JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 69B, Nos. 1 and 2, January–June 1965

Minimum Partition of a Matroid Into Independent Subsets[1]

Jack Edmonds

(December 1, 1964)

A matroid M is a finite set M of elements with a family of subsets, called independent, such that (1) every subset of an independent set is independent, and (2) for every subset A of M, all maximal independent subsets of A have the same cardinality, called the rank $r(A)$ of A. It is proved that a matroid can be partitioned into as few as k sets, each independent, if and only if every subset A has cardinality at most $k \cdot r(A)$.

1.0. Introduction

Matroids can be regarded as a certain abstraction of matrices [8].[2] They represent the properties of matrices which are invariant under elementary row operations but which *are not* invariant under elementary column operations—namely properties of dependence among the columns. For any matrix over any field, there is a matroid whose elements correspond to the columns of the matrix and whose independent sets of elements correspond to the linearly independent sets of columns. A matroid M is completely determined by its elements and its independent sets of elements.

The same letter will be used to denote a matroid and its set of elements. The letter I with various sub or superscripts will be used to denote an independent set.

The interest of matroids does not lie only in how they generalize some known theorems of linear algebra. There are examples, which I shall report elsewhere, of matroids which do not arise from any matrix *over any field*—so matroid theory does truly generalize an aspect of matrices. However, matroid theory is justified by new problems in matrix theory itself—in fact by problems in the special matrix theory of graphs (networks). It happens that an axiomatic matroid setting is most natural for viewing these problems and that matrix machinery is clumsy and superfluous for viewing them. The situation is somewhat similar to the superfluity of (real) matrices to the theory of linear operators, though there a quite different aspect of matrices is superfluous. When it comes to implementing either theory, matrices are often the way to do it.

Matroid theory so far has been motivated mainly by graphs, a special class of matrices. A graph G may be regarded as a matrix $N(G)$ of zeroes and ones, mod 2, which has exactly two ones in each column. The columns are the edges of the graph and the rows are the nodes of the graph. An edge and a node are said to meet if there is a one located in that column and that row. Of course a graph can also be regarded visually as a geometric network. It is often helpful to visualize statements on matroids for the case of graphs, though it can be misleading. Matroids do not contain objects corresponding to nodes or rows.

Theorem 1 on "minimum partitions," the subject of this paper, was discovered in the process of unifying results described in the next paper, "On Lehman's Switching Game and a Theorem of Tutte and Nash-Williams" (denoted here as "Part II"), which is a direct sequel. Theorem 1 is shown there to be closely related to those results. Lately, I have learned that Theorem 1 for the case of graphs (see sec. 1.7) was anticipated by Nash-Williams [5].

By borrowing from work of others, I intend that this paper together with possible sequels be partly expository and technically almost self-contained.

1.1. The Problem

Various aspects of matroids—in particular, the first pair of axioms we cite—hold intrinsic interest which is quite separate from linear algebra.

AXIOM 1: *Every subset of an independent set of elements is independent.*

Any finite collection of elements and family of so-called independent sets of these elements which satisfies axiom 1 we shall call an independence system. This also happens to be the definition of an abstract simplicial complex, though the topology of complexes will not concern us.

It is easy to describe implicitly large independence systems which are apparently very unwieldy to analyze. First example: given a graph G, define an *independent* set of nodes in G to be such that no edge of G meets two nodes of the set. Second example: define an independent set of edges in G to be such that

[1] Sponsored by the Army Research Office (Durham). Presented at the Seminar on Matroids, National Bureau of Standards, Aug. 31-Sept. 11, 1964. I am much indebted to Alfred Lehman for encouraging my interest in the subject.

[2] Figures in brackets indicate the references at the end of this paper.

no node meets two edges of the set. Third example: define an independent set of edges in G to be such that the edges of the set, as column vectors of $N(G)$, are linearly independent. The third example is the prototype of the systems we shall study here.

A *minimum coloring* of the nodes of a graph G is a partition of the nodes into as few sets (colors) as possible so that each set is independent. A good characterization of the minimum colorings of the nodes in a graph is unknown (unless the graph is bipartite, i.e., the nodes can be colored with two colors). To find one would undoubtedly settle the "four color" conjecture.

