Marriage, Magic, and Solitaire

David B. Leep and Gerry Myerson

1. SOLITAIRE. Here's a solitaire game you can always win.

Deal out a deck of cards, face up, into a 4×13 array. The object of the game is to select 13 cards, one from each column, in such a way as to get one card of each denomination.

It turns out that it is always possible to make such a selection. The proof is a simple application of Hall's Marriage Theorem, as we show in Example 1 in the next section. In Sections 3 and 4, we identify winning the solitaire game with decomposing a semi-magic square into a linear combination, with positive integer coefficients, of permutation matrices. The remainder of the paper discusses the number of permutation matrices needed to express a given semi-magic square.

2. MARRIAGE. Suppose there are sets $A_1, A_2, \ldots, A_n$, and you wish to know whether there exist distinct objects $x_1, x_2, \ldots, x_n$, such that x_1 is in A_1, x_2 is in $A_2, \ldots,$ and x_n is in A_n—we'll call this a *transversal.* If any A_j is empty, then it's clear that x_j does not exist; a simple necessary condition for the existence of a transversal is that $\#A_j \geq 1$ for all j—we write $\#S$ for the cardinality of the set S.

If among the sets $A_1, \ldots, A_n$ there are two whose union has only one element, then there can be no transversal. More generally, a necessary condition for the existence of a transversal is that $\#\bigcup_{j \in J} A_j \geq \#J$ for every index set $J \subset \{1, \ldots, n\}$.

Hall's Marriage Theorem states that this simple necessary condition is also sufficient:

Theorem 1. *There exist distinct $x_1, \ldots, x_n$ such that $x_j \in A_j$ for all j if and only if $\#\bigcup_{j \in J} A_j \geq \#J$ for all $J \subset \{1, \ldots, n\}$.*

Many proofs are known, and the reader with access to combinatorics and/or graph theory textbooks will have little difficulty finding one, so we do not present one here. The compilation [2] contains Hall's original proof, and the spiffy proof of Halmos and Vaughan. The interpretation wherein the "objects" are men and A_j is the set of suitable marriage partners for the jth woman is the origin of the name, "Marriage Theorem."

The application to the solitaire game is as follows.

Example 1. Let the objects be the 13 denominations, and let A_j be the set of all denominations of cards in the jth column. For example, if column 7 has an ace, a deuce, and two jacks, then $A_7 = \{\text{ace, deuce, jack}\}$. Any collection of k columns, $1 \leq k \leq 13$, contains $4k$ cards, hence contains cards of at least k different denominations (since there are only 4 cards of each denomination). But this is precisely the condition for Hall's Theorem to apply, and it tells us we can choose a different denomination from each column.

3. MAGIC. That could be the end of the discussion, but instead we approach the problem from a different point of view, in order to introduce the topic we really want to talk about: semi-magic squares. Much of what we have to say applies, mutatis mutandis, to doubly-stochastic matrices, so there should be something here to appeal to a variety of mathematical tastes.

Having dealt out the cards, construct a 13×13 matrix A, as follows. Each column in A corresponds to a column of cards, and each row to a denomination. The value of a_{ij} (the usual notation for the entry in row i, column j of A, although we also write $A(i, j)$) is then taken to be the number of cards of denomination i in column j. In Example 1, we would have $a_{\text{ace, 7}} = 1$, $a_{\text{jack, 7}} = 2$, and $a_{\text{queen, 7}} = 0$.

The matrix so constructed enjoys the following properties;

1. its entries are non-negative integers,
2. the entries in each row add up to 4 (because there are exactly 4 cards of each denomination), and
3. the entries in each column also add up to 4 (because there are exactly 4 cards in each column of cards).

Thus, the matrix is a *semi-magic square*; a square array of non-negative integers having constant line-sums. "Line-sums" means both row and column sums. The common value of the line-sums is called the *magic constant* of the semi-magic square, and is denoted by m. In a *magic square*, the entries along each diagonal also add up to m, but we do not invoke this condition in the sequel.

Hall's Theorem has the following consequence:

Theorem 2. *A non-zero semi-magic square has a transversal all of whose elements are non-zero.*

In this context, "transversal" means a set of entries meeting each line exactly once (that is, one entry from each column, each from a different row). For, let the columns correspond to sets, and the rows to objects, and let a_{ij} non-zero mean that object i is in set j. In any k columns, the non-zero entries add up to km. Restricting our attention to those k columns, if fewer than k rows meet those columns in non-zero entries, then at least one row meets those columns in entries that add up to more than m; but this is impossible, since the entries in each row add up to exactly m. Thus, Hall's Theorem applies, and there is a choice of a different object from each set; a non-zero entry from each column, each from a different row.

