ON THE SOLUTION OF MOSER'S PROBLEM IN FOUR DIMENSIONS, AND RELATED ISSUES

a collection of two papers

ON THE SOLUTION OF MOSER'S PROBLEM IN FOUR DIMENSIONS

and

INDEPENDENT PERMUTATIONS AS RELATED TO A PROBLEM OF MOSER AND A THEOREM OF PÓLYA

BY

ASHOK K. CHANDRA

STAN-CS-72-286
MAY 1972

COMPUTER SCIENCE DEPARTMENT
School of Humanities and Sciences
STANFORD UNIVERSITY

ON THE SOLUTION OF MOSER'S PROBLEM IN FOUR DIMENSIONS,

AND RELATED ISSUES

a collection of two papers

ON THE SOLUTION OF MOSER'S PROBLEM IN FOUR DIMEJXSIONS

and

INDEPENDENT PERMUTATIONS AS RELATED TO A PROBLEM OF MOSER

AND A THEOREM OF PÓLYA

by

Ashok K. Chandra

This research was supported by the National Science Foundation under grant number GJ-992. Reproduction in whole or in part is permitted for any purpose of the United States Government.

ON THE SOLUTION OF MOSER'S PROBLEM IN FOUR DIMENSIONS

Abstract

The problem of finding the largest set of nodes in a d-cube of side 3 such that no three nodes are collinear was proposed by Moser. Small values of d (viz., $d \leq 3$) resulted in elegant symmetric solutions. It is shown that this does not remain the case in 4 dimensions where at most 43 nodes can be chosen, and these must not include the center node.

1. Introduction

Given a standard 2-dimensional tic-tat-toe board, what is the maximum number of squares that can be occupied such that no three occupied squares are in a straight line? The largest solution occupies six squares, and it is unique modulo rotation. The problem as generalized to a d-dimensional tic-tat-toe board was proposed by Moser [3], [2]. A set of nodes of a d-dimensional board is said to be a solution if no three nodes of the set are in a straight line. The problem is to determine the largest solution for d-dimensions. We denote the number of points in the largest solution by F(d) . We have

$F(1) = 2$ (two solutions modulo rotation),

$F(2) = 6$ (unique solution modulo rotation), and

$F(3) = 16$ (unique solution modulo rotation -- see Figure 1).

The "unique" solution for $d = 3$ is shown in Figure 1. It is easy to show that $40 \leq F(4) \leq 46$. Chvátal [1] demonstrated a lower bound for $F(d)$ that gives $F(4) \geq 42$, and, in general, $F(d) > c3^d/\sqrt{d}$. He also showed that there exists a solution using 43 nodes.

Maximal solutions in one, two and three dimensions have the property that at least one in each case is symmetric about the center, leading one to hope that there might exist such nice" maximal solutions for all dimensions. Unfortunately, this is not true for the four dimension case. It is shown that any maximal solution in 4 dimensions has 43 nodes, and the center node is not occupied, i.e., it cannot be symmetric about the center,,

2. Some Results for Two and Three Dimensions

The following results can be easily verified, and are stated without proof.

(1) The unique solution for $F(2)$ occupies all four side nodes and two opposite corner nodes.

There are five solutions for a two-dimensional board with 5 occupied nodes (modulo rotation and mirror image). These are shown in Figure 2, and will subsequently be referred to as a , b , c , d , e .

(2) For a three-dimensional board, the unique best solution has 16 nodes distributed 6, 4, 6 in the three parallel planes (along major axes) as presented in Figure 1.

x	x	
x		x
	x	x

x		x
x		x

	x	x
x		x
x	x	

Figure 1

The 16-node solution in three dimensions.

x	x	
x		x
	x	

a

x	x	
x		x
		x

b

x		x
x	x	
	x	

c

x		x
x		x
	x	

d

x		x
x		
	x	x

e

Figure 2

The five-node solutions in two dimensions.

(3) For a three-dimensional board, if 6 nodes are occupied in the middle plane, the best solution has 14 occupied nodes.

(4) If a solution for the 3-D problem has 6, 5, 4 occupied nodes in parallel planes then the middle five must be of type e, and of the 4, one must be a center node in the plane.

(5) If a solution for the 3-D problem has 5, 5, 5 occupied nodes, the configuration must be (a,e,c) or (a,e,e).