A problem closely related to minimum coloring is the "packing problem." That is to find a good characterization (and an algorithm) for maximum cardinality independent sets. More generally the "weighted packing problem" is, where each element of the system carries a real numerical weight, to characterize the independent sets whose weight-sums are maximum. The packing problem for the systems of the first example is also very much unsolved (unless the graph is bipartite).

The minimum coloring problem for the systems of the second example is unsolved (unless the graph is bipartite). Its solution would also undoubtedly settle the four-color conjecture. However the packing problem, and more generally the weighted packing problem, is solved for the second example by the extensive theory of "matchings in graphs."

For the third example the packing problem is in a sense trivial. It is well known that the system of linearly independent sets of edges in a graph, and more generally the system of linearly independent sets of columns in a matrix, satisfies the following:

AXIOM 2: *For any subset A of the elements, all maximal independent sets contained in A contain the same number of elements.*

A *matroid* is a (finite) system of elements and sets of elements which satisfies axioms 1 and 2.

For any independence system, any *subsystem* consisting of a subset A of the elements and all of the independent sets contained in A is an independence system. Thus, a matroid is an independence system where the packing problem is postulated to be trivial for the system and all of its subsystems. For me, having spent much labor on packing problems, it is pleasant to study such systems. Matroids have a surprising richness of structure, as even the special case of graphic matroids shows.

Clearly, a subsystem of a matroid M is a matroid. We call it a *submatroid* and we use the same symbol to denote it and its set of elements. The *rank*, $r(A)$, of a set A of elements in M or the *rank*, $r(A)$, of the submatroid A of M is the number of elements in each maximal independent set contained in A, i.e., the number of elements in a base of A.

The main result of this paper is a solution of the minimum coloring problem for the independent sets of a matroid. Another paper will treat the weighted packing problem for matroids.

1.2. Ground Rules

One is tempted to surmise that a minimum coloring can be effected for a system by some simple process like extracting a maximal independent set to take on the first color, then extracting a maximal independent set of what is left to take on the second color, and so on till all elements are colored. This is usually far from being successful even for matroids, though it is precisely matroids for which a similar sort of monotonic procedure always yields a maximum cardinality independent set and, as we shall see, in another paper, also always yields a maximum weight-sum independent set when the elements carry arbitrary real weights.

Consider the class of matroids implicit in the class M_F of all matrices over fields of integers modulo primes. (For large enough prime, this class includes the matroid of any matrix over the rational field.) We seek a good algorithm for partitioning the columns (elements of the matroid) of any one of the matrices (matroids) into as few sets as possible so that each set is independent. Of course, by carrying out the monotonic coloring procedure described above in all possible ways for a given matrix, one can be assured of encountering such a partition for the matrix, but this would entail a horrendous amount of work. We seek an algorithm for which the work involved increases only algebraically with the size of the matrix to which it is applied, where we regard the size of a matrix as increasing only linearly with the number of columns, the number of rows, and the characteristic of the field. As in most combinatorial problems, finding a finite algorithm is trivial but finding an algorithm which meets this condition for practical feasibility is not trivial.

We seek a good characterization of the minimum number of independent sets into which the columns of a matrix of M_F can be partitioned. As the criterion of "good" for the characterization we apply the "principle of the absolute supervisor." The good characterization will describe certain information about the matrix which the supervisor can require his assistant to search out along with a minimum partition and which the supervisor can then use with ease to verify with mathematical certainty that the partition is indeed minimum. Having a good characterization does not mean necessarily that there is a good algorithm. The assistant might have to kill himself with work to find the information and the partition.

Theorem 1 on partitioning matroids provides the good characterization in the case of matrices of M_F. The proof of the theorem yields a good algorithm in the case of matrices of M_F. (We will not elaborate on how.) The theorem and the proof apply as well to all matroids via the matroid axioms. However, the "goodness" for matrices depends on being able to carry out constructively with ease those matrix operations which correspond to the existential assertions of the theory. A fundamental problem of matroid theory is to find a good representation for general matroids—good perhaps relative to the rank and the number of elements in the matroids. There is a very elegant lattice representation (geometric lattices, [1, 2]), but it is not something you would want to record except for the very simplest matroids.