In the 13×13 semi-magic square constructed in Example 1 from an array of cards, a transversal corresponds to a selection of one card from each column, each of a different denomination. Thus we have a second way to use Hall's Theorem to prove that we can always win this game of solitaire.

4. PERMUTATIONS. Perhaps the simplest non-zero semi-magic squares are those with all line-sums 1, the *permutation matrices*. A permutation matrix is a matrix of zeros and ones, the ones forming a transversal. The name arises from the association of each such matrix A to a permutation σ via $a_{ij} = 1$ if and only if $\sigma(i) = j$. This association is a group isomorphism from the multiplicative group of $n \times n$ permutation matrices to the group of all permutations of $\{1, \ldots, n\}$.

We can reformulate Theorem 2: if A is a non-zero semi-magic square, then there is a permutation matrix P such that $A - P$ has non-negative entries. But then $A - P$ is itself clearly a semi-magic square, whence, by induction, we deduce

Theorem 3. *Every semi-magic square can be expressed as a sum of permutation matrices.*

Theorems 2 and 3 are due to Kőnig [**3**]. As an illustration of Theorem 3, we note that

$$\begin{pmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{pmatrix} = 7\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} + 4\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} + 2\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$
$$+\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

A *doubly-stochastic* matrix is a matrix with non-negative real entries and all line-sums equal to one. Dividing any non-zero semi-magic square by its magic constant yields a doubly-stochastic matrix. Birkhoff [**1**] proved that every doubly-stochastic matrix is a convex combination of permutation matrices; see also [**6**, Theorem 5.4 of Chapter 5].

An expression of a semi-magic square as a sum of permutation matrices is, in general, not unique. We may ask for an expression that uses as few distinct permutation matrices as possible. The rest of this paper is an attempt to come to grips with this and related questions.

5. THE BASIS. The concepts of permutation matrix and semi-magic square generalize readily to square matrices with entries from any ring R with unit. Let the unit element of R be 1. Then a permutation matrix over R is, as before, a matrix of zeros and ones, the ones forming a transversal. A constant line-sum matrix over R is a square array of elements of R having all line-sums equal. We reserve the term "semi-magic square" for a constant line-sum matrix over the integers with non-negative entries. Any linear combination of permutation matrices with coefficients in R is a constant line-sum matrix over R. We have seen that any semi-magic square with non-negative integer entries is an integer-linear combination of permutation matrices, and we now show that this, too, generalizes to constant line-sum matrices over R. The case $n = 1$ is trivial, and a 2×2 constant line-sum matrix must look like

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus, we may assume $n \geq 3$. Let $\mathscr{B}_n$ be the set of all permutation matrices corresponding to those transpositions and 3-cycles that move 1, together with the identity matrix. That is, $\mathscr{B}_n$ contains the permutations of the form $(1j)$, $2 \leq j \leq n$, and those of the form $(1jk)$, $2 \leq j \leq n$, $2 \leq k \leq n$, $j \neq k$, and the identity. Then $\mathscr{B}_n$ is a linearly independent set, over any ring whatsoever. For if $\sum_{P_\sigma \in \mathscr{B}_n} a_\sigma P_\sigma = 0$, then $a_{(1jk)}$ must be zero, since $P_{(1jk)}$ is the only matrix in $\mathscr{B}_n$ with a non-zero entry in row j, column k. And if all the $a_{(1jk)}$ are zero, then $a_{(1j)}$ must be zero, since each $P_{(1j)}$ has a one in the first row that none of the others has. Finally, $a_{()}$ must be zero.

Now let A be any $n \times n$ constant line-sum matrix over R. Let $B = A - \sum_{j,k} a_{jk} P_{(1jk)}$, taking the sum over all j and k distinct from each other and one; then $b_{jk} = 0$ for all these j and k. Let $C = B - \sum_{j=1}^{n} b_{1j} P_{(1j)}$. Then C has all line-sums zero, since its first row is entirely zeros. Each column of C, other than

the first, has $n-1$ zeros, hence, n zeros; then, looking across the rows, we see that all the entries in the first column must be zero as well. Thus, $A = \Sigma a_{jk} P_{(1jk)} + \Sigma b_{1j} P_{(1j)}$ expresses A as a linear combination of permutation matrices (with coefficients in the ring generated by the entries of A).

Summing up, we have proved:

Theorem 4. *For any ring R with unit, the set of all R-linear combinations of elements of $\mathscr{B}_n$ is the set of all $n \times n$ constant line-sum matrices with entries in R.*

A closer look at the proof leads to our next result.