(6) If the center node is occupied in a solution for the 3-D problem then no more than 14 nodes can be occupied. This follows from the general result that if the center node is occupied in a solution for d dimensions then the solution can have at most $(3^d+1)/2$ nodes.

(7) If the left plane in a 3-D solution has 6 occupied nodes and the right plane has either 5 in configuration e or the 4 corners then the middle plane can have at most 3 occupied nodes.

(8) There exists no 5, 4, 5 solution in 3-D where the two 5's are in configuration e (in any relative orientation).

3. <u>The Proof of $F(4) \leq 43$</u>

A 4-D board is represented by a tableau of 9 planes each containing nine points. The planes will be referred to as A,B,...,I as below.

A	B	C
D	E	F
G	H	I

$|A|$ will represent the number of occupied nodes in A , etc. In addition, implicit use will be made of the symmetries of the problem. Points in a plane will be referred to by adjectives "center", "side", and "corner". Also, planes A, C, G and I will be called corner-planes, etc. "Mid row" refers to D, E, F , similarly for "mid col", etc. |Mid row| obviously means the number of occupied nodes in the middle row, and so on. The row-vector of a solution refers to the number of occupied nodes in the three columns, e.g., (15,14,13) means $|\text{left col}| = |A| + |D| + |G| = 15$, etc.; and similarly for the column vector (the first element refers to the top row).

In the proof below it is assumed that there is a solution with 44 nodes and a contradiction is obtained by case analysis. The cases where $|E| \leq 3$ and $|E| = 6$ are easy and are disposed of first.

$|E| \leq 3$ in a Solution with 44 nodes

Both $|D|$ and $|F|$ cannot be 6 , otherwise the best possible row vector is (14,15,14) by (3) and (2) (since $|E| \neq 4$) and that sums to only 43 .

If (mid row| $\geq$ 15 it must be distributed 6,3,6 -- contradiction.

If |mid row| = 14 , i.e., 6,3,5 the best row vector is (14,14,15) since the middle column also can't contain 15 nodes (by the previous case).

If |mid row| = 13 , i.e., 5,3,5 , 6,3,4 or 6,2,5 the best row vectors are (15,13,15) , (14,13,16) and (14,13,15) respectively.

If |mid row\ = 12 , i.e., both $|D|$ and $|F|$ are not 4 , then a row vector (16,12,16) is impossible.

If |mid row| $\leq$ 11 the best row vector is (16,11,16) .

$|E| = 6$ in a Solution with 44 Nodes

By (3), $|A| + |I| \le 8$, $|B| + |H| \le 8$, $|C| + |G| \le 8$, $|D| + |F| \le 8$, which gives a maximum possible solution of only 38 nodes.

We next prove a contradiction if $|E| = 5$.

$|E| = 5$ in a Solution with 44 Nodes

Case 1: $|\text{mid row}| = 15$

(i) If the mid row is 5,5,5 and the column vector is (16,15,13) . Then D is a , E is e and $|F| = 5$ by (5), and $|A| = |C| = 6$. Since $|A| = 6$ and D is a , $|G| \le 3$ by (4). Since $|C| = 6$ and $|F| = 5$, $|I| \le 4$ by (2). As $|\text{bot row}| = 13$, $|H| = 6$, but this is impossible because in B all four corners are occupied and in E(=e) three are occupied.

(ii) If mid row is 5,5,5 and the column vector is (15,15,14) . Then D is a , E is e, $|F| = 5$ as before. The best row vector is then (14,15,15) for which F is e by (4), (5).

If $|C| = 6$ then by (4), $|G| \le 4$, $|I| \le 4$, and since $|\text{bot row}| = 14$, $|H| = 6$ and $|G| = |I| = 4$. Then, as $|\text{left col}| = 14$, $|A| = 5$ and then $|B| = 4$. But from H , E and B and by (4) the center node of B must be occupied, which implies that $|\text{top row}| \le 14$ by (6) -- a contradiction.

If $|C| = 5$ then $|I| = 5$ and $|A| = 5$ (since $|A| \le 5$ by A , E , I and if $|A| < 5$ then $|\text{top row}| < 15$). Now if we look at the triangle formed by A , C and I , each line is distributed 5,5,5 which means that one end of each line must be configuration a , and the other not an a , by (5); and that is clearly impossible.