1.3. The Theorem

The cardinality of a set A is denoted by $|A|$. The rank of a set A is denoted by $r(A)$.

THEOREM 1: *The elements of a matroid* M *can be partitioned into as few as* k *sets, each of which is independent, if and only if there is no subset* A *of elements of* M *for which*

$$|\mathrm{A}| > \mathrm{k} \cdot \mathrm{r(A)}.$$

The theorem makes sense for any independence system M if we define the rank $r(A)$ of any subset A to be the maximum cardinality of an independent set in A. In fact, the "only if" part of the theorem is true for any independence system M. Let $I_i (i=1, \ldots, k)$ be k independent sets in M for which

$$\bigcup_{i=1}^{k} I_i = M.$$

For any subset A of M, $|I_i \cap A| \leq r(A)$ and

$$|A| \leq \sum_{i=1}^{k} |I_i \cap A| \leq k \cdot r(A).$$

Thus the "only if" part is proved.

In general for the coloring problem in nonmatroidal systems, the other half of the theorem is not true. However, the Konig theorem on matchings in bipartite graphs can be regarded as a valid instance of theorem 1 for certain nonmatroidal systems. A bipartite graph is a graph whose nodes can be partitioned into two sets each independent (by coincidence, an instance of the coloring problem in our first example). The Konig theorem says that for a bipartite graph G the minimum number of nodes which meet all the edges equals the maximum number of edges such that no node meets more than one of them. (This theorem solves the packing problem for a special case of our second example of independence system.)

Fourth example: For a graph G, let the elements of the system M be the edges of G. For each node of G, let the set of edges which meet the node be an independent set in M. Let the subsets of these sets be the rest of the independent sets in M. The Konig relation for a graph G implies theorem 1 for system M.

Theorem 1 for the system M arising from G does not imply the Konig theorem for G. For independence systems in general the relation represented by theorem 1 is weaker than the relation represented by the Konig theorem—the latter being that the minimum number of independent sets which together contain all the elements equals the maximum number of elements in a set of rank one. It's nice to have the weaker relation of theorem 1 because it might apply to other systems where the well known Konig relation does not.

1.4. Terminology

There are various families, (1) through (6), of subsets of the elements in a matroid M which are used in describing the structure of M.

(1) The family of independent sets of M.

(2) The family of minimal dependent sets of elements in M (where dependent means not independent). These are called the *circuits* in M. The letter C with various sub or superscripts will be used to denote a circuit.

(3) The family of *spans* or *closed sets* in M. A *span* S in M is a set of elements such that no circuit of M contains exactly one element not in S. That is, $|S \cap C| \neq 1$ for every circuit C in M.

The *span* or *closure of* a subset A of M is the minimal span in M which contains A. Clearly, the span of A, which we always denote by $S(A)$, is unique. Where A is a subset of column vectors in a matrix M of column vectors, $S(A)$ is all the columns in M which are linear combinations of A.

The terms above are used extensively in section 1.5 and section 1.6 to prove theorem 1. The terms below, through (4) and (5), are used extensively in Part II.

A subset A of M is said *to span* a subset K of M when $K \subset \mathrm{S(A)}$. It follows from proposition 4, to come, that A spans K in M if and only if for each element $e \epsilon K$ either $e \epsilon A$ or their is a circuit C of M such that $e \epsilon C$ and $C - e \subset A$.

(4) The family of spanning sets of M. A *spanning subset* of M is a subset of M which spans M—in other words, a subset of M whose span is M.

(5) The family of bases of M. A *base* of M is a maximal independent set of M. A base can also be defined as a minimal spanning set of M.

The terms in (1), (2), and (5) are taken from Whitney [8]. The terms "closed set" and "span of A" are taken from Lehman [3]. There is an alternative terminology due to Tutte [7]. Since these are major sources on matroids, it is worthwhile to set down the relationship. To do so it is necessary to invoke the much used notion of "dual matroid," though it is not used here or in Part II. Papers [3], [7], and [8] show that the set-complements of the bases in a matroid M are the bases of a so-called *dual matroid* M*.

The bases of matroid M are called by Tutte the *dendroids* of M. The elements of M are called by Tutte the *cells* of M. The independent sets of M are called by Lehman the *trees* of M.