Theorem 5. *Each $n \times n$ permutation matrix can be written as a ± 1-combination of at most $2n-1$ elements of $\mathscr{B}_n$ (meaning, a linear combination in which each coefficient is 1 or -1).*

Proof: Let A in the proof of Theorem 4 be a permutation matrix. For each j, $2 \le j \le n$, there is at most one k, $k \ne 1$, $k \ne j$, such that $a_{jk} = 1$. Thus, at most $n-1$ of the coefficients $a_{(1jk)}$ are one (the rest being zero), and no two of these have the same value of j. So, the first row of $B = A - \Sigma a_{(1jk)} P_{(1jk)}$ takes all n of its entries from $\{-1, 0, 1\}$, and $b_{(1j)}$ is in $\{-1, 0, 1\}$ for all j. ∎

That Theorems 4 and 5 proclaim a special property of $\mathscr{B}_n$ can be seen from the following equation, valid for any $n \ge 4$:

$$2I = (12) + (23) + (34) + (41) - (1234) - (4321), \tag{1}$$

where we have adopted the notational convenience of replacing a permutation matrix with the permutation it represents. It is easy to check that the six matrices on the right are linearly independent over any ring R that does not have a non-zero element x satisfying $x + x = 0$; but the identity matrix cannot be expressed as a ± 1-combination of any linearly independent set that includes these six matrices, and it cannot be written as an R-linear combination at all, if R has no element x satisfying $x + x = 1$ (for example, if R is the integers).

This example suggests a question, for which we do not know the answer: given n, for which integers m does there exist an $n \times n$ semi-magic square A, a linearly independent set of permutation matrices $\{P_1, \ldots, P_r\}$, and non-negative integers $c_1, \ldots, c_r$ with $\gcd(c_1, \ldots, c_r) = 1$, such that $mA = \Sigma_j c_j P_j$? Equation (1) shows that we may take $m = 2$ for every $n \ge 4$; indeed, from

$$(m-2)I = (12) + (23) + \cdots + (m-1\ m) + (m\ 1) - (12\ldots m) - (m\ m-1\ldots 1)$$

it is easy to verify that for any n we can take any m not exceeding $n-2$.

6. HOW MANY? (BIG FIELDS). It is easy to see that the set of all $n \times n$ constant line-sum matrices over a field F forms a vector space over F. What is the dimension of this space?

Theorem 6. *The dimension of the vector space of all $n \times n$ constant line-sum matrices over a field F is $n^2 - 2n + 2$.*

This can be seen in several different ways.

1) Assign arbitrary values to a_{ij}, $1 \le i \le n-1$, $1 \le j \le n-1$, and also to a_{1n}, making $(n-1)^2 + 1$ arbitrary choices in all. There is a unique choice of each a_{in},

$2 \le i \le n-1$, and each a_{nj}, $1 \le j \le n-1$, that makes the corresponding row or column sum equal to the sum of the entries in the first row, and then a unique choice of a_{nn} to complete the constant line-sum matrix.

2) To be a constant line-sum matrix is to satisfy $2n-1$ equations of the form, "the entries in row 1 add up to the same number as the entries in a different line." There is one dependence relation among these equations, since the sum of all the row sums equals the sum of all the column sums, so the vector space has codimension $2n-2$ in the vector space of all $n \times n$ matrices, which means that the dimension is $n^2 - (2n-2)$.

3) The basis $\mathscr{B}_n$ has $(n-1)(n-2)$ elements of the form $(1jk)$, $n-1$ of the form $(1j)$, and the identity, making $n^2 - 2n + 2$ in all.

It follows from Theorems 4 and 6 that, over a field, any $n \times n$ constant line-sum matrix can be expressed as a linear combination of $n^2 - 2n + 2$ or fewer permutation matrices. It also follows that, over an infinite field (or, indeed, a sufficiently large finite field), there exist constant line-sum matrices that cannot be expressed as a linear combination of fewer than $n^2 - 2n + 2$ permutation matrices. This is based on the observation that no vector space over an infinite field is the union of finitely many proper subspaces, which is a corollary to a technical lemma that we have relegated to the appendix.

7. HOW MANY? (NON-NEGATIVE INTEGERS) (THEORY). Life is somewhat different over a (small) finite field, but we postpone discussion of that situation until we have considered the integers. Results about linear combinations with positive integer coefficients do not follow trivially from results about fields, but they do follow:

Theorem 7. *Each $n \times n$ semi-magic square can be expressed as a linear combination, with positive integer coefficients, of $n^2 - 2n + 2$ or fewer permutation matrices.*