If $|C| < 4$ then $|I| = 6$, $|A| = 6$ since $|\text{third col}| = |\text{top row}| = 15$; but that is impossible (A,E,I) .

(iii) If mid row is 6,5,4 , i.e., $|F| = 4$, then the center node of F is occupied by (4), and the best possible row vector is (14,15,14) by (3),(2), and (6).

Case 2: $|\text{mid row}| \leq 14$, and $|\text{mid col}| \leq 14$

Now $|D|+|F| \leq 9$ and $|B|+|H| < 9$ as $|E| = 5$. Also, $|A|+|I| \leq 10$, and $|C| + |G| \leq 10$ by (2); hence the solution has no more than 43 nodes.

This leaves only the most "difficult" possibility open, i.e., $|E| = 4$.

$|E| = 4$ in a Solution with 44 Nodes

Case 1: $|\text{mid row}| = 16$

By (2), $|D| = |F| = 6$, and E has the four corner nodes occupied. By (3), $|\text{left col}|, |\text{right col}| \leq 14$, leaving $|B| = |H| = 6$. It follows that $|\text{left col}| = |\text{right col}| = |\text{top row}| = |\text{bot row}| = 14$. Now consider the planes A , C , G and I . Since all side nodes in B , D , F and H are occupied, at most 4 side noes of A and C together can be occupied; and similarly for G and I . Also, as all 4 corner nodes of E are occupied, A and I together can have at most 4 occupied corner nodes; and likewise for C and G . This, together with the four center nodes of A , C , G and I gives a total of 20 . We want 16 of these nodes to be occupied.

(i) If any corner plane, say A , has all 4 corner nodes occupied its center node can not be occupied, and also no corner nodes can be occupied in C , G or I , leaving at most 3 center nodes and 8 side nodes -- a total of only 4 + 3 + 8 = 15 .

(ii) If any corner plane, say A , has 3 corner nodes occupied, then no corner node of C or G can be occupied, and at most one of I can be occupied. Also, only 3 center nodes and 8 side nodes can be occupied, giving only 3 + 1 + 3 + 8 = 15 .

(iii) If in A two "adjacent" corner nodes are occupied there can be no corner nodes in C or G , leaving a total of 2 corners (in A) + 2 corners (in I) + 4 centers + 8 sides = 16 . But all 16 cannot be taken since, as all centers are occupied, each of A , C , G and I must have 2 adjacent sides occupied (to total 8). But the orientation of the two sides in I has to be the same as in A (and different from C and G). But this conflicts with the corners occupied in I .

(iv) If in A two opposite corner nodes are occupied, say top-right and bottom-left (abbreviated tr and bl), then the tr , bl nodes in I cannot be occupied. If any of the other two corner nodes in I is occupied then no corner node in C or G can be occupied. And, if no corner node in I is occupied then only the tr , bl nodes in C , G can be occupied, and at most 2 of these can be taken. Either way, the maximum possible is only 4 corners + 3 centers + 8 sides = 15 .

(v) Hence each of A , C , G and I must have exactly 1 corner node occupied (to total 16). But this cannot be done owing to the orientation of the corner nodes in B , D , F and H and the fact that all their side nodes are occupied (see Figure 1).

Case 2: $|\text{mid row}| = 15$, and $|\text{mid col}| \leq 15$

$|D| = 6$, $|F| = 5$. Thus $|\text{left col}| \leq 14$ by (3), and as $|\text{mid col}| < 15$ we must have $|\text{right col}| \geq 15$, i.e., F is e by (4), (5); but a 6,4,e (D,E,F) is not a solution in 3-D by (7).

Case 3: $|\text{mid row}| = 14$, and $|\text{mid col}| \leq 14$

If the mid row is 6,4,4 , i.e., $|D| = 6$, then $|\text{left col}| \leq 14$ implying $|\text{mid col}| = 14$ and $|\text{right col}| = 16$, i.e., F has four corner nodes occupied; but this is impossible (D,E,F) by (7).

If the mid row is 5,4,5 then $|\text{left col}| \leq 15$ and $|\text{right col}| \leq 15$ and as $|\text{mid col}| < 14$ all are satisfied with equalities. Thus D and F are both of type e by (4), (5) and D,E,F is impossible by (8).

