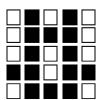
A combinatorial problem associated with nonograms

Jessica Benton Rion Snow Nolan Wallach March 21, 2005

1 Introduction.

This work was motivated by a question posed by the second named author to the first named author about a game that goes by many names but we will refer to it here as the nonogram game. We first describe a nonogram. The starting point is an $m \times n$ board with all squares white. One puts black squares in a selection of positions on the board for example:

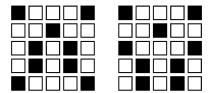


We have a "picture" in a 5×5 board. Now one looks at each row and puts together a sequence of positive integers that gives a list of the numbers of contiguous black squares and one gets a sequence of m lists. One does the same for the columns getting n lists. The nonogram is this pair of lists of lists. Thus the nonogram associated with the above picture is

$$[[1, 1], [3], [1, 1], [2, 2], [3]], [[1], [5], [1, 1], [5], [1]].$$

The puzzle is to be given a nonogram and to construct a picture that yields it. Thus the picture above is a solution to the corresponding nonogram. One can see easily that this nonogram has a unique solution (i.e. picture). We note that the two pictures below are solutions to

[[1,1],[1],[1,1],[1,1],[1,1]],[[1,1],[2],[1],[2],[1,1]].



There are also nonograms that are not related to pictures. For example,

$$[[5], [1, 1, 1], [1], [1], [1], [[1, 2], [5], [1], [1], [1]].$$

No "good" algorithms have been found to determine if a nonogram corresponds to a picture and, if so, find a picture. In fact, this leads to an NP-complete problem.

Having described the actual puzzle let us describe the question. We simplify the nonogram and replace the arrays of arrays with row sums and column sums where we think of the original picture as an $m \times n$ matrix with entries consisting of 0 or 1. Thus the first picture above yields (2,3,2,4,3) for the rows and (1,5,2,5,1) for the columns. The second pair give (2,1,2,2,2), (2,2,1,2,2). The question is how many possible pairs of row sums and column sums are there for $m \times n$ matrices with entries consisting only of 0 or 1? Is there a method of finding all such possiblities? For example the impossible nonogram above corresponds to (5,3,1,1,1), (3,5,1,1,1) which is not even possible as a row and column sum of such a 5×5 matrix. The second named author found that for 1×1 , 2×2 , 3×3 , 4×4 the number of such is respectively, 2,15,328,16145

In this paper we give a method of answering both questions. It is very intriguing that this seemingly innocent question led us to look at fairly deep aspects of the combinatorics of the symmetric group and a further property of Young's raising operators (actually we do lowering) and Schur functions. We also develop a q analogue of the question and a conjecture about divisibility by the q-analogue of n+1, for the case of $n\times n$ matrices (notice that the numbers above are respectively divisible by 2,3,4,5). D. Goldstein and R. Stong [GS] have proved recursion formula for this q analogue and in particular give a relatively fast recursion to count the possible pairs and a proof of the conjecture.

Goldstein and Stong have pointed out to the authors that the main theorem in this paper, Theorem 6, can be found in the standard literature (cf. [BR] and [vLW]). Our method of proof is different and it yields an algorithm for constructing the pertinent matrices.

2 Row and column sum.

We denote by $B_{m,n}$ the set of all $m \times n$ matrices with entries in the set $\{0,1\}$. If $M \in B_{m,n}$ then we write $M = [m_{ij}]$. We set $x_i(M) = \sum_j m_{ij}$ for i = 1, ..., m and set $y_j(M) = \sum_i m_{ij}$ for j = 1, ..., n. We put $x(M) = (x_1(M), x_2(M), ..., x_m(M))$ and $y(M) = (y_1(M), y_2(M), ..., y_n(M))$. In what follows we the notation will not be consistent with right and left actions of groups. The lemma below should clarify the inconsistencies. If $\sigma \in S_m$ and if $M = [m_{ij}]$ is an $m \times n$ matrix then we set $\sigma M = [m_{\sigma i,j}]$ and if $\sigma \in S_n$ then we set $M\sigma = [m_{i,\sigma j}]$. If $v = (v_1, ..., v_n)$ then we set $v\sigma = (v_{\sigma 1}, ..., v_{\sigma n})$ for $\sigma \in S_n$. The following result is proved by the obvious calculation.

