JOURNAL OF COMBINATORIAL THEORY, Series B 56, 69–73 (1992)

# On Secret-Sharing Matroids

P. D. SEYMOUR

*Bellcore, 445 South St., Morristown, NJ 07962*

*Communicated by the Editors*

Received October 23, 1990

A matroid $M$ is *secret-sharing* if there is a finite set $S$ and a matrix $A=(a_{ij}: i\in I, j\in E(M))$ with entries in $S$, such that for all $X\subseteq E(M)$, the submatrix $(a_{ij}: i\in I, j\in X)$ has precisely $|S|^{\mathrm{rk}(X)}$ distinct rows. Such matroids occur naturally in the study of secret-sharing schemes in cryptography. Brickell and Davenport (*J. Cryptography*, to appear) asked if every matroid is a secret-sharing matroid. We answer this negatively, by showing that the Vamos matroid is not. 

## 1. INTRODUCTION

Let $A=(a_{ie}: i\in I, e\in E)$ be a finite matrix with entries from some finite set $S$. For $i\in I$, $e\in E$, and $X\subseteq E-\{e\}$, let us define

$$n(i, e, X)=\{a_{je}: j\in I, a_{jx}=a_{ix} \text{ for all } x\in X\}.$$

We say that $A$ is a *secret-sharing matrix over* $S$ if for all $e\in E$ and all $X\subseteq E-\{e\}$, either $n(i, e, X)=S$ for all $i\in I$, or $|n(i, e, X)|=1$ for all $i\in I$.

The study of such matrices is motivated by cryptographic considerations. For let $A=(a_{ie}: i\in I, e\in E)$ be any matrix with entries from $S$. Suppose that some row $i\in I$ has been chosen, but its value has been kept secret; and we wish to determine as much as possible about the values $a_{ie}$ $(e\in E)$. The matrix $A$ is known to us, but we do not know which row has been selected. Suppose that by some means we have been able to determine the values $a_{if}$ for all $f\in X\subseteq E$, and let $e\in E-X$. How much can be deduce from our current information about the value of $a_{ie}$? The possible values of $a_{ie}$ consistent with our information are precisely the members of $n(i, e, X)$ (and this set can be determined from our information, despite the fact that we do not know the value of $i$). It is of interest in cryptography to require that $a_{ie}$ either be completely determined or not be determined at all; and that which of these happens (for given $X, e$) be independent of the choice of $i$. This is one reason for interest in secret-sharing matrices. Another reason, more genuine but more complex, is given in [1].



0095-8956/92 $5.00

Let $A=(a_{ie}: i\in I, e\in E)$ be a secret-sharing matrix over $S$. Let us say that $X\subseteq E$ *spans* $e\in E-X$ if $|n(i, e, X)|=1$ for all $i\in I$, and that $Y\subseteq E$ is *independent* if for all $e\in Y$, $Y-\{e\}$ does not span $e$. It was observed in [1] that this defines the independent sets of a matroid $M$ with element set $E$; and we call $A$ a *secret-sharing matrix for $M$ over $S$*. Any matroid arising in this way (for some appropriate $S$) is called a *secret-sharing matroid.*

For instance, any matroid representable over a finite field is secret-sharing (let $M$ be represented by the columns of the matrix $B$ over the finite field $S$, and let $A$ be the matrix with rows all linear combinations of the rows of $B$). The secret-sharing matrices for a given matroid seem to be much more wild than the representations of the matroid. For example let $M$ be the uniform rank 2 matroid with 3 elements; then the secret-sharing matrices for $M$ over $S$ correspond to the $|S|\times|S|$ latin squares. This leads one to hope that perhaps every matroid is secret-sharing, and this question was raised in [1]. But we shall see that the Vamos matroid is not secret-sharing.

The Vamos matroid $V$ is defined as follows. It has eight elements $\{1, 2, ..., 8\}$, and its independent sets are all the sets of cardinality $\leqslant 4$ except for five, namely

$$\{1, 2, 3, 4\},\ \{1, 2, 5, 6\},\ \{3, 4, 5, 6\},\ \{3, 4, 7, 8\},\ \{5, 6, 7, 8\}.$$

We observe

**1.1.** *Let $A=(a_{ie}: i\in I, e\in E)$ be a matrix with entries from some finite set $S$, and let $M$ be a matroid with element set $E$. Then $A$ is a secret-sharing matrix for $M$ if and only if for all $X\subseteq E$, the submatrix $(a_{ie}: i\in I, e\in X)$ has precisely $|S|^{\mathrm{rk}(X)}$ distinct rows, where $\mathrm{rk}(X)$ denotes the rank of $X$ in $M$.*

We omit the proof, which is easy.