Case 4: $|\text{mid row}| \leq 13$, and $|\text{mid col}| \leq 13$.

One row and one column must have 16 -- say the top row and the left column. Then $|A| = |C| = |G| = 6$. Now looking at the triangle A,C,G , each line is distributed 6,4,6 , and by (2) the orientation of the two 6's is opposite in each line. And this is clearly impossible for the triangle.

This exhausts all possibilities, implying that there is no solution for the 4-D tic-tac-toe problem with 44 nodes. Thus, solutions with 43 nodes are optimal.

Acknowledgment

The author would like to thank Dr. V. Chvátal for several helpful suggestions.

References

[1] V. Chvátal, "Remarks on a problem of Moser", Canad. Math. Bull., Vol. 15 (1), 1972.

[2] L. Moser, "Problem 21", Proceedings of 1963 Number Theory Conference, University of Colorado, mimeographed, 79.

[3] L. Moser, "Problem P.170", Canad. Math. Bull., Vol. 13, pg. 268 (1970).

INDEPENDENT PERMUTATIONS AS RELATED TO A PROBLEM OF MOSER

AND A THEOREM OF PÓLYA

Abstract

Independent permutations and their properties are discussed, and they are shown to be related to the generalization of Moser's problem to d-cubes of side n with the constraint that a solution have no n collinear points. It follows, for example, that there exist total solutions (i.e., solutions with n^d-n^{d-1} nodes) in arbitrarily large dimensions. These problems are also related to the problem of placing n noncapturing superqueens (chess queens with wrap around capability) on an $n \times n$ board. As a special case of this treatment we get Pólya's theorem that n superqueens can be placed on an $n \times n$ board if and only if n is not a multiple of 2 or 3 .

1. Introduction

A chess queen is a piece that can move horizontally, vertically, or diagonally, any number of squares. We define a more powerful piece which we call a superqueen. A superqueen moves like a queen, but when it reaches an edge of the board it can wrap around to the opposite edge. Effectively it treats the board as if it were a torus. A typical superqueen on a 7×7 board is shown in Figure 1. Squares marked x denote the squares the superqueen can reach in one move. We ask -- for what values of n $(n > 1)$ can n superqueens be placed on an $n \times n$ board such that no superqueen can capture another? Pólya[7] proved that

x		x		x		
		x			x	x
		x			x	x
x		x		x		
	x	x	x			
x	x	Q	x	x	x	x
	x	x	x			

Figure 1

this can be done if and only if the smallest prime factor of n is at least five. We relate Pólya's theorem to a concept of independent permutations on the set $D_n = \{0,1,\ldots,n-1\}$. Indeed, we obtain bounds on the largest number $S(n)$ of independent permutations on D_n and show that Pólya's theorem follows from these bounds. We also introduce two other pieces even more powerful than the superqueen and mention the conditions under which n of these pieces can be placed on an $n \times n$ board such that no piece can capture another.

We also relate independent permutations to a problem posed by Moser [5], [6]. Moser asked for the maximum number $f(n,d)$ of nodes of a d-dimension hypercube of side n such that no n of these nodes are collinear. We find that if $d \leq S(n)$ then $f(n,d) = n^d - n^{d-1}$.

2. Independent Permutations

Given a set $D_n = \{0,1,\ldots,n-1\}$, a permutation on D_n is a 1-1 function from D_n onto itself. For any permutation P on D_n and integers a,b where b is 0, 1 or -1, the function P' given by $P'(x) = P((a+bx) \bmod n)$ is said to be a <u>modification of P</u>. In the special case where b is zero, P' is a constant function, and hence any constant function P' given by $P'(x) = a$, $a \in D_n$, is a modification of P.