Lemma 1 With these notations in place we have

$$x(\sigma M) = x(M)\sigma, y(\sigma M) = y(M)$$

and

$$x(M\sigma) = x(M), y(M\sigma) = y(M)\sigma.$$

We set $RC(m,n) = |\{(x,y)|x = x(M), y = y(M), M \in B_{m,n}\}|$. We are interested in calculating this function. We set $\mathcal{RC}(m,n) = \{(x,y)|x = x(M), y = y(M), M \in B_{m,n}\}$. Clearly, $RC(m,n) = |\mathcal{RC}(m,n)|$. We will now give a preliminary description of $\mathcal{RC}(m,n)$.

We say that an element $x \in \mathbb{N}^n$ is dominant if $x_i \geq x_{i+1}$ for i=1,...,n-1. If $x \in \mathbb{N}^n$ then there exists a unique dominant element of the form $x\sigma$ with $\sigma \in S_n$. Set $\mathcal{RC}_+(m,n) = \{(x,y) \in \mathcal{RC}(m,n) | x,y \text{ dominant } \}$. If $x \in \mathbb{N}^n$ is dominant then we set $orb_n(x) = \{x\sigma | \sigma \in S_n\}$. For such x we define $l_1,...,l_p > 0$ with $l_1 + ... + l_p = n$ and $x_1 = ... = x_{l_1}, x_{l_1+1} = ... = x_{l_1+l_2}, x_{l_1+l_2+1} = ... = x_{l_1+l_2+l_3},...$ Then $|orb_n(x)| = \frac{n!}{l_1! \cdots l_p!}$. We set $\lambda_n(x) = (l_1,...,l_p)$. If $\alpha \in \mathbb{N}^p$ then we set $\alpha! = \alpha_1! \cdots \alpha_p!$.

Lemma 2 We have

$$RC(m,n) = \sum_{(x,y) \in \mathcal{RC}_+(m,n)} |orb_m(x)| |orb_n(y)| = m!n! \sum_{(x,y) \in \mathcal{RC}_+(m,n)} \frac{1}{\lambda_m(x)! \lambda_n(y)!}.$$

Our problem is thus to determine the elements of $\mathcal{RC}_+(m,n)$. If $x = (x_1,...,x_m)$ is dominant and $x_1 \leq n$ then we can define $M \in B_{m,n}$ by $m_{1i} = 1$ for $i = 1,...,x_1, m_{2i} = 1$ for $i = 1,...,x_2$, etc. and all other entries 0. Then x = x(M) and we set $\mu(x) = y(M)$. In the theory of partitions $\mu(x)$ is the dual partition of x possibly expanded to have n rows by including 0 rows. We note that $(x,\mu(x)) \in \mathcal{RC}_+(m,n)$. If x is dominant and $x_1 \leq n$ then we set $Y(x) = \{y | (x,y) \in \mathcal{RC}_+(m,n)\}$. Thus $\mu(x) \in Y(x)$.

We now define two orders on \mathbb{N}^n . $(\mathbb{N} = \{0, 1, 2, ...\})$. The first is the lexicographic order that is x > y if $x_i = y_i$ for i < j and $x_j > y_j$. The other is the root order (or dominance order) which is only a partial order that is $x \succ y$ if $\sum_{i \le j} (x_i - y_i) \ge 0$ for all j = 1, ..., n and at least one of these sums is positive. If $0 \le r \le mn$ we define $\nu_r = \nu_{r,m,n}$ a dominant element of \mathbb{N}^n as follows: Let $c \ge 0$ be defined by

$$(c-1)n < r < cn$$
.

Then since $r \leq mn$ we see that $0 \leq c \leq m$. Define $(\nu_r)_i = c$ for i = 1, ..., r - (c-1)n, and $(\nu_r)_i = c-1$ for i > r - (c-1)n. Notice that if r = 0 then c = 0 and r - (c-1)n = n so $\nu_0 = (0, ..., 0)$. If $0 < r \leq n$ then c = 1 and $\nu_r = (1, 1, ..., 1, 0, ..., 0)$ with r ones. If r > n then c > 1 we have ν_r is dominant and

$$\sum_{i} (\nu_r)_i = c(r - (c - 1)n) + (c - 1)(n - r + (c - 1)n)$$
$$= c(r - (c - 1)n) + (c - 1)(cn - r) = r.$$

In general if $x \in \mathbb{N}^n$ then we set $|x| = x_1 + ... + x_n$.