Proof: We follow the argument by which Marcus and Ree [5] proved that every doubly-stochastic matrix is a convex combination of $n^2 - 2n + 2$ or fewer permutation matrices. Let A be a non-zero $n \times n$ semi-magic square (if $A = 0$, there is nothing to prove). By Theorem 2 we know there is a permutation matrix P_1 such that $A - P_1$ has non-negative integer entries. Choose m_1 as large as possible, subject to $A_1 = A - m_1 P_1$ having non-negative entries. Note that P_1 has a one in some spot where A_1 has a zero and that the magic constant of A_1 is strictly less than that of A. Now apply the same procedure to A_1, and iterate to termination. Termination must occur, since the magic constants form a strictly decreasing sequence of non-negative integers. When the procedure terminates, we have $A = m_1 P_1 + \cdots + m_r P_r$ for some r. But the matrices $P_1, \ldots, P_r$ are linearly independent (over, say, the rationals), since each has a one in a spot where its successors all have zero. So, r is no greater than the dimension of the space spanned by all the $n \times n$ permutation matrices, and we know from Section 6 that this dimension is $n^2 - 2n + 2$. ∎

We would like to know whether there is an "integer proof" of Theorem 7, that is, a proof that does not rely on embedding the integers into a field and using dimension, a vector space concept.

Theorem 8. *For every n there exist $n \times n$ semi-magic squares that cannot be expressed as a linear combination, with non-negative integer coefficients, of $n^2 - 2n + 1$ permutation matrices.*

We give three proofs.

First proof: Let A be an $n \times n$ constant line-sum matrix with non-negative rational entries, and assume that A is not a linear combination with rational coefficients of $n^2 - 2n + 1$ permutation matrices. Such matrices exist by a corollary to the technical lemma in the appendix. Let m be a common multiple of the denominators of the entries of A. Then mA is a semi-magic square, and is not expressible as a linear combination with rational coefficients (nor, *a fortiori*, with non-negative integer coefficients) of $n^2 - 2n + 1$ permutation matrices. For, if there were such an expression for mA, then dividing through by m would give an expression for A as a rational linear combination of $n^2 - 2n + 1$ permutation matrices. ■

Second proof: We count the number of $n \times n$ semi-magic squares with magic constant N, and the number of linear combinations of $n^2 - 2n + 1$ permutation matrices with positive integer coefficients adding up to N, and we see that, if N is large enough, there are too many of the former to be accounted for by the latter.

Given integers a_{ij} with $N(n-2)/(n-1)^2 \le a_{ij} \le N/(n-1)$ for $1 \le i \le n-1$ and $1 \le j \le n-1$, there exist non-negative integers a_{in}, $1 \le i \le n$, and a_{nj}, $1 \le j \le n$, such that A is a semi-magic square with magic constant N. Thus, the number of squares with magic constant N is at least $c_1 N^{(n-1)^2}$. Here and in the following discussion $c_1, c_2, \ldots$ depend on n but not on N, and the exact nature of the dependence is irrelevant.

To count the number of non-negative integer linear combinations of $n^2 - 2n + 1$ permutation matrices, with all line-sums equal to N, we note first that there are $\binom{n!}{(n-1)^2} = c_2$ ways of choosing the permutation matrices. Having chosen them, we have only to count the number of expressions $\sum_{j=1}^{n^2-2n+1} a_j P_j$ subject to the conditions $\sum a_j = N$ and $a_j \ge 0$ for all j. But the number of ways to meet the conditions is $\binom{N + (n-1)^2 - 1}{(n-1)^2 - 1}$, which is a polynomial in N of degree $(n-1)^2 - 1$ and is thus bounded above by $c_3 N^{(n-1)^2-1}$ for some c_3. So, the total number of semi-magic squares of magic constant N representable as non-negative integer linear combinations of $n^2 - 2n + 1$ permutation matrices is at most $c_4 N^{(n-1)^2-1}$, where $c_4 = c_2 c_3$. If N is large enough, $c_1 N^{(n-1)^2} > c_4 N^{(n-1)^2-1}$, so there must be semi-magic squares that cannot be expressed as a non-negative integer linear combination of $n^2 - 2n + 1$ permutation matrices. ■

We could use this second proof to estimate the value of N needed, but we have thrown too much away for the estimate to be any good. Our third proof actually constructs the object whose existence is established by the first two proofs.

Third proof: Let $P_1, \ldots, P_d$, $d = n^2 - 2n + 2$, be the special basis $\mathscr{B}_n$ discussed in Section 5, ordered in such a way that all the 3-cycles come first, then the transpositions, finally, the identity. Let $A = \sum_{j=1}^{d} c_j P_j$, where c_j is any sequence of positive integers growing fast enough to satisfy $c_j > \sum_{k=1}^{j-1} (j-k) c_k$ for all j (the sequence $1, 2, 5, 13, 34, \ldots$ of alternate Fibonacci numbers will do, barely). We claim that A cannot be expressed as a positive integer linear combination of fewer than $n^2 - 2n + 2$ permutation matrices.