A set of permutations $\{P_1, P_2, \ldots, P_d\}$ is said to be <u>independent</u> if for every $P_1', P_2', \ldots, P_d'$ where P_1' is a modification of P_1, P_2' is a modification of P_2, etc., not all modifications constant, the function $P_1' + P_2' + \ldots + P_d'$ (defined in the obvious way, having the value $(P_1(x) + P_2'(x) + ... + P_d'(x) \bmod n)$ for argument x) is also a permutation. Equivalently, for every sequence $a_1, a_2, \ldots, a_d$ of integers and every sequence $b_1, b_2, \ldots, b_d$ in $\{-1,0,1\}^d$ such that not all b_i's are zero, the function P defined by

$P(x) = P_1(a_1 + b_1 x) + \ldots + P_d(a_d + b_d x) \bmod n$, is a permutation. As an example, consider the domain D_5 ; the set of permutations $\{P_1, P_2\}$ below is independent.

x	$P_1(x)$	$P_2(x)$
0	0	0
1	4	2
2	3	4
3	2	1
4	1	3

Their independence can be checked by the definition, but intuitively the justification is the following: the difference between successive values of $P_1(x)$ is $-1 \pmod 5$, and any nonconstant modification P_1' must have difference 1 or -1 ; similarly, any P_2' must have difference 2 or -2 . Adding P_1' and P_2' must result in a function that has a constant nonzero difference between successive values, and it must hence be a permutation.

Some of the interesting properties of independent permutations are the following:

(1) If $\{P_1, P_2, \ldots, P_d\}$ is independent then so is $\{P_1', P_2, \ldots, P_d\}$ where P_1' is any nonconstant modification of P_1 .

(2) Any subset of an independent set is independent.

(3) If $\{P_1, P_2, \ldots, P_d\}$ is independent then so is $\{P_1+k, P_2, \ldots, P_d\}$ where k is any integer and P_1+k is defined in the obvious way, i.e., $(P_1(x)+k \bmod n)$.

(4) If $\{P_1, P_2, .$ [illegible] is independent then so is $\{k \cdot P_1, k \cdot P_2, \ldots, k \cdot P_d\}$, where k is any integer that is prime with respect to n , and $k \cdot P_i$ is defined in the obvious way as being $(k \cdot P_i(x) \bmod n)$ for argument x .

(5) If $\{P_1, P_2, \ldots, P_d\}$ is independent then so is $\{-P_1, P_2,$ [illegible] .

The first four properties are obvious; the fifth one can be proved as follows. Note: all arithmetic below is modulo n .

Suppose $\{-P_1, P_2, \ldots, P_d\}$ is not independent. Then for some $a_1, a_2, \ldots, a_d$ and $b_1, b_2, \ldots, b_d$ where a_i's are integers and each b_i is 0 , 1 or -1 (not all b_i's zero) there exist distinct integers x and y in the domain D_n such that

$$-P_1(a_1 + b_1 x) + P_2(a_2 + b_2 x) + \cdots + P_d(a_d + b_d x) =$$
$$-P_1(a_1 + b_1 y) + P_2(a_2 + b_2 y) + \cdots + P_d(a_d + b_d y) .$$

Case 1. If $b_1 = 0$, then we can find an a_1' in D_n such that $P_1(a_1') = -P_1(a_1)$ since P_1 is a permutation. Then

$$P_1(a_1') + \sum_{2 \le i \le d} P_i(a_i + b_i x) = P_1(a_1') + \sum_{2 \le i \le d} P_i(a_i + b_i y)$$

and this would imply that $\{P_1, P_2, \ldots, P_d\}$ is not independent -- a contradiction.

Case 2. If $b_1 = 1$ then

$$P_1(a_1+y) + \sum_{2\le i\le d} P_i(a_i+b_ix) = P_1(a_1+x) + \sum_{2\le i\le d} P_i(a_i+b_iy) ,$$

and hence

$$P_1((a_1+x+y)-x) + \sum_{2\le i\le d} P_i(a_i+b_ix) =$$

$$P_1((a_1+x+y) -y) + \sum_{2\le i\le d} P_i(a_i+b_iy) .$$

But this implies that $\{P_1, P_2, \ldots, P_d\}$ is not independent -- a contradiction.

Case 3. $b_1 = -1$. This is handled in quite the same way as Case 2 above: by choosing $a_1' = a_1-x-y$ and $b_1' = 1$ we get

$$P_1(a_1' + b_1'x) + \sum_{2\le i\le d} P_i(a_i+b_ix) =$$

$$P_1(a_1'+b_1'y) + \sum_{2\le i\le d} P_i(a_i+b_iy)$$

implying that $\{P_1, \ldots, P_d\}$ is not independent -- a contradiction.