Lemma 3 Let $0 \le r \le mn$ and let $\mathcal{P}_{m,n}(r)$ denote the set of all x dominant with $x_i \le m$ and |x| = r. Then $\nu_{r,m,n}$ is the unique minimal element in $\mathcal{P}_{m,n}(r)$ relative to both the lexicographic and the root order.

Proof. Let $x \in \mathcal{P}_{m,n}(r)$ and suppose that $x_1 < c$ then $x_1 \le c - 1$ thus $|x| \le (c-1)n < r$. Set k = r - (c-1)n. Then if $x_i = c$ for $i < j \le k$ and $x_j < c$ then the same argument shows that |x| < r. Thus we must have $x_i = c$ for i = 1, ..., k. Now assume that |x| = r and $x \le \nu$ in the lexicographic order. Thus we have $x_i = c$ for i = 1, ..., k and $x_{k+1} \le c - 1$. If $x_i = c - 1$ for i = k + 1, ..., k + l - 1 but $x_{k+l} < c - 1$ then |x| < r. Thus the assertion about the lexicographic order follows. We will now prove the assertion about the root order. We first observe that if $x, y \in \mathbb{N}^n$ and if x > y and if |x| = |y| then

$$x = y + \sum_{i < j} a_{ij} (e_i - e_j)$$

with e_i the usual vector with a one in the *i*-th position and all the other entries 0 with each a_{ij} a non-negative integer and some $a_{ij} > 0$. Assume that $a_{ij} = 0$ for $i < i_o$ and $a = \sum_i a_{i_o j} > 0$. Then $x_i = y_i$ for $i < i_o$ and $x_{i_o} = y_{i_o} + a > y_{i_o}$.

Thus if $x \succ y$ then x > y. This implies that ν_r is a minimal element relative to the root order. We will now show that it is the only one. We note that $\lambda(\nu_r) = (r - (c-1)n, cn - r)$ (if c = 0 then r = 0 and we should interpret this as only having one entry, similarly for r = un so c = u). If $x \in \mathcal{P}_{m,n}(r)$ and if $x_i - x_{i+1} \ge 2$ then $x - e_i + e_{i+1} \in \mathcal{P}_{m,n}(r)$. So x cannot be minimal in $\mathcal{P}_{m,n}(r)$. Thus if x is minimal then $x_i - x_{i+1} \le 1$. Suppose now that $\lambda(x) = (l_1, ..., l_p)$ with $p \ge 3$. Then $x - e_{l_1} + e_{l_1 + l_2 + 1} \in \mathcal{P}_{m,n}(r)$. Thus if x is minimal with respect to the root order then p = 1 or 2. If p = 1 then x = (u, ..., u) and so r = un and $\nu_r = x$. If p = 2 then if x were minimal then $x_1 = u$ and $x_{l_1+1} = u - 1$. Thus we have

$$ul_1 + (u-1)l_2 = r$$

and

$$l_1 + l_2 = n.$$

Hence $l_2 = un - r$. Since $l_2 > 0$ we see that $u \ge c$. If u > c then $l_1 = n - l_2 = n - un + r = r - (u - 1)n < 0$. Thus u = c so $x = \nu_r$.

The technique in the proof of the preceding lemma suggests some operations on the elements of $\mathcal{RC}_{+}(m,n)$ which we will make precise in the next section.

3 Some operations on dominant elements

If $x \in \mathcal{P}_{m,n}(r)$ recall that $Y(x) = \{y \in \mathcal{P}_{m,n}(r) | (x,y) \in \mathcal{RC}_+(m,n)\}$. In this section we study two operations on Y(x) that decrease elements in the root order.

Move 1. If $y \in Y(x)$ and $y_i - y_{i+1} > 1$ then $y - e_i + e_{i+1} \in Y(x)$.

Indeed, let $M \in B_{m,n}$ be such that x = x(M) and y = y(M). Suppose that $m_{ki} = 1$ implies that $m_{ki+1} = 1$ for all k = 1, ..., n. Then $y_i \leq y_{i+1}$. Since we have assumed the contrary, there exists k so that $m_{ki} = 1$ and $m_{ki+1} = 0$. Thus if $M' = [m'_{rs}]$ with $m'_{rs} = m_{rs}$ for $(r, s) \notin \{(k, i), (k, i + 1)\}$ and $m'_{ki} = 0$, $m'_{ki+1} = 1$ then x(M') = x and $y(M') = y - e_i + e_{i+1}$. Since $y_i \geq y_{i+1} + 2$, $y - e_i + e_{i+1}$ is dominant.

