_i\right) - 1 < \sigma_{S'} - 1 < \sigma_{S'}$ by definition.
  If $1 \in S'$ and $2 \in S'$ then $\sum_{i \in S'} d_i = \left(\sum_{i \in S'} a_i\right) < \sigma_{S'}$.
  If $1 \notin S'$ and $2 \notin S'$ then $\sum_{i \in S'} d_i = \left(\sum_{i \in S'} a_i\right) < \sigma_{S'}$.
  Consider $1 \notin S'$ and $2 \in S'$. Then

$$\sum_{i \in S'} d_i = \left(\sum_{i \in S'} a_i\right) + 1 \leq \sigma_{S'}.$$

  If $S' = \{2\}$ then $\sum_{i \in S'} d_i = d_2 = a_2 + 1 \leq b_2 < \sigma_{S'}$.
  Suppose then that $S' = \{2, 3\}$ and $\sum_{i \in S'} d_i = d_2 + d_3 = a_2 + a_3 + 1 = \sigma_{S'}$. If $a_3 \leq b_3$ then $a_2 + a_3 + 1 < b_2 + b_3 + 1 < \sigma_{S'}$, which contradicts the assumption. So we must have $a_3 > b_3$. Let

$$\begin{aligned} a_1 &= b_1 + \Delta_1, \ \Delta_1 > 0, \\ a_2 &= b_2 - \Delta_2, \ \Delta_2 > 0, \\ a_3 &= b_3 + \Delta_3, \ \Delta_3 > 0. \end{aligned}$$

  Hence $\Delta_1 + \Delta_3 = \Delta_2$. Now $a_2 + a_3 < \sigma_{\{2,3\}}$ and $a_2 + a_3 + \Delta_1 = b_2 + b_3 < \sigma_{\{2,3\}}$ by definition. So $a_2 + a_3 + 1 = \sigma_{\{2,3\}} \leq a_2 + a_3 + \Delta_1 < \sigma_{\{2,3\}}$ which is a contradiction. Hence we must have $\sum_{i \in S'} d_i < \sigma_{\{2,3\}}$.

Hence in all cases when $S_1 = S_2$, B is a base.

(b) $S_1 \neq S_2$:

(i) $S_1 \cap S_2 = \emptyset$:

Suppose B_1 is of type $(a_1, 0, a_3)$ and B_2 of type $(0, b_2, b_3)$. If $a_3 \neq 0$ then $b_3 = 0$ and if $b_3 \neq 0$ then $a_3 = 0$. Let $x \in B_1 \setminus B_2$. Then there is a $y \in (B_2 \setminus B_1) \cap V_2$. The set $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1 - 1, 1, a_3)$.

- $d_1 + d_2 + d_3 = a_1 + a_3 = r$.
- If $a_3 = 0$ then $a_1 - 1 > 0$ and $d_i \neq 0$ if and only if $i \in \{1, 2\}$ and $\sigma_{\{1,2\}} \geq \sigma_{\{1\}} > r$.
  If $a_3 \neq 0$ then $b_3 = 0$. If $a_1 - 1 = 0$ then $d_i \neq 0$ if and only if $i \in \{2, 3\}$ and $\sigma_{\{2,3\}} \geq \sigma_{\{2\}} > r$. If $a_1 - 1 \neq 0$ then $d_i \neq 0$ if and only if $i \in \{1, 2, 3\}$ and $\sigma_{\{1,2,3\}} \geq \sigma_{\{1,3\}} > r$.
- If $a_3 = 0$ then $d_1 = a_1 - 1 < a_1 < \sigma_{\{1\}}$ and $d_2 = 1 < \sigma_{\{2\}}$.
  If $a_3 \neq 0$ then $d_1 = a_1 - 1 < a_1 < \sigma_{\{1\}}$, $d_2 = 1 < \sigma_{\{2\}}$, $d_3 = a_3 < \sigma_{\{3\}}$, $d_1 + d_2 = a_1 < \sigma_{\{1\}} \leq \sigma_{\{1,2\}}$, $d_1 + d_3 = a_1 - 1 + a_3 < \sigma_{\{1,3\}}$ and $d_2 + d_3 = a_3 + 1 \leq a_3 + a_1 = b_2 < \sigma_{\{2\}} \leq \sigma_{\{1,3\}}$.

Hence B is always a base.

(ii) $S_1 \subset S_2$:

(1) Let B_1 be of type $(a_1, 0, 0)$ and B_2 of type $(b_1, b_2, 0)$. (So $a_1 = r > 1$, $b_1 < a_1$ and $b_1 + b_2 = a_1$.) If $x \in B_1 \setminus B_2$ then there is a $y \in (B_2 \setminus B_1) \cap V_2$ such that $(B_1 \cup y) \setminus x$ is a set of type $(a_1 - 1, 1, 0)$. This is a base.