## 2. The Proof

All graphs in this paper are assumed to be simple. If $G$ is a graph, a subset $X\subseteq V(G)$ is *stable* if no two members of $X$ are adjacent; and a *triangle* of $G$ is a circuit of length 3. For $k\geqslant 1$, $K_{k,k,k}$ denotes a "complete tripartite graph" with vertex set $V_1\cup V_2\cup V_3$, where the $V_i$'s are mutually disjoint and each of cardinality $k$, and for $1\leqslant i<j\leqslant 3$, every vertex in $V_i$ is adjacent to every vertex in $V_j$. We begin with the following lemma.

**2.1.** *Let $k\geqslant 1$ be an integer, let $G$ be a graph, and let $T_1, T_2, T_3\subseteq V(G)$ be mutually disjoint stable sets with union $V(G)$, each of cardinality $k^2$.*

*Suppose that for* $1 \leqslant i, j \leqslant 3$ *with* $i \neq j$, *every vertex in* $T_i$ *has* $\leqslant k$ *neighbours in* $T_j$. *Suppose also that* $G$ *has* $\geqslant k^4$ *triangles. Then every component of* $G$ *is isomorphic to* $K_{k,k,k}$.

*Proof.* For $1 \leqslant i \leqslant 3$ and $t \in V(G)$ let $d_i(t)$ be the number of neighbours of $t$ in $T_i$.

(1) *$G$ has at most $\sum_{t \in T_1} d_2(t)\, d_3(t)$ triangles.* For if $t \in T_1$ there are at most $d_2(t)\, d_3(t)$ triangles containing $t$, and every triangle meets $T_1$.

(2) *For $1 \leqslant j \leqslant 3$, if $t_0 \in V(G) - T_j$ then $d_j(t_0) = k$. Moreover, if $t_i \in T_i$ $(i = 1, 2, 3)$ and one of $t_1, t_2, t_3$ is adjacent to the other two, then all three are pairwise adjacent.* For we may assume that $t_0 \in T_1$, and that $t_1$ is adjacent to $t_2$ and to $t_3$. Since $d_2(t)\, d_3(t) \leqslant k^2$ for all $t \in T_1$ by hypothesis, and $|T_1| = k^2$, and $G$ has $\geqslant k^4$ triangles, we deduce from (1) that each $t \in T_1$ is in precisely $d_2(t)\, d_3(t)$ triangles and that $d_2(t) = d_3(t) = k$. The first claim follows. Moreover, every neighbour of $t$ in $T_2$ is adjacent to every neighbour of $t$ in $T_3$, for all $t \in T_1$. The second claim follows by setting $t = t_1$.

(3) *Any induced path of $G$ meets at most two of $T_1, T_2, T_3$.* For if $P$ is a path meeting all three of $T_1, T_2, T_3$, then since $T_1, T_2, T_3$ are stable there is a 2-edge subpath $P'$ of $P$ meeting all of $T_1, T_2, T_3$. But then by (2) the ends of $P'$ are adjacent, and so $P$ is not induced.

(4) *Any induced path of $G$ has $\leqslant 2$ edges.* For suppose that $P$ is an induced path with $\geqslant 3$ edges, and let $t_1, t_2, t_3, t_4$ be its first four vertices. By (3) we may assume that $t_1 \in T_1$, $t_2 \in T_2$, $t_3 \in T_1$, $t_4 \in T_2$. Let $s \in T_3$ be a neighbour of $t_2$ (this exists since $d_3(t_2) = k \geqslant 1$, by (2)). By (2), $s$ is adjacent to $t_1$ and to $t_3$, since $t_1, t_3$ are both neighbours of $t_2$ in $T_1$. By (2) again, $s$ is adjacent to $t_4$, because $s$ and $t_4$ are neighbours of $t_3$. Hence, by (2) again, $t_1$ is adjacent to $t_4$, because they are both neighbours of $s$. But then $P$ is not induced, a contradiction.

(5) *For $1 \leqslant i < j \leqslant 3$, if $u \in T_i$ and $v \in T_j$ belong to the same component of $G$ then they are adjacent.* For let $P$ be the shortest path of $G$ between $u$ and $v$. Then $P$ is induced, and by (3), $V(P) \subseteq T_i \cup T_j$. By (4), $|E(P)| \leqslant 2$, and since $|E(P)|$ is odd it follows that $|E(P)| = 1$, as required.

Now let $C$ be a component of $G$. For $1 \leqslant i < j \leqslant 3$, every vertex in $V(C) \cap T_i$ is adjacent to every vertex in $V(C) \cap T_j$. Choose $t \in V(C)$; we may assume that $t \in T_1$. By (2), $d_2(t) = d_3(t) = k$, and so $|V(C) \cap T_2| = |V(C) \cap T_3| = k$. In particular, $V(C) \cap T_2 \neq \emptyset$, and so similarly (choosing $t \in V(C) \cap T_2$) we deduce that $|V(C) \cap T_1| = k$. Hence $C$ is isomorphic to $K_{k,k,k}$, as required. ∎

Now we prove our main result.