Move 2. If $y \in Y(x)$ and if $y_i > y_{i+1} \ge y_{i+2} \ge \ge y_{i+k} > y_{i+k+1}$ then $y - e_i + e_{i+k+1} \in Y(x)$.

Indeed, let $M \in B_{m,n}$ be such that x = x(M) and y = y(M). Arguing as in the justification of Move 1 we see that there exists $1 \le l \le n$ with $m_{li} = 1$ and $m_{l,i+k+1} = 0$. Define M' as above to have all entries but the ones in the l, i and the l, i+k+1 positions the same as those of M but with the two indicated values interchanged. Then as above x = x(M') and $y - e_i + e_{i+k+1} = y(M') \in Y(x)$.

Lemma 4 Let $0 \le r \le mn$ and let $x \in \mathcal{P}_m(r)$. Then $\mu(x)$ is the maximum element of Y(x) with respect to the lexicographic order and it is the unique maximal element of Y(x) with respect to the root order. Also $\nu_{m,n,r}$ is the minimal element in Y(x) with respect to the lexicographic order and the unique minimal element in Y(x) with respect to the root order.

Proof. Let $z = \mu(x)$ and let $y \in Y(x)$. Let $M \in B_n$ be such that x(M) = x and y(M) = y. Then we note that the number of j with $m_{j,1} = 1$ is equal to y_1 and is less than the number of j such that $x_j \neq 0$. Thus $y_1 \leq z_1$ and if $y_1 = z_1$ then $m_{j1} = 1$ precisely if $x_j \neq 0$. We show by induction that if $y_i = z_i$ for $i \leq k - 1$ then $y_k \leq z_k$ and if $y_k = z_k$ then $m_{jk} = 1$ precisely when $x_j \geq k$. We have proved this for k = 1. Assume for $k \leq l$ and we will now prove it for k = l + 1. Suppose that $y_k > z_k$. Then then the number of j such that $m_{jk} = 1$ is larger than the number of l such that $x_l \geq k$. Thus there exists l with $x_l \leq k - 1$ and $m_{l,k} = 1$. The inductive hypothesis implies that $m_{ls} = 1$ for $s = 1, ..., x_l$. But then if $m_{l,k} = 1$ we would have $x_l > x_l$. This contradiction shows that $y_k \leq z_k$ and that $m_{jk} = 1$ implies that $x_j \geq k$. We have observed that of $\alpha \succ \beta$ then $\alpha > \beta$. This shows that $z = \mu(x)$ is maximal in Y(x) in the root order.

Set $Y(x) = \{y | (x,y) \in \mathcal{RC}(m,n)\}$. Suppose that $y \in Y(x)$ is maximal in the root order. Then we assert that $y \in Y(x)$ (we will leave this as an exercise to the reader). Thus the maximal elements of Y(x) are exactly the same as those of $\tilde{Y}(x)$. Now let $y \in Y(x)$ be maximal in the root order. Let $M \in B_{m,n}$ be such that x(M) = x and y(M) = y. Suppose that $y_1 < z_1$. Then the number if indices such that $m_{j,1} = 1$ must be less than the number of j such that $x_j > 0$. Hence there is a j with $x_j > 0$ and $m_{j,1} = 0$. Hence there must be a k > 1 with $m_{j,k} = 1$. If we define M' to have the same entries as M except that $m'_{j,1} = 1$ and $m'_{j,k} = 0$ then x(M') = x and $y(M') = y + e_1 - e_k$. Thus $y(M') \succ y$ in $\tilde{Y}(x)$. This is a contradiction. Now suppose that we have shown that $y_i = z_i$ for $i \le k - 1$. But $y_k < z_k$. Then we can apply the argument in the

previous part to see that $x_j \geq k-1$ if and only if $m_{jl} = 1$ for $j \leq k-1$. Now since $y_k < z_k$ there must be an index j such that $x_j \geq k$ but $m_{jk} = 0$. There must therefore be an index s > k with $m_{js} = 1$. We can therefore argue as in the case when k = 1 to see that $y + e_k - e_s \in \tilde{Y}(x)$. The obvious induction now shows that y is greater than z in the lexicographic order.