Recall that each P_j has a "special spot" where it has a one and where each P_k, $k > j$, has a zero. Given any j, and any matrix B, we write $B(j)$ for the entry of B in the special spot of P_j.

Let $A = \sum_{j=1}^{r} a_j Q_j$ for some positive integers a_j and some permutation matrices Q_j. Since $A(1) = c_1 \geq 1$, we must have $Q_j(1) = 1$ for some j. Re-ordering, if necessary, we may assume $Q_1(1) = 1$. It follows that $a_1 = c_1$. Let $A_1 = A - a_1 Q_1$.

Now suppose that for $1 \leq j \leq k-1$ we have $Q_j(j) = 1$, $1 \leq a_j \leq \sum_{t=1}^{j} c_t$, and $A_j = A_{j-1} - a_j Q_j = A - a_1 Q_1 - \cdots - a_j Q_j$. Note that $c_k \leq A(k) \leq \sum_{j=1}^{k} c_j$. It follows that

$$1 \leq c_k - \sum_{j=1}^{k-1} (k-j)c_j = c_k - \sum_{j=1}^{k-1} \sum_{t=1}^{j} c_t \leq c_k - \sum_{j=1}^{k-1} a_j \leq A_{k-1}(k) \leq \sum_{j=1}^{k} c_j.$$

Since $A_{k-1}(k) \geq 1$, we must have $Q_j(k) = 1$ for some $j \geq k$. Re-ordering, if necessary, we may assume $Q_k(k) = 1$. Then $1 \leq a_k \leq \sum_{t=1}^{k} c_t$.

By induction, we see that $Q_j(j) = 1$ for $1 \leq j \leq n^2 - 2n + 2$, and $r = n^2 - 2n + 2$. ∎

8. HOW MANY? (NON-NEGATIVE INTEGERS) (PRACTICE). Let's look at some numerical examples. The third proof of Theorem 8, in the case $n = 3$, produces the semi-magic square

$$\begin{pmatrix} 34 & 6 & 15 \\ 7 & 47 & 1 \\ 14 & 2 & 39 \end{pmatrix}$$

with magic constant 55, so this matrix cannot be written as a positive integer linear combination of fewer than 5 permutation matrices. But the same is true of the semi-magic square

$$\begin{pmatrix} 1 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 2 & 2 \end{pmatrix}$$

with magic constant 7. For to account for the entry in the upper left corner, either the identity or (23) must be involved. By symmetry, it doesn't matter which, so let's assume I is a summand. Subtracting I leaves a one in the $(2,2)$ position, which forces involvement of (13), and a one in the $(3,3)$ position, which forces involvement of (12). Subtracting these leaves a matrix with two non-zero entries in each line, so two more matrices are needed; in total, 5.

By brute force, one can show that this result is sharp, that is, that every 3×3 semi-magic square with magic constant less than 7 can be written as a positive integer linear combination of 4 or fewer permutation matrices.

Theorems 7 and 8 imply that every 4×4 semi-magic square can be written as a non-negative integer linear combination of 10 permutation matrices, and that there exist 4×4 semi-magic squares that cannot be written as a non-negative integer linear combinations of 9 permutation matrices. A 4×4 semi-magic square that requires 10 permutations is

$$A = \begin{pmatrix} 5 & 5 & 7 & 14 \\ 11 & 18 & 1 & 1 \\ 10 & 3 & 16 & 2 \\ 5 & 5 & 7 & 14 \end{pmatrix}$$

with magic constant 31; we have been unable to find an example with a smaller magic constant. The proof that this semi-magic square requires 10 permutations reveals a method for producing, for any n, an $n \times n$ semi-magic square that cannot be represented by (that is, written as a non-negative linear combination of) fewer than $n^2 - 2n + 2$ permutation matrices.

Let $A = \sum_{j=1}^{r} a_j Q_j$ with positive integers a_j and permutation matrices Q_j. Since $A(2,3) = 1$, there must be some j such that $Q_j(2,3) = 1$. We may assume $Q_1(2,3) = 1$. Then $a_1 = 1$. Let $A_1 = A - a_1 Q_1$.

Now $A(2,4) = 1$ and $Q_1(2,4) = 0$ (since $Q_1(2,3) = 1$—this is a refinement in the reasoning of the third proof of Theorem 7). So $A_1(2,4) = 1$, and we may assume $Q_2(2,4) = 1$ and $a_2 = 1$. Let $A_2 = A_1 - a_2 Q_2$.

Since $1 \le A_2(3,2) \le 3$, we may assume $Q_3(3,2) = 1$ and $1 \le a_3 \le 3$.

By similar reasoning we find $Q_4(3,4) = Q_5(4,2) = Q_6(4,3) = 1$, $1 \le a_4 \le 2$, $1 \le a_5 \le 5$, and $1 \le a_6 \le 7$. Let $A_6 = A - \sum_{j=1}^{6} a_j Q_j$.