(2) Let B_1 be of type $(a_1, 0, 0)$ and B_2 of type (b_1, b_2, b_3). If $x \in B_1 \setminus B_2$ then there is a $y \in (B_2 \setminus B_1) \cap V_2$ such that $(B_1 \cup y) \setminus x$ is a set of type $(a_1 - 1, 1, 0)$ and this is a base since $\sigma_{\{1,2\}} \geq \sigma_{\{1\}} > r$.

(3) Let B_1 be of type $(a_1, a_2, 0)$ and B_2 of type (b_1, b_2, b_3). (So $a_1 + a_2 = b_1 + b_2 + b_3 = r > 2$.) Let $x \in B_1 \setminus B_2$, say $x \in V_1$. If $a_1 \leq b_1$ then the argument of (a)(i) and (ii) holds and $(B_1 \cup y) \setminus x$ is a base for some $y \in (B_2 \setminus B_1)$.

Suppose then $a_1 > b_1$. If $b_2 > a_2$ then there is a $y \in (B_2 \setminus B_1) \cap V_2$ and $(B_1 \cup y) \setminus x$ is a set of type $(a_1 - 1, a_2 + 1, 0)$, which is a base. So suppose that $b_2 \leq a_2$ and there is no $y \in (B_2 \setminus B_1) \cap V_2$. Then there is a $y \in (B_2 \setminus B_1) \cap V_3$ and $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1 - 1, a_2, 1)$.

- $d_1 + d_2 + d_3 = a_1 + a_2 = r$.
- $d_i \neq 0$ if and only if $i \in \{1, 2, 3\}$ and $d_1 + d_2 + d_3 = r < \sigma_{\{1,2\}} \leq \sigma_{\{1,2,3\}}$.
- $d_1 = a_1 - 1 < \sigma_{\{1\}}$, $d_2 = a_2 < \sigma_{\{2\}}$, $d_3 = 1 < \sigma_{\{3\}}$, $d_1 + d_2 < a_1 + a_2 < \sigma_{\{1,2\}}$, $d_1 + d_3 = a_1 < \sigma_{\{1\}} \leq \sigma_{\{1,3\}}$. Consider $d_2 + d_3 = a_2 + 1$:

$$d_2 + d_3 = a_2 + 1 \leq \sigma_{\{2\}} \leq \sigma_{\{2,3\}}.$$

So we must have either $a_2 + 1 < \sigma_{\{2\}}$ or $\sigma_{\{2\}} < \sigma_{\{2,3\}}$. Suppose $a_2 + 1 = \sigma_{\{2\}} (= k_2 + 1)$ and $\sigma_{\{2\}} = \sigma_{\{2,3\}} (= k_2 + 1)$. Since there is a base of type (b_1, b_2, b_3) we must have $b_2 + b_3 < \sigma_{\{2,3\}}$. Now let $a_1 = b_1 + \Delta_1$, $\Delta_1 > 0$, $a_2 = b_2 + \Delta_2$, $\Delta_2 \geq 0$. Then $\Delta_1 + \Delta_2 = b_3$, and

$$b_2 + b_3 = (a_2 - \Delta_2) + (\Delta_1 + \Delta_2) = k_2 + \Delta_1 < \sigma_{\{2,3\}} = k_2 + 1.$$

So $0 < \Delta_1 < 1$, which is impossible, so one of the inequalities must hold.

Hence B is always a base.

(iii) $S_1 \supset S_2$:

(1) Let B_1 be of type (a_1, a_2, a_3) and B_2 of type $(b_1, 0, 0)$. (So $b_1 > a_1$.)
If $x \in B_1 \setminus B_2$, $x \in V_1$, then there is a $y \in (B_2 \setminus B_1) \cap V_1$ such that $(B_1 \cup y) \setminus x$ is again of type (a_1, a_2, a_3) and hence is a base.
If $x \in B_1 \setminus B_2$, $x \in V_2$, then $B = (B_1 \cup y) \setminus x$ must be of type $(d_1, d_2, d_3) = (a_1 + 1, a_2 - 1, a_3)$.