The last assertion is implied by Lemma 3.

Theorem 5 Let $0 \le r \le mn$ and let $x \in \mathcal{P}_m(r)$. Then $Y(x) = \{y \in \mathcal{P}_n(r) | \mu(x) \succeq y \succeq \nu_r\}$.

We will actually prove a much more general result. In the following $\mathcal{P}_n(r)$ can be replaced by the set of all dominant n-tuples with non-negative entries that sum to r. The condition that the entries need be at most m can be dropped.

Theorem 6 Let $z, y \in \mathcal{P}_n(r)$ with $z \succeq y$ then there exist elements $z^{(i)} \in \mathcal{P}_n(r)$, i = 0, ..., m such that $z^{(0)} = z$ and $z^{(m)} = y$ and $z^{(i+1)}$ is obtained from $z^{(i)}$ by a Move 1 or a Move 2.

Theorem 5 follows from Theorem 6. Indeed, we have observed that these "moves" preserve Y(x). So applying Theorem 6 to $\mu(x)$ we will have proved Theorem 5. We note that the proof we give of Theorem 6 actually gives an algorithm for the construction of the connecting sequence. Here is a demonstration. Consider z=(7,5,5,3,3,3,2) and y=(5,5,4,4,4,4,2). Then z-y=(2,0,1,-1,-1,-1,0). So $z\succ y$. The method of the proof below would choose $z^{(1)}=(6,6,5,3,3,3,2)$ by Move 1, $z^{(2)}=(6,5,5,4,3,3,2)$ Move 2, $z^{(3)}=(5,5,5,5,5,3,3,2)$ Move 2, $z^{(4)}=(5,5,5,4,4,3,2)$ Move 1, $z^{(5)}=(5,5,4,4,4,2)$ Move 2.

We will now prove Theorem 6. We will prove the theorem by induction on z in the order \succ . If z is the minimal element, ν_r , of $\mathcal{P}_n(r)$ the result is obvious since then $y = \nu_r$ and we take m = 0. So assume the result for all $u \in \mathcal{P}_n(r)$ with $z \succ u$. We now prove the result for z. If z = y then there is nothing to prove. Thus there exists i_o such that $z_i = y_i$ for $i \le i_o$ and $z_{i_o} > y_{i_o}$.

If $z_{i_o} > z_{i_o+1} + 1$ then we may apply Move 1 to z and get $z^{(1)}$. We show that $z^{(1)} \succeq y$. Indeed we have $z_1^{(1)} = y_1, z_2^{(1)} = y_2, ..., z_{i_o-1}^{(1)} = y_{i_o-1}$ thus $\sum_{i \leq j} (z_i^{(1)} - y_i) = 0$ for $j < i_o$. $\sum_{i \leq i_o} (z_i^{(1)} - y_i) = z_{i_o} - y_{i_o} - 1 \geq 0$ and $\sum_{i \leq k} (z_i^{(1)} - y_i) = \sum_{i \leq k} (z_i - y_i)$ for $k > i_o$. Since $z \succ z^{(1)}$ the inductive hypothesis implies the result in this case. We may thus assume that $z_{i_o} \leq z_{i_o+1} + 1$.

If $z_{i_o}=z_{i_o+1}+1$. Then since we have $z_{i_o}>y_{i_o}\geq y_{i_o+1}$ we see that $z_{i_o+1}\geq y_{i_o+1}$. Now suppose that we have $z_j=z_{i_o+1}$ for all $j\geq i_o+1$. Then it is easily seen (arguing as in the proof of the minimality of ν_r) that this is

impossible. Thus there exists a first j such that $j \geq i_o + 1$ and $z_j > z_{j+1}$. We can apply Move 2 to z and get $z^{(1)} = z - e_{i_o} + e_{j+1}$. We will now show that $z^{(1)} \succeq y$ which will complete the induction in this case. We note that we have $z_{i_o+1} = \ldots = z_j > z_{j+1}$. Since $y_{i_o+1} \geq \ldots \geq y_j \geq y_{j+1}$ we have $z_k \geq y_k$ for $i_o + 1 \leq k \leq j$. This implies that

$$\sum_{i \le k} (z_i^{(1)} - y_i) \ge 0$$

for
$$k \leq j$$
. Now $\sum_{i \leq j+1} (z_i^{(1)} - y_i) = \sum_{i \leq j} (z_i^{(1)} - y_i) + z_{j+1} - y_{j+1} + 1 = \sum_{i \leq j+1} (z_i - y_i) \geq 0$ and $\sum_{i \leq k} (z_i^{(1)} - y_i) = \sum_{i \leq k} (z_i - y_i) \geq 0$ for $k > j+1$. Thus $z^{(1)} \succeq y$.

