ON DEPENDENCE IN MATROIDS

D. J. A. Welsh

In this note we study dependence in matroids as an exercise in combinational algebra. Because the work seems to have little connection with graph theory we will not use Tutte's approach (1) which uses dual concepts. To define a matroid we use Edmunds (2).

A matroid is a finite set S together with a family $\underline{M}$ of independent subsets of S such that (1) every subset of an independent set is independent. (2) For every subset A of S all maximal independent subsets of A have the same cardinality, called the rank $r(A)$ of A. $A \subset S$ is a dependent subset of $(S, \underline{M})$ if A is not independent.

An element x is dependent on a set Y if

$$r(x+Y) = r(Y).$$

A base is a maximal independent set of $(S, \underline{M})$. Clearly every element of S is dependent on a base of $(S, \underline{M})$.

If x, y are members of S we write

$$x \sim y$$

if x is dependent on y. It is easy to see that $\sim$ is an equivalence relation on the set S. Let now B be any fixed base of $(S, \underline{M})$. For any $x \varepsilon S$ define $D(x, B) \equiv D(x)$ to be the subset A of B such that x is dependent on A but on no proper subset of A.

THEOREM 1. $D(x)$ is uniquely defined.

Proof. When $\{x\}$ is a dependent set then $D(x)$ is the null set. When $x \varepsilon B$ then $D(x) = x$. When $x \notin B$ theorem 1 is a particular case of Lemma 3 of Edmunds and Fulkerson (3).

Let $B = (b_1, b_2, \ldots b_r)$. Let f be the mapping of S into the set of r-tuples of zeros and ones defined by

$$f(x) = (x_1, x_2, \ldots x_r)$$

https://doi.org/10.4153/CMB-1967-060-3 Published online by Cambridge University Press

where $x_i = 1$ if $b_i \varepsilon D(x)$ and $= 0$ otherwise.

By theorem 1, $f(.)$ is a well defined function. Clearly $f(x)$ is the zero vector if and only if $\{x\}$ is dependent. Less obvious is

THEOREM 2. If both x and y are independent elements but $x \sim y$ then $f(x)$ and $f(y)$ are identical.

Proof: It is sufficient to prove that

$$D(x) = D(y).$$

Let $D(x) = A$ so that

$$r(A + x) = |A| \tag{1}$$

Now $r(x + y + A) \geqslant r(A)$. Suppose $r(x + y + A) = r(A) + 1$. Then the maximal independent subset of $x + y + A$ containing x would have cardinality $r(A) + 1$. This implies that either

a) $(x + A)$ is independent

or

b) $(x + y + A - c)$ is independent for some $c \varepsilon A$.

a) would imply $r(x + A) = |A| + 1$ contradicting (1), and b) would imply (x, y) is independent, contradicting the dependence of x on y. Hence $r(x + y + A) = r(A)$. Hence $r(y + A) \leqslant r(A)$ and thus $D(y) \subset D(x)$. Interchanging x and y in the argument above we get the required result.

We may now define an 'inner product' on the elements of the matroid $(S, \underline{M})$ by letting

$$<x, y> = \sum_{i=1}^{r} x_i y_i$$

where

$$(x_1, x_2, \ldots x_r) = f(x)$$

$$(y_1, y_2, \ldots y_r) = f(y)$$

Two elements x, y of S are said to be orthogonal if

$$<x, y> = 0$$

https://doi.org/10.4153/CMB-1967-060-3 Published online by Cambridge University Press

LEMMA 1. Distinct elements of the base B are orthogonal.

LEMMA 2. If x is orthogonal to y and z is dependent on x then z is orthogonal to y.

Proof: By theorem 2, $D(z) = D(x)$. x orthogonal to y implies

$$D(x) \cap D(y) = \phi$$

and thus

$$D(z) \cap D(y) = \phi$$

which implies $\langle z, y\rangle = 0$.

A set A of elements of S is an orthogonal set if any two distinct members of A are mutually orthogonal.

LEMMA 3. Any subset of the fixed base B is an orthogonal set.

The proof of this lemma is trivial but we also have the stronger result.

THEOREM 3. If A is any orthogonal set in a matroid and A does not contain any dependent singletons then A is an independent set.

This is analogous to the theorem that non-zero orthogonal vectors in a Euclidean vector space are linearly independent. The converse of this is, as expected, untrue (see the example in the conclusion).