The circuits of a matroid M are what Tutte calls the *atoms* of dual matroid M^*. The circuits of M^* are the atoms of M. Thus here is another special family of subsets of a matroid M.

(6) The family of atoms (dual circuits) in M.

The rows of a matrix N_0, under addition and subtraction, generate a group of row vectors which Tutte calls a *chain-group*, say the *chain-group* N of matrix N_0. The matroid M of matrix N_0 is of course an invarient of chain-group N, and it is what Tutte calls the matroid of chain-group N. An *atom* of M of N is defined as a set of elements in M which corresponds to a minimal nonempty set of row-vector components such that there is some member of chain-group N which has its nonzero values in precisely these components. The row-vectors orthogonal to each row of matrix N_0 form another chain-group, say N^*. Its matroid is M^*, the dual of M. Atoms of M^* by definition correspond to minimal dependent sets of columns in matrix N_0. That is, they are the circuits of the matroid M of N_0.

Tutte defines a flat of matroid M to be a union of atoms of M, or the empty set. It can be shown that a flat of M is the set-complement of a span (closed set) in M, and conversely.

Where A is a subset of elements in M, Tutte denotes by $M \cdot A$ what here is called the submatroid A of M (following Whitney). The meanings of the rank $r(M)$ of matroid M coincide, and Tutte denotes by $r(M \cdot A)$ what here is called the rank $r(A)$ of set A in M (following Whitney). However, for a set A, what Tutte denotes by r A *is not* $r(A)=r(M \cdot A)$ but "$r(M \times A)$" which is used in Part II.

1.5. The Lemmas

In the proof of theorem 1 we will use axiom 1 and the following axiom 2′ for matroids instead of axioms 1 and 2.

AXIOM 2′: *The union of any independent set and any element contains at most one circuit (minimal dependent set).*

PROPOSITION 1: *Axioms 1 and 2′ are equivalent to axioms 1 and 2.*

PROOF: Assuming 1 and 2, suppose independent set I together with element e contains two distinct circuits C_1 and C_2. Assume I is minimal for this possibility. $e \epsilon C_1 \cap C_2$. There is an element $e_1 \epsilon C_1 - C_2$ and an element $e_2 \epsilon C_2 - C_1$. Set $I \cup e - e_1 - e_2$ is independent since otherwise $(I - e_1)$ is a smaller independent set than I for which $(I - e_1) \cup e$ contains more than one circuit. Set I and set $I \cup e - e_1 - e_2$ are maximal independent subsets of set $I \cup e$. This contradicts axiom 2.

Assuming 1 and 2′, suppose I_1 and I_2 are both maximal independent subsets of a set A such that $|I_1| < |I_2|$. Assume $I_1 \cup I_2$ is minimal for this possibility. There is an e_1 in $I_1 - I_2$ and $I_2 \cup e_1$ is dependent. By 2′, $I_2 \cup e_1$ contains a unique circuit C which must contain some element e_2 not in I_1. Since I_2 is larger than I_1 it must contain another element besides e_2 not in I_1 and hence $I_2 \cup I_1 - e_2$ is dependent. Therefore, since $I_2 \cup e_1 - e_2$ is independent, there is some I_1' such that $e_1 \epsilon I_1' \subset I_1 - I_2$ and such that $I_2' = I_2 \cup I_1' - e_2$ is maximal independent in A. Because I_1' contains an element not in I_2, $|I_2'| \geqslant |I_2| > |I_1|$. However, since $I_1 \cup I_2'$ is a proper subset of $I_1 \cup I_2$, this contradicts the minimality assumption for $I_1 \cup I_2$. The proposition is proved.

PROPOSITION 2: *Axioms 1 and 2′ are equivalent to the following axioms,* 1_c *and* 2_c, *for a matroid in terms of its circuits (where starting with circuits, independent sets are defined as sets containing no circuits).*

AXIOM 1_c: No circuit contains another circuit.

AXIOM 2_c: If distinct circuits C_1 and C_2 both contain an element e then $C_1 \cup C_2 - e$ contains a circuit.

A proof of proposition 2 is obvious.

The next very useful proposition is taken in [7] and [8] to be an axiom instead of 2_c. Alfred Lehman discovered that 1_c and 2_c suffice.