Now comes the tricky part; showing that $A_6(1,1) \ge 1$ (whence $Q_j(1,1) = 1$ for some $j \ge 7$). If $Q_3(1,1) = 1$ then, since Q_3 is a permutation matrix and $Q_3(3,2) = 1$ we must have $Q_3(2,3) = 1$ or $Q_3(2,4) = 1$. Thus, $Q_3(1,1) \le Q_3(2,3) + Q_3(2,4)$. Similarly, $Q_5(1,1) \le Q_5(2,3) + Q_5(2,4)$ and $Q_6(1,1) \le Q_6(2,4) + Q_6(3,4)$. It follows that

$$\begin{aligned}\sum_{j=1}^{6} a_j Q_j(1,1) &\le (a_3 Q_3(2,3) + a_5 Q_5(2,3) + a_1) \\ &\quad + (a_3 Q_3(2,4) + a_5 Q_5(2,4) + a_6 Q_6(2,4) + a_2) \\ &\quad + (a_6 Q_6(3,4) + a_4) \\ &\le A(2,3) + A(2,4) + A(3,4) = 4.\end{aligned}$$

Since $A(1,1) = 5$, we have established $A_6(1,1) \ge 1$. With the obvious definitions, the same sort of reasoning shows that $A_7(1,2)$, $A_8(1,3)$, and $A_9(1,4)$ are all positive, so $r \ge 10$.

We can prove that any 4×4 square with magic constant 14 or less can be written with fewer than 10 permutation matrices, but we have been unable to close the gap between 14 and 31, or the much larger gaps in our knowledge for $n > 4$.

9. HOW MANY? (SMALL MODULI). Let q be a positive integer, and let A be an $n \times n$ constant line-sum matrix over $\mathbf{Z}/q\mathbf{Z}$. We showed in Section 6 that A can be expressed as a $\mathbf{Z}/q\mathbf{Z}$-linear combination of no more than $n^2 - 2n + 2$ permutation matrices. If q is not too big (relative to n), we can do better.

Theorem 9. *Any $n \times n$ constant line-sum matrix over $\mathbf{Z}/q\mathbf{Z}$ can be written as a $\mathbf{Z}/q\mathbf{Z}$-linear combination of no more than $(q-1)n$ permutation matrices.*

We note that $(q-1)n$ is less than $n^2 - 2n + 2$, provided $q \le n - 1$. We illustrate Theorem 9 with an example before embarking on the proof. Working over $\mathbf{Z}/3\mathbf{Z}$, consider

$$A = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 \\ 1 & 0 & 0 & 1 \\ 1 & 2 & 2 & 0 \end{pmatrix}. \tag{2}$$

We can construct a semi-magic square A' that is congruent to A (modulo 3), with magic constant $8 = (q-1)n$:

$$A' = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 4 & 1 & 1 & 2 \\ 1 & 3 & 3 & 1 \\ 1 & 2 & 2 & 3 \end{pmatrix}.$$

Trivially, A' can be written as a sum of 8 permutation matrices; this serves to express A as a $\mathbf{Z}/3\mathbf{Z}$-linear combination of 8 permutation matrices.

Proof of Theorem 9: Let A be an $n \times n$ constant line-sum matrix over $\mathbf{Z}/q\mathbf{Z}$. We may view the entries of A as integers a_{ij} satisfying $0 \le a_{ij} \le q - 1$. Working now in $\mathbf{Z}$, let the maximal line sum in A be m; note that $m \le (q-1)n$. We now construct a semi-magic square A', congruent, entrywise, to A (modulo q), with magic constant m. Choose any row of A whose entries do not add up to m (if there is no such row, A is already semi-magic), and any column of A whose entries do not add up to m. Where the chosen row and column intersect, add to the entry a large enough multiple of q to bring the larger of the row and column sums up to m. This does not change the congruence class of the entry (modulo q), and it decreases by at least one the number of lines with line-sum not equal to m. After at most $2n - 2$ applications of this procedure we arrive at a semi-magic square, A'.

Now A' is a semi-magic square with magic constant m, so it can certainly be written as a sum of m permutation matrices. As corresponding entries in A' and A are congruent (modulo q), the same m permutation matrices sum to A when viewed over $\mathbf{Z}/q\mathbf{Z}$. Since $m \le (q-1)n$, we are done. ∎

In the case $q = 2$, Theorem 9 is best possible, since it is clear that the $n \times n$ all-ones matrix requires n permutation matrices. In other cases, we can often do better; if q is not a prime, we can always do better. It helps to introduce some notation here. Let $\beta(A, q)$ denote the least r such that A can be written as a $\mathbf{Z}/q\mathbf{Z}$-linear combination of r permutation matrices, and let $\beta(n, q)$ denote the maximum value of $\beta(A, q)$ over all $n \times n$ constant line-sum matrices A. In this notation, Theorem 9 says $\beta(n, q) \le (q-1)n$.