To those familiar with (1) and (4) it is apparent that when $x \notin B$, $x + D(x)$ is the fundamental circuit of the matroid determined by B and the element x. Fundamental circuits are extremely important in the theory of binary matroids (Tutte (1)). It is clear that theorem 3 has a corollary:

If $C(x), C(y), \ldots C(w)$ are disjoint fundamental circuits of a matroid determined by a fixed B and elements $x, y, \ldots w$ then $x, y, \ldots w$ is an independent set of the matroid.

https://doi.org/10.4153/CMB-1967-060-3 Published online by Cambridge University Press

Proof of Theorem 3. Let $A = \{a_1, a_2, \ldots, a_n\}$ and let $A \cap B = \phi$. Let $D(a_i) = A_i$. Suppose A is a dependent set. Then by Whitney (4) it contains a circuit (minimal dependent set). Without loss of generality let this circuit be

$$A' = \{a_1, a_2, \ldots a_k\} .$$

Now by definition $a_1 + A_1$ is a circuit. Hence by a fundamental property of circuits (Whitney (4)),

$$A_1' = a_2 + \ldots + a_k + A_1$$

must contain a circuit C_1. C_1 must contain a subset of $\{a_2 \ldots a_k\}$ since A_1 is a subset of B and hence is independent. Let $C_1 = a_2 + C_1'$. But $a_2 + A_2$ is a circuit and hence

$$A_2' = C_1' + A_2$$

must contain a circuit C_2. Again C_2 must contain an element of $\{a_3 \ldots a_k\}$. Let it be a_3. Then $a_3 + A_3$ a circuit implies that $A_3' = a_4 + \ldots + a_k + A_3$ contains a circuit. Repeating the above k times we eventually arrive at the contradiction that either a subset of $A_1 + A_2 + \ldots A_k$ is a circuit or that the null set is a circuit.

This proves the theorem when $A \cap B = \phi$. Suppose now that $A = A' + B' \subset B$, and $A' \cap B = \phi$. Let A be dependent. Then A again contains a circuit C which must contain elements of A'. Let $C = a_1 + a_2 + \ldots a_k + D$ where D is a subset of B' and hence of B. Using the above argument on the set $a_1 \ldots a_k$, it is easy to see that we again get contradiction that a subset of B contains a circuit.

This completes the proof of the whole theorem. Theorem 3 can also be proved constructively by finding a base of the matroid containing the orthogonal set A.

Conclusion. Although most of the above is prompted by results in ordinary vector space theory this 'vector representation' is in no way an attempt to imbed a matroid in a vector space in such a way as to preserve dependence relations. This is an extremely difficult unsolved problem. For example: Let $(S, \underline{M})$ be the matroid

$$S = \{1, 2, 3, 4, 5\}$$

with bases all subsets of three elements which contain the element $\{1\}$. Let the fixed base B be $\{1, 2, 3\}$. Then the 'vector representations' of the elements 4, 5 as defined above are both $(0, 1, 1)$ whereas $(4, 5)$ is an independent set in the matroid. However the following conjectures seem likely to be true and give interesting problems in combinational matroid theory.

Problem 1. Let A be any independent set. The span of A is the set of elements dependent on A, (see Edmunds (2)). Let x be an element of $(S, \underline{M})$ which is orthogonal to every element of A. Then x is orthogonal to every element in the span of A.

Problem 2. Let B be the fixed base defining the vector representation. Let $B' \equiv (c_1, c_2, \ldots, c_r)$ be any other base of $(S, \underline{M})$, and let $(c_{i1}, c_{i2}, \ldots, c_{ir})$ be the vector representation of c_i. Then the matrix $\underline{C} \equiv \{c_{ij}\}$ is a unimodular matrix.

REFERENCES

1. W. T. Tutte, Lectures on Matroids, J. Res. NBS 69B 1-47, (1965).

2. J. Edmunds, Minimum Partition of a Matroid into Independent Subsets, J. Res. NBS 69B 67-72 (1965).

3. J. Edmunds and D.R. Fulkerson, Transversals and Matroid Partition, J. Res. NBS 69B 147-153 (1965).

4. H. Whitney, The Abstract Properties of Linear Dependence, Amer. J. Math. 57 507-533 (1935).

Merton College, Oxford.