PROPOSITION 3: If C_1 and C_2 are circuits of a matroid M with an element $e \epsilon C_1 \cap C_2$ and an element $a \epsilon C_1 - C_2$, then there is a circuit C such that

$$a \epsilon C \subset C_1 \cup C_2 - e.$$

PROOF (Lehman): Assuming 1_c and 2_c, suppose C_1, C_2, a, and e are such that the theorem is false and $C_1 \cup C_2$ is minimal. There is a circuit $C_3 \subset C_1 \cup C_2 - e$, but $a \notin C_3$. There is an element $b \epsilon C_3 \cap (C_2 - C_1)$. By minimality of $C_1 \cup C_2$ for falsity of the theorem and since $a \notin C_2 \cup C_3$, there is a circuit C_4 such that $e \epsilon C_4 \subset C_2 \cup C_3 - b$. Again by the minimality and since $b \notin C_1 \cup C_4$, there is a circuit C such that

$$a \epsilon C \subset C_1 \cup C_4 - e \subset C_1 \cup C_2 - e,$$

contradicting the falsity of the theorem.

PROPOSITION 4: *An element* e *of a matroid* M *is in the span* S(A) *of a set* A *in* M *if and only if* e *is in* A *or there is a circuit* C *of* M *for which* C − A = e.

PROOF: The "if" part of the theorem is asserted in the definition of span. Assuming the "only if" part false, by the definition of span there must be an A and $e \epsilon S(A) - A$ for which there is no C with $C - A = e$ but for which there is a C and nonempty E with $C - (A \cup E) = e$ where for each $e' \epsilon E$ there is a C' with $C' - A = e'$. Assume E to be minimal so that $E \subset C$. By prop. 3, for any e' and C' there is a C_1 for which $e \epsilon C_1 \subset C \cup C' - e'$. Hence, $C_1 - (A \cup E_1) = e$ where E_1 is a proper subset of E, contradicting the minimality of E.

Besides axioms 1 and 2′ and the definitions of circuit and span, the only other fact on matroids used to prove theorem 1 is

PROPOSITION 5: *The span of a set* A *in a matroid* M *is the (unique) maximal set* S *in* M *which contains* A *and which has the same rank as* A.

In particular the additional fact used in proving theorem 1 is that the span of an independent set I has rank equal to the cardinality of I.

PROOF OF PROP 5: If, for $S(A)$ the span of A, $r(S(A)) > r(A)$, then by axiom 2 a base I of A is not a base of S(A), i.e., there is an element $e \epsilon S(A) - I$ such that $I \cup e$ is independent. By prop. 4, e is not in the span $S(I)$ of I but A is in $S(I)$. Since the span of a set is the minimal span containing the set, $S(A) \subset S(I)$. Thus, by contradiction, $r(S(A)) = r(A)$.

Let $e \epsilon S'(A)$ where $A \subset S'(A)$ and $r(A) = r(S'(A))$. Then, where I is a base of A, either $e \epsilon I$ or $e \cup I$ is dependent. Thus $e \epsilon S(A)$. Therefore, $S(A)$ is the unique maximal set where $A \subset S(A)$ and $r(S(A)) = r(A)$.

1.6. The Main Proof

PROOF of theorem 1 (the "if" part): Assume that for every subset A of matroid M, $|A| \leqslant k \cdot r(A)$. Actually, it is sufficient that for every span S in M, $|S| \leqslant k \cdot r(S)$.

The goal is to get all the elements of M into just k independent sets of M. Let F be a family of k mutually disjoint independent sets of M. Any number of these sets may be empty. These sets are to be regarded as labeled so that each may be altered in the course of the proof while still maintaining its label-identity. Suppose there is an element x of M such that $\cup\{I : I\epsilon F\} \subset M-x$. We shall see how to rearrange elements among the members of F to make room for x in one of them while preserving the independence (and mutual disjointness) of them all. The process can be repeated until each element of M is in a member of F. Thus the theorem will be proved.