- $d_1 + d_2 + d_3 = a_1 + a_2 + a_3 = r$.
- If $d_2 \neq 0$, then $d_i \neq 0$ if and only if $i \in \{1, 2, 3\}$ and $\sigma_{\{1,2,3\}} > r$ by definition. If $d_2 = 0$, then $d_i \neq 0$ if and only if $i \in \{1, 3\}$ and $\sigma_{\{1,3\}} \geq \sigma_{\{1\}} > r$, since there is a base of type $(b_1, 0, 0)$.
- $d_1 \leq b_1 < \sigma_{\{1\}}$, $d_2 < a_2 < \sigma_{\{2\}}$, $d_3 = a_3 < \sigma_{\{3\}}$, $d_1 + d_2 = a_1 + a_2 < \sigma_{\{1,2\}}$, $d_2 + d_3 < a_2 + a_3 < \sigma_{\{2,3\}}$, while $d_1 + d_3 = a_1 + a_3 + 1 \leq \sigma_{\{1,3\}}$. Now,

$$a_1 + a_3 + 1 \leq a_1 + a_2 + a_3 = b_1 \leq k_1 < \sigma_{\{1\}} \leq \sigma_{\{1,3\}}.$$

Hence B is a base.

(2) Let B_1 be of type $(a_1, a_2, 0)$ and B_2 of type $(b_1, 0, 0)$. (So $b_1 > a_1$.)
If $x \in B_1 \setminus B_2$, $x \in V_1$ then there is a $y \in (B_2 \setminus B_1) \cap V_1$ so that $(B_1 \cup y) \setminus x$ is again of type $(a_1, a_2, 0)$ and hence is a base.
If $x \in B_1 \setminus B_2$, $x \in V_2$ then there is a $y \in (B_2 \setminus B_1) \cap V_1$ so that $(B_1 \cup y) \setminus x$ is of type $(a_1 + 1, a_2 - 1, 0)$ which is a base.

(3) Let B_1 be of type (a_1, a_2, a_3) and B_2 of type $(b_1, b_2, 0)$.
Let $x \in B_1 \setminus B_2$, $x \in V_1$. If $a_1 \leq b_1$ then there is $y \in (B_2 \setminus B_1) \cap V_1$ and $(B_1 \cup y) \setminus x$ is again of type (a_1, a_2, a_3) and hence a base. If $a_1 > b_1$ then there is $y \in (B_2 \setminus B_1) \cap V_2$ and $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1 - 1, a_2 + 1, a_3)$. Since $a_1 > b_1$, we have $b_2 > a_2 + a_3$, so $a_2 + a_3 + 1 \leq b_2 < \sigma_{\{2\}} \leq \sigma_{\{2,3\}}$. So B is a base.
Let $x \in B_1 \setminus B_2$, $x \in V_3$. Without loss of generality let $b_1 > a_1$. Then there is $y \in (B_2 \setminus B_1) \cap V_1$ and $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1 + 1, a_2, a_3 - 1)$. Since $a_1 + a_2 + 1 \leq b_1 + b_2 < \sigma_{\{1,2\}}$, so B is a base.

Hence B is always a base.

(iv) $|S_1 \cap S_2| = 1$: Let B_1 be of type $(a_1, a_2, 0)$ and B_2 of type $(b_1, 0, b_3)$.

Let $x \in B_1 \setminus B_2$, $x \in V_1$. If $a_1 \le b_1$ then there is $y \in (B_2 \setminus B_1) \cap V_1$ such that $(B_1 \cup y) \setminus x$ is again a base.

If $a_1 > b_1$ then there is $y \in (B_2 \setminus B_1) \cap V_3$ such that $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1 - 1, a_2, 1)$. Now, $d_i \ne 0$ if and only if $i \in \{1,2,3\}$ and $\sigma_{\{1,2,3\}} \ge \sigma_{\{1,2\}} > r$. Since $a_1 > b_1$, we have $b_3 > a_2$. So $d_2 + d_3 = a_2 + 1 \le b_3 < \sigma_{\{3\}} \le \sigma_{\{2,3\}}$. Hence B is a base.

Let $x \in B_1 \setminus B_2$, $x \in V_2$. If $a_1 \le b_1$ the above argument holds. If $a_1 > b_1$ then there is $y \in (B_2 \setminus B_1) \cap V_3$ such that $B = (B_1 \cup y) \setminus x$ is a set of type $(d_1, d_2, d_3) = (a_1, a_2 - 1, 1)$.

If $a_2 - 1 \ne 0$ then $d_i \ne 0$ if and only if $i \in \{1,2,3\}$ and $\sigma_{\{1,2,3\}} \ge \sigma_{\{1,2\}} > r$. If $a_2 - 1 = 0$ then $d_i \ne 0$ if and only if $i \in \{1,3\}$ and $\sigma_{\{1,3\}} > r$. Also $d_1 + d_3 = a_1 + 1 = r - (a_2 - 1) \le r < \sigma_{\{1,3\}}$ or $\sigma_{\{1,2,3\}}$. So B is a base.