Theorem 10. *Let s and t be integers, and let A be an $n \times n$ constant line-sum matrix over $\mathbf{Z}/st\mathbf{Z}$. Then $\beta(A, st) \le \beta(A, s) + \beta(n, t)$.*

Proof: Let $\beta(A, s) = k$, so $A = \sum_1^k c_j P_j + sA_1$ for some integers $c_1, \ldots, c_k$, some permutation matrices $P_1, \ldots, P_k$, and some constant line-sum matrix A_1. Then we see that $A_1 = \sum_1^l d_j Q_j + tA_2$ for some integers $d_1, \ldots, d_l$, some permutation matrices $Q_1, \ldots, Q_l$, and some constant line-sum matrix A_2, with $l \le \beta(n, t)$. Then

$$A \equiv \sum^{k} c_j P_j + \sum^{l} s d_j Q_j \pmod{st},$$

and $k + l \le \beta(A, s) + \beta(n, t)$. ∎

Corollary 11. *Let the factorization of q into powers of distinct primes be $q = p_1^{a_1} \cdots p_r^{a_r}$. Then*

$$\beta(n, q) \le \sum_1^r a_j \beta(n, p_j) \le \sum_1^r a_j (p_j - 1)n. \tag{3}$$

If q is not a prime then (3) is always an improvement over the bound in Theorem 9. We can often make a small improvement on the bound (3), even for prime q. Rather than state the result in its full (and somewhat tedious) generality, we illustrate its application to 4×4 matrices over $\mathbf{Z}/3\mathbf{Z}$ by establishing that $\beta(4, 3) \le 7$; Theorem 9 allows us to conclude only that $\beta(4, 3) \le 8$. Let A be any 4×4 constant line-sum matrix over $\mathbf{Z}/3\mathbf{Z}$ that, when viewed as an integer matrix, has maximal line-sum 8; for example, the matrix (2). Then $2A$ has all line-sums

congruent to 1 (mod 3), thus, maximal line-sum at most 7 (when viewed as an integer matrix). In our example,

$$2A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 1 \\ 2 & 0 & 0 & 2 \\ 2 & 1 & 1 & 0 \end{pmatrix}.$$

By the procedure of the proof of Theorem 9, $2A$ can be expressed, over $\mathbf{Z}/3\mathbf{Z}$, as a sum of 7 permutation matrices. Multiplication by 2 yields an expression for A as a $\mathbf{Z}/3\mathbf{Z}$-linear combination of 7 permutation matrices, whence $\beta(4,3) \leq 7$.

With a bit more work, we can actually prove $\beta(4,3) = 6$. For it follows from the work of Marcus and Minc [4] that if B is a 4×4 semi-magic square with magic constant 7, then there is a permutation matrix P such that $B - 2P$ has non-negative entries. Since $B - 2P$ is a semi-magic square with magic constant 5, B is a positive integer linear combination of 6 or fewer permutation matrices. Thus, the number of permutation matrices necessary to represent a 4×4 constant line-sum matrix over $\mathbf{Z}/3\mathbf{Z}$ is at most 6, which is best possible:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 2 & 2 & 2 & 0 \\ 2 & 2 & 2 & 0 \end{pmatrix}$$

cannot be written as a $\mathbf{Z}/3\mathbf{Z}$-linear combination of fewer than 6 permutation matrices (exercise for the reader). The general question of evaluating $\beta(n,q)$ appears to be very intricate.

10. APPENDIX. We present a result about vector spaces that is somewhat technical, together with two useful corollaries. We would like to thank Bruce Reznick for suggestions that improved the exposition in the proof of this lemma.

Lemma 12. *Let V be a vector space over a field F. Let $v_1, \ldots, v_d$ and z be in V, and let $W_1, \ldots, W_m$ be subspaces of V. Assume that no W_i contains the subspace V_0 generated by $\{v_1, \ldots, v_d\}$. Let $S \subseteq F$ be any set with $m + 1$ or more elements. Then there is a vector v in V that can be written as $v = a_1v_1 + \cdots + a_dv_d + z$ with each a_i in S, but v is not in $W_1 \cup \cdots \cup W_m$.*

Corollary 13. *No vector space V over an infinite field F is a finite union of proper subspaces.*

Proof: Let $W_1, \ldots, W_m$ be proper subspaces of V. Choose v_i in V such that v_i is not in W_i for $1 \leq i \leq m$. Now apply Lemma 12, with $S = F$ and $z = 0$. ■