**2.2.** *The Vamos matroid is not secret-sharing.*

*Proof.* Let $V$ be the Vamos matroid, with $E(V) = \{1, ..., 8\}$, defined as before. Suppose that $A = (a_{ij}: i \in I, 1 \leqslant j \leqslant 8)$ is a secret-sharing matrix for $V$ over some finite set $S$, where $|S| = k$. For $1 \leqslant r \leqslant 4$, let

$$T_r = \{(s_1, s_2, r): s_1, s_2 \in S\}.$$

Then $T_1, ..., T_4$ are mutually disjoint. Let $H$ be the graph with vertex set $T_1 \cup \cdots \cup T_4$ in which $(s_1, s_2, r)$ is adjacent to $(s_1', s_2', r')$ if $r \neq r'$ and there exists $i \in I$ with

$$a_{i,2r-1} = s_1,\ a_{i,2r} = s_2,\ a_{i,2r'-1} = s_1',\ a_{i,2r'} = s_2'.$$

In other words, for each $i \in E$ we make

$$(a_{i1}, a_{i2}, 1),\ (a_{i3}, a_{i4}, 2),\ (a_{i5}, a_{i6}, 3),\ (a_{i7}, a_{i8}, 4)$$

mutually adjacent.

(1) *For $1 \leqslant r, r' \leqslant 4$ with $r \neq r'$ and $\{r, r'\} \neq \{1, 4\}$, each vertex in $T_r$ has $\leqslant k$ neighbours in $T_{r'}$.* For $\{2r-1, 2r, 2r'-1, 2r'\}$ is a circuit of $V$, and so no two rows of $A$ agree in precisely three of these four positions. Hence if $(s_1, s_2, r)$ is adjacent both to $(s_1', s_2', r')$ and to $(s_1'', s_2'', r')$, and the latter two are distinct, then $s_1' \neq s_1''$. The claim follows.

If $X \subseteq V(H)$, we denote by $H \backslash X$ the graph obtained by deleting $X$.

(2) *$H \backslash T_4$ and $H \backslash T_1$ both have $\geqslant k^4$ triangles.* For if $i \in I$, the vertices $(a_{i1}, a_{i2}, 1)$, $(a_{i3}, a_{i4}, 2)$, $(a_{i5}, a_{i6}, 3)$ form a triangle of $H \backslash T_4$; and if $i, i' \in I$ yield the same triangle, then $a_{ie} = a_{i'e}$ $(1 \leqslant e \leqslant 6)$. Since by **1.1** there are $k^4$ values of $i$ pairwise different somewhere in the first six columns, we deduce that $H \backslash T_4$ has $\geqslant k^4$ triangles. Similarly so does $H \backslash T_1$, as required.

From (1), (2) and **2.1**, we see that

(3) *Every component of $H \backslash T_4$ is isomorphic to $K_{k,k,k}$, and so is every component of $H \backslash T_1$.*

In particular, every component of $H \backslash T_4$ includes a unique component of $H \backslash (T_1 \cup T_4)$, and so does every component of $H \backslash T_1$. We deduce

(4) *There is a partition $(X_j: j \in J)$ of $V(H)$ such that for all $j \in J$, $X_j \cap (T_1 \cup T_2 \cup T_3)$ is the vertex set of a component of $H \backslash T_4$, and $X_j \cap (T_2 \cup T_3 \cup T_4)$ is the vertex set of a component of $H \backslash T_1$. Moreover, for all $j \in J$, $|X_j \cap T_r| = k$ for $1 \leqslant r \leqslant 4$.*

(5) *The submatrix $(a_{ie}: i \in I, e \in \{1, 2, 7, 8\})$ of $A$ has $\leqslant k^3$ different rows.* For let $i \in I$; then $(a_{i1}, a_{i2}, 1) \in T_1$. Let $(a_{i1}, a_{i2}, 1) \in X_j$, where $j \in J$. Since

$(a_{i1}, a_{i2}, 1)$ is adjacent in $H\backslash T_4$ to $(a_{i3}, a_{i4}, 2)$ it follows from (4) that $(a_{i3}, a_{i4}, 2) \in X_j$. Similarly, since $(a_{i3}, a_{i4}, 2)$ and $(a_{i7}, a_{i8}, 4)$ are adjacent in $H\backslash T_1$, it follows that $(a_{i7}, a_{i8}, 4) \in X_j$. We deduce that every neighbour in $T_4$ of $(a_{i1}, a_{i2}, 1)$ belongs to $X_j$, and since $|X_j \cap T_4| \leqslant k$, we deduce that $(a_{i1}, a_{i2}, 1)$ has $\leqslant k$ neighbours in $T_4$. Consequently the graph $H\backslash(T_2 \cup T_3)$ has at most $k^3$ edges. The claim follows.

But (5) contradicts **1.1**, because $rk(\{1, 2, 7, 8\}) = 4$. This completes the proof. ∎

## ACKNOWLEDGMENT

Thanks to K. Gopalakrishnan for pointing out an error in an earlier version of this paper.

## REFERENCE

1. E. F. BRICKELL AND D. M. DAVENPORT, On the classification of ideal secret sharing schemes, *J. Cryptography*, to appear.