Hence Conjecture 4.5 holds for $N = 3$.

6 The independent sets of a matroid

Theorem 6.1 Let $\mathcal{M}$ be a connected matroid with N strong connectivity classes $V_1, \dots, V_N$, with $\mathcal{M}|_{V_i} = \mathcal{U}_{k_i, n_i}$ for $i = 1, \dots, N$. For each $S \subseteq \{1, \dots, N\}$, let

$$r_S = \operatorname{rank}(\cup_{i \in S} V_i) = \operatorname{rank}(\mathcal{M}|_{\cup_{i \in S} V_i}).$$

Then r_S, $|S| \ge 2$, satisfies

$$\max_{S' \subset S} \{r_{S'}\} \le r_S \le \min_{x, y \in S} \left\{ r_{S \setminus \{x\}} + r_{S \setminus \{y\}} - r_{S \setminus \{x, y\}} \right\},$$

and an independent set I of $\mathcal{M}$ satisfies the following:

If I is of type $(i_1, \dots, i_N)$ and support S, then

1. $i_j \le k_j$ for all $j \in S$;
2. $\sum_{j \in S} i_j \le r_S$.

□

It is clear that this theorem follows immediately from the definition of independent sets.

The converse is stated as follows:

Let V be a disjoint union of $V_1, \dots, V_N$. Let $|V_i| = n_i$ and let $k_i < n_i$ be an integer associated with V_i for $i = 1, \dots N$. For $S \subseteq \{1, \dots, N\}$, let r_S be integers such that

$$r_{\{i\}} = k_i,\ i \in \{1, \dots, N\},$$
$$\max_{S' \subset S} \{r_{S'}\} \le r_S \le \min_{x, y \in S} \left\{ r_{S \setminus \{x\}} + r_{S \setminus \{y\}} - r_{S \setminus \{x, y\}} \right\} \text{ if } |S| \ge 2.$$

Let $\mathcal{I}$ be the collection of all subsets I of V, where I is of type $(i_1, \dots, i_N)$, support S, satisfying

1. $i_j \le k_j$ for all $j \in S$;
2. $\sum_{j \in S} i_j \le r_S$.

Conjecture 6.2 The set $\mathcal{I}$ is the collection of independent sets of a matroid. □

However, there is a counter example:

Example 6.3 Let $V_1 = \{a_1, \dots, a_{n_1}\}$, $V_2 = \{b_1, \dots, b_{n_2}\}$, $V_3 = \{c_1, \dots, c_{n_3}\}$, and $k_1 = 1$, $k_2 = 2$, $k_3 = 3$. Then the following values of r_S satisfy the hypothesis of the conjecture:

$$\begin{aligned} r_{\{1\}} &= 1, & r_{\{1,2\}} &= 2, \\ r_{\{2\}} &= 2, & r_{\{1,3\}} &= 3, \\ r_{\{3\}} &= 3, & r_{\{2,3\}} &= 4, \\ & & r_{\{1,2,3\}} &= 4. \end{aligned}$$

Let $X = \{a_1, b_1, b_2, c_1\}$, so X is of type $(1,2,1)$ and $X \in \mathcal{I}$. Let $Y \subset X$, $Y = \{a_1, b_1, b_2\}$, which is of type $(1,2,0)$. Since $|Y| > r_{\{1,2\}}$, $Y \notin \mathcal{I}$. This contradicts the independent set axiom which states that any subset of an independent set is again independent. Hence $\mathcal{I}$ is not the collection of independent sets of a matroid. □

7 Conclusion

All our conjectures have failed for the case $N > 3$. The common theme in all the conjectures has been the attempt to define a structure on the equivalence classes. The problem is that this structure does not seem to be well-defined: it matters how many (though not which) points of each equivalence class is in a subset. Not all sets of a specific support and size are circuits (or bases, or independent sets) even if some of them are. For example, in Conjecture 6.2, we attempt to define r_S as a rank function, but r_S only gives the size of the largest independent set with support S and does not speficy *where* in V_i, $i \in S$, these points must be. It is likely that conditions on equivalence classes will not be sufficient to define a matroid.

References

[1] S. -L. Ng and M. Walker. On the composition of matroids and ideal secret sharing schemes. To appear in *Des. Codes. Cryptogr.*

[2] S. -L. Ng. On secret sharing matroids. Submitted to *Des. Codes. Cryptogr.*

[3] D. J. A. Welsh. *Matroid Theory.* Academic Press, London, 1976.