A set of permutations $\{P_1, P_2, \ldots, P_d\}$ is said to be *additive* if for every sequence $c_1, c_2, \ldots, c_d$ where each c_i is 0 , 1 or -1 but not all c_i's are zero,

$$\sum_{1\le i\le d} c_i \cdot P_i$$

is a permutation. It is easy to check that the properties similar to (2)-(5) above hold for additive permutations. In addition, additive permutations have the property that if the set $\{P_1, P_2, \ldots, P_d\}$ is additive and P is any permutation then $\{P_1 \circ P, P_2 \circ P, \ldots, P_d \circ P\}$ is additive where $P_1 \circ P(x) = P_1(P(x))$, etc. The property of independence is not preserved in this transformation.

It follows from the property (4) above that independence implies additivity. The converse is not true, as may be seen from the following example. Permutations P_1 , P_2 below are additive, but not independent. A direct check for additivity is trivial, but we may also observe that P_1 , P_2 are additive because they can be obtained by permuting the previous example (of an independent, and hence additive, set). They are not independent because taking P_1' to be P_1 itself, i.e., (0,3,4,2,1) and P_2' to be (3,0,4,2,1) , and adding we get (3,3,3,4,2) which is not a permutation.

x	$P_1(x)$	$P_2(x)$
0	0	0
1	3	4
2	4	2
3	2	1
4	1	3

The property of additivity is an important one for independent permuations and we will take recourse to this later.

3. Bounds on S(n)

We are interested in the largest set of independent permutations for any domain D_n -- let its size be S(n) . Some values of S(n) are given below.

n	S(n)
1	1
2	1
3	1
4	1
5	2
6	1
7	2
8	1
9	1
10	1
11	3

It follows from (3) above that for the evaluation of S(n) we need only consider permutations P for which P(0) = 0 .

3.1 Lower Bound

If n is a prime then the set of permutations

$$\{I, 2\cdot I, 4.1, .-a , 2^k\cdot I\}$$

where $k = \lfloor \log_2(n) \rfloor - 1$ and I is the identity permutation over D_n , is obviously independent.

This construction produces an independent set of permutations for any n by taking $k = \lfloor \log_2(m) \rfloor - 1$ where m is the smallest prime factor of n . Thus we obtain the following result.

Theorem 1. For $n > 1$, $S(n) \geq \lfloor \log_2(m) \rfloor$, where m is the smallest prime factor of n .

The construction above uses permutations of a very special kind, namely, $a\cdot I$ where a is some integer, and the set of permutations includes the identity permutation itself. It is interesting that the smallest example of an independent pair $\{I,P\}$ where $P \neq a.I+b$ for any a,b is over the domain D_{13} (note: for any n, if an independent pair $\{P_1,P_2\}$ exists, then there exists a pair of the form $\{I,P\}$). Several examples exist for D_{13}, one is:

x	I(x)	P(x)
0	0	0
1	1	3
2	2	8
3	3	11
4	4	5
5	5	1
6	6	10
7	7	4
8	8	7
9	9	12
10	10	2
11	11	9
12	12	6

3.2 Upper Bounds

Lemma. If $\{P_1,\ldots,P_d\}$ is an independent set of permutations over D_n, $n > 1$, such that for all $i \leq d$, $P_i(0) = 0$, then for every pair of sequences $a_1,a_2,\ldots,a_d$ and $b_1,b_2,\ldots,b_d$ where each a_i and each b_i is 0 or 1,

$$a_1 \cdot P_1(1) + \ldots + a_d \cdot P_d(1) = b_1 \cdot P_1(1) + \ldots + b_d \cdot P_d(1) \bmod n$$

if and only if $a_1 = b_1, a_2 = b_2, \ldots, a_d = b_d$.

Proof. The "if" part is trivial.

For the proof in the other direction assume that there exist distinct sequences of a_i's and b_i's for which $a_1 \cdot P_1(1) + \ldots + a_d \cdot P_d(1) = b_1 \cdot P_1(1) + \ldots + b_d \cdot P_d(1) \bmod n$. Now consider the sequence $c_1, c_2, \ldots, c_d$ where $c_i = a_i - b_i$ for each $i \leq d$. Each c_i is 0 , 1 or -1 , not all c_i's are zero, and

$$c_1 \cdot P_1(0) + \ldots + c_d \cdot P_d(0) = 0 \qquad \text{as } P_i(0) = 0 \text{ for all } i$$

and

$$c_1 \cdot P_1(1) + \ldots + c_d \cdot P_d(1) = 0 \qquad \bmod n$$

i.e., $\{P_1, \ldots, P_d\}$ is not additive, but this is impossible as shown by property (4) of independent permutations. This completes the proof.