We are left with the case when $z_{i_o}=z_{i_o+1}$. We note that since |z|=|x| there must be a first j such that $z_k=z_{i_o}$ for $k\leq j$ and $z_{j+1}< z_{j}$. There are two cases. First, if $z_j>z_{j+1}+1$. Then we can do Move 1 to get $z^{(1)}=z-e_j+e_{j+1}$. As in the other cases we have $z_k>y_k$ for all $k=i_o,...,j$. So the argument for the first part of the proof implies that $z^{(1)}\succeq y$. We may thus assume that $z_j=z_{j+1}+1$. Now as above there must be another descent that is l>j such that $z_k=z_{j+1}$ for $j+1\leq k\leq l$ and $z_l>z_{l+1}$. We now do Move 2 to get $z^{(1)}=z-e_j+e_{l+1}$. We note that as before $z_k\geq y_k$ for $j+1\leq k\leq l$ and so the argument above implies that $z^{(1)}\succeq y$. The proof is now complete.

4 A q-analogue

In this section we will study

$$RC(q, m, n) = \sum_{(x,y) \in \mathcal{RC}(m.n)} q^{|x|}.$$

The results of the previous section imply that

$$RC(q, m, n) = m! n! \sum_{r} q^{r} \sum_{x \in \mathcal{P}_{m}(r)} \frac{1}{\lambda_{m}(x)!} \sum_{\substack{y \in \mathcal{P}_{n}(r) \\ \mu(x) \succeq y}} \frac{1}{\lambda_{n}(y)!}.$$

We note that the polynomial RC(q,n,n) is of degree n^2 and that it is easily seen that the coefficient of q^j is the same as that of q^{n^2-j} for $0 \le j \le n^2$.

Conjecture 7 The polynomial RC(q, n, n) = RC(q, n) is evenly divisible by $1 + q + q^2 + ... + q^n$.

Here are some examples.

$$RC(q, 1) = 1 + q.$$

 $RC(q, 2) = (1 + q + q^2)(1 + 3q + q^2)$

$$RC(q,3) = (1+q+q^2+q^3)(1+8q+18q^2+28q^3+18q^4+8q^5+q^6)$$

This conjecture has been proved by D. Goldstein and R. Stong. They also prove that the polynomials P(m,n)=RC(q,m,n) satisfy the following recursion. Set $[m+1]_q=1+q+\ldots+q^m$. Then

- 1. P(0, n) = 1 for $n \ge 0$.
- 2. P(m, n) = P(n, m).

3. If
$$m \le n$$
 then $P(m,n) = \sum_{i=1}^{m} (-1)^{i+1} {m \choose i} [m+1]_q^i P(m,n-i)$.
Obviously, this proves the conjecture. Note that this implies that $P(1,n) =$

Obviously, this proves the conjecture. Note that this implies that $P(1, n) = (q+1)^n$. so we could add this to stop the recursion at m=1. This recursion is easily implemented in Mathematica or Maple. Here is a sample Mathematica code (you will have to type out the exponents):

 $P[m_{-}, n_{-}] := Block[\{i\}, If[m == 0, Return[1]]; If[n < m, Return[P[n, m]]]; If[m == 1, Return[(1 + q)^n]]; Return[Expand[Sum[(-1)^{i+1}Binomial[m, i](Factor[(1 - q^{m+1})/(1 - q)]^i)* P[m, n - i], \{i, 1, m\}]]]]$

References

[BR]R.H.Brualdi and H.J.Ryser, Combinatorial Matrix Theory, Cambridge University Press, 1991.

[GS] Daniel Goldstein and Richard Stong, On the number of possible row and column sums of 0,1-matrices, Preprint.

[vLW] J.H.van Lint and R.M.Wilson. A course in combinatorics. Cambridge University Press, 1992.