Implementing this proof to an algorithm for partitioning (if possible) a matroid M into k independent sets is quite straight-forward as long as an algorithm is known for the following: for any $A\subset M$ and $e\epsilon M$, find a circuit C such that $e\epsilon C\subset A\cup e$ or else determine that there is none. In the algorithm for partitioning M, one of course would *not* first verify $|A| \leqslant k \cdot r(A)$ for all $A\subseteq M$, but would simply proceed on the assumption that it is true and then stop if a contradiction arises.

If every member of F contained as many as $r(M)$ elements, then since they are disjoint and do not contain x, the union of all k of them together with x, which is a subset of M, would have cardinality greater than $k \cdot r(M)$. However, $|M| \leqslant k \cdot r(M)$. Hence there is an $I_1\epsilon F$ for which $|I_1| < r(M)$. Similarly, $x\epsilon S_1 = S(I_1)$ implies that there is an $I_2\epsilon F$ for which $|I_2\cap S_1| < r(S_1)$, since if each member of F had $r(S_1)$ elements in S_1, then their union together with x would be more than $k \cdot r(S_1)$ elements in S_1, but $|S_1| \leqslant k \cdot r(S_1)$.

Denoting M by S_0, then likewise in general

$$x\epsilon S_i = S(I_i\cap S_{i-1})$$

implies that there is an $I_{i+1}\epsilon F$ for which $|I_{i+1}\cap S_i| < r(S_i)$, since $|S_i| \leqslant k \cdot r(S_i)$. These I_i's are not necessarily distinct members of F.

Where

$$S_{i+1} = S(I_{i+1}\cap S_i),$$

we have

$$r(S_{i+1}) < r(S_i).$$

Since rank is a nonnegative integer, we must eventually reach an integer h for which

$$x\notin S_h = S(I_h\cap S_{h-1})$$

and

$$x\epsilon S_i \text{ for } i=1, \ldots, h-1.$$

By construction, $S_1\supset S_2\supset \ldots \supset S_h$.

If $I_h\cup x$ is independent then replacing I_h by $I_h\cup x$ disposes of x. Otherwise there is a unique circuit $C\subset I_h\cup x$. Since $C-x\subset S_{h-1}$ would imply $x\epsilon S_h = S(I_h\cap S_{h-1})$, there is an $x_1\epsilon C-x$ such that $x_1\notin S_{h-1}$. We replace I_h in F by independent set $I_h\cup x-x_1$. The new family is still called F and the new set carries the label-identity in F which I_h had. This and the following informal conventions are used simply to avoid introducing a lot more indices. Any other I_i which was the same member of F as I_h is now $I_h\cup x-x_1$. We will distinguish between the current I_i and the original I_i. The S_i's do not change.

We have disposed of x and now we must find a place for x_1 in some member of F. Since $x_1\notin S_{h-1}$ and $x_1\epsilon S_0$, and since the S_i's are monotonically nested, there is some index $i(1) \leqslant h-1$ for which

$$x_1\notin S_{i(1)} \text{ and } x_1\epsilon S_{i(1)-1}.$$

Denote h by $i(0)$ and denote x by x_0. Assume inductively that $x_0\notin S_{i(0)}$, $x_0\epsilon S_{i(0)-1}$, $x_1\notin S_{i(1)}$, $x_1\epsilon S_{i(1)-1}, \ldots,$ $x_j\notin S_{i(j)}$, $x_j\epsilon S_{i(j)-1}$, where $i(0) > i(1) > \ldots > i(j)$. Assume further that $I_{i(0)}$ was replaced in F by $I_{i(0)}\cup x_0 - x_1$, then $I_{i(1)}$ was replaced in F by $I_{i(1)}\cup x_1 - x_2, \ldots,$ and then $I_{i(j-1)}$ was replaced in F by $I_{i(j-1)}\cup x_{j-1} - x_j$; where $x_1\epsilon C_0\subset I_{i(0)}\cup x_0$, $x_2\epsilon C_1\subset I_{i(1)}\cup x_1, \ldots,$ and $x_j\epsilon C_{j-1}\subset I_{i(j-1)}\cup x_{j-1}$.