Corollary 14. *For every n there is an $n \times n$ constant line-sum matrix with non-negative rational entries that is not a rational linear combination of $n^2 - 2n + 1$ permutation matrices.*

Proof: In Lemma 12, let F be the rationals, and let S be the non-negative rationals. Take $d = n^2 - 2n + 2$, and let $v_1, \ldots, v_d$ be a linearly independent set of permutation matrices. Let V be the span of $\{v_1, \ldots, v_d\}$, which is the space of all $n \times n$ constant line-sum matrices with rational entries. Let $W_1, \ldots, W_m$ be the subspaces generated by sets of $n^2 - 2n + 1$ permutation matrices—one subspace

for each set of permutation matrices. Lemma 12 ensures that there exist $a_1, \ldots, a_d$, all non-negative rationals, such that $v = a_1v_1 + \cdots + a_dv_d$ is not in any W_i. This v is a constant line-sum matrix with non-negative rational entries, and is not a rational linear combination of $n^2 - 2n + 1$ permutation matrices. ■

Proof of Lemma 12. We may assume that $v_1, \ldots, v_d$ are linearly independent, for, if $v_1, \ldots, v_r$ are linearly independent, and $v_{r+1}, \ldots, v_d$ are dependent on $v_1, \ldots, v_r$, we may choose $a_{r+1}, \ldots, a_d$ arbitrarily from S, let $z' = a_{r+1}v_{r+1} + \cdots + a_dv_d + z$, and find a vector v that can be written as $v = a_1v_1 + \cdots + a_rv_r + z'$.

For each j, let $X_j = W_j \cap V_0$. Then $X_1, \ldots, X_m$ are proper subspaces of V_0. We may assume that S has exactly $m + 1$ elements, and let $T = \{\sum_{i=1}^{d} a_iv_i + z : a_i \in S\}$, so T has cardinality $(m + 1)^d$. We wish to conclude that T is not contained in $X_1 \cup \cdots \cup X_m$.

In fact, we prove that $\#(X_j \cap T) \leq (m + 1)^{d-1}$, from which it follows that

$$\#((X_1 \cup \ldots \cup X_m) \cap T) \leq \sum_j \#(X_j \cap T) \leq m(m + 1)^{d-1} < (m + 1)^d = \#(T).$$

For, suppose $\#(X_1 \cap T) > (m + 1)^{d-1}$. Then for each k, $1 \leq k \leq d$, the pigeonhole principle implies that there exist $c_1, \ldots, c_{k-1}, c_{k+1}, \ldots, c_d$ in S such that $c_1v_1 + \cdots + bv_k + \cdots + c_dv_d + z$ is in X_1 for two distinct elements b of S, say, $b = b_1$ and $b = b_2$. Then $(b_2 - b_1)v_k$ is in X_1, hence v_k is in X_1. But this is true for each k, contradicting the hypothesis that X_1 is a proper subspace of V_0. The same argument applies to each X_j. ■

REFERENCES

1. G. Birkhoff, Tres observaciones sobre el algebra lineal, *Univ. Nac. Tucumán Rev. Ser. A* 5 (1946) 147–151.
2. Ira Gessel, Gian-Carlo Rota, eds., *Classic Papers in Combinatorics*, Birkhauser, 1987.
3. D. Kőnig, Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, *Math. Annalen* 77 (1915–6) 453–465.
4. M. Marcus, H. Minc, Some results on doubly-stochastic matrices, *Proc. Amer. Math. Soc.* 13 (1962) 571–579.
5. M. Marcus, R. Ree, Diagonals of doubly stochastic matrices, *Quart. J. Math.* 10 (1959) 295–302.
6. H. J. Ryser, *Combinatorial Mathematics*, Mathematical Association of America, 1963.

DAVID LEEP attended MIT and Michigan and had postdoc positions at Chicago and Berkeley. Now at the University of Kentucky, his research interests include quadratic forms, number theory, finite fields, and occasional dabbling in algebraic geometry. His outside interests include Baroque trumpet music, traveling, and day dreaming.
University of Kentucky, Lexington, KY 40506-0027, USA
leep@ms.uky.edu

GERRY MYERSON attended Harvard, Stanford, Cambridge, and Michigan. It was at Michigan that he met David Leep. His first publication, joint work with David and fellow Michigan student Brian Conrey, was Advanced Problem 6200 in the MONTHLY, March, 1978. It has taken only a bit over 20 years for him to team up with David again. He arrived at Macquarie University on the day supernova SN 1987a was detected in the Large Magellanic Cloud, but attributes no significance to this coincidence. He enjoys folk music, baseball, and writing about himself in the third person.
Centre for Number Theory Research, E7A, Macquarie University, NSW 2109 Australia
gerry@mpce.mq.edu.au