Suppose there is a circuit $C_j\subset I_{i(j)}\cup x_j$. Set $I_{i(j)}$ might have the same label-identity in F as $I_{i(q)}$ for several values of $q<j$, and so the contents of $I_{i(j)}$ may have changed several times since the original $I_{i(j)}$ which gave rise to $S_{i(j)} = S(I_{i(j)}\cap S_{i(j)-1})$. In particular, x_q for some $q<j$ may have been adjoined to $I_{i(j)}$. However, by the induction hypothesis any such x_q is contained in $S_{i(q)-1}$ and thus in $S_{i(j)}$.

Therefore all elements of $C_j - x_j$ which are not in the original $I_{i(j)}$ are in $S_{i(j)}$. By definition of $S_{i(j)}$, all elements of the original $I_{i(j)}$ which are in $S_{i(j)-1}$ are also in $S_{i(j)}$. Thus if all elements of $C_j - x_j$ are in $S_{i(j)-1}$ then they are all in $S_{i(j)}$, but since $S_{i(j)}$ is a span then x_j also would be in $S_{i(j)}$, contradicting the inductive hypothesis. Hence, there exists some element x_{j+1} of C_j such that $x_{j+1}\notin S_{i(j)-1}$. Since $x_{j+1}\epsilon S_0$, there is some $i(j+1) < i(j)$ such that $x_{j+1}\notin S_{i(j+1)}$ and $x_{j+1}\epsilon S_{i(j+1)-1}$.

Therefore when there exists a C_j, we repeat the inductive step by replacing $I_{i(j)}$ by $I_{i(j)} \cup x_j - x_{j+1}$.

Since $i(0) > i(1) > \ldots$, eventually we must reach an $i(j)$ for which there is no $C_j\subset I_{i(j)}\cup x_j$. Then we can replace $I_{i(j)}$ in F by independent set $I_{i(j)} \cup x_j$ without having to displace another element x_{j+1}. End of proof.

1.7. Corollary

For the special case where M is the matroid of a graph G, theorem 1 can be simplified somewhat:

Corollary (Nash-Williams [5]): *The edges of a graph* G *can be colored with as few as* k *colors so that no circuit of* G *is all one color, if and only if there is no subset* U *of nodes in* G *such that, where* E_U *is the set of edges in* G *which have both ends in* U,

$$|E_U| > k(|U|-1).$$

Symbols $|U|$ and $|E_U|$ denote, respectively, the cardinalities of U and E_U.

Not every subset A of elements in the matroid $M(G)$ of G, nor even every closed set A of elements in $M(G)$, corresponds to a set of edges of type E_U. However, the relation $|A| \leqq k \cdot r(A)$ for every set A corresponding to a set E_U of edges which form a connected subgraph of G implies the relation for every subset A of elements in $M(G)$.

The corollary follows (we omit the proof) from theorem 1 by using the following characterization of the rank function of a graph due to Whitney:

The rank $r(E)$ of any subset E of edges in G, i.e., the rank of the matroid subset corresponding to E, equals the number of nodes minus the number of connected components in the subgraph, $G \cdot E$, consisting of the edges E and the nodes they meet, or equivalently in the subgraph, $G : E$, consisting of the edges E and all the nodes of G. The notation $G \cdot E$ and $G : E$ is due to Tutte, chapter III of [7].

References

[1] G. Birkhoff, Abstract linear dependence and lattices, Amer. J. Math. 57, 800–804 (1935).

[2] H. Crapo, Single-element Extensions of Matroids, J. Res. NBS 69B (Math. and Math. Phys.) No. 1,

[3] A. Lehman, A solution of the Shannon switching game, Univ. of Wisc. Math. Research Center Report #308, 1962, to appear in the SIAM Journal.

[4] C. St. J. A. Nash-Williams, Edge-disjoint spanning trees of finite graphs, J. London Math. Soc. **36,** 445–450 (1961).

[5] C. St. J. A. Nash-Williams, Decomposition of finite graphs into forests, J. London Math. Soc. **39,** 12 (1964).

[6] W. T. Tutte, On the problem of decomposing a graph into n connected factors, J. London Math. Soc. **36,** 221–230 (1961).

[7] W. T. Tutte, Lectures on matroids, J. Res. NBS 69B (Math. and Math. Phys.) No. 1,

[8] H. Whitney, On the abstract properties of linear dependence, Amer. J. Math. 57, 509–533 (1935).

(Paper 69B1–134)