It follows from this lemma that $2^d \leq n$, and hence:

Theorem 2. For $n > 1$, $S(n) \leq \lfloor \log_2(n) \rfloor$.

This upper bound is about the best nondecreasing bound one can hope for, since by the lower bound theorem it is tight when n is a prime.

Theorem 3. For $n > 1$, let m denote the smallest prime factor of n . Then

$$S(n) \leq \frac{m}{2} \quad .$$

Proof. We will first consider the case m = 2 and show that $S(n) \leq 1$, and then show the theorem for odd m . In each case we will only use the additive property of independent permutations, and hence the upper bound is shown to be true even for additive permutations.

n even, m = 2 . Suppose there exist two permutations P_1 and P_2 over D_n that are independent. We wish to derive a contradiction from this.

Now $P_1(0), P_1(1), \ldots, P_1(n-1)$ are the numbers $0, 1, \ldots, n-1$ in some order, as are $P_2(0), P_2(1), \ldots, P_2(n-1)$, and also $P_1(0) + P_2(0) \bmod n$, $P_1(1) + P_2(1) \bmod n$, $\ldots$, $P_1(n-1) + P_2(n-1) \bmod n$, by the additive property. Therefore

$$\sum_{0 \le x \le n-1} P_1(x) = \frac{n.(n-1)}{2} = \left(\frac{n}{2}\right) \bmod n ,$$

$$\sum_{0 \le x \le n-1} P_2(x) = \frac{n.(n-1)}{2} = \left(\frac{n}{2}\right) \bmod n ,$$

$$\sum_{0 \le x \le n-1} P_1(x) + P_2(x) = \frac{n.(n-1)}{2} = \left(\frac{n}{2}\right) \bmod n .$$

But

$$\sum_{0 \le x \le n-1} P_1(x) + P_2(x) \bmod n = \sum_{0 \le x \le n-1} P_1(x) + \sum_{0 \le x \le n-1} P_2(x) \bmod n$$

$$= \frac{n}{2} + \frac{n}{2} \bmod n$$

$$= 0 \bmod n$$

which is a contradiction.

n odd, m odd . Let

$$\sigma = \sum_{0 \le x \le n-1} x^{m-1}$$

We will first show that $\sigma \not\equiv 0 \bmod n$, and then use this result in the proof that follows. We have

$$\sigma = \sum_{0 \le x \le n-1} x^{m-1} = \sum_{0 \le x \le n-1} \ \sum_{0 \le i \le m-1} \left\{ {m-1 \atop i} \right\} i! \binom{x}{i} ,$$

where $\left\{ {m-1 \atop i} \right\}$ represents Stirling numbers of the second kind -- see, for example, Knuth [4], pg. 65. Note that when $x < i$ then $\binom{x}{i} = 0$ by definition. Hence

$$\sigma = \sum_{0 \le i \le m-1} \ \sum_{0 \le x \le n-1} \left\{ {m-1 \atop i} \right\} i! \binom{x}{i}$$

$$= \sum_{0 \le i \le m-1} \left\{ {m-1 \atop i} \right\} i! \binom{n}{i+1}$$

$$= \left\{ {m-1 \atop m-1} \right\} (m-1)! \binom{n}{m} + \sum_{0 \le i \le m-2} \left\{ {m-1 \atop i} \right\} i! \frac{n!}{(i+1)!\,(n-i-1)!} ,$$

so

$$\sigma \cdot (m-1)! = (m-1)! \frac{n}{m} \frac{(n-1)!}{(n-m)!} + \sum_{0 \le i \le m-2} \left\{ {m-1 \atop i} \right\} \frac{(m-1)!}{i+1} \, n \, \frac{(n-1)!}{(n-i-1)!} .$$

Now, the first term on the right hand side is

$$\left(\frac{n}{m}\right)(m-1)!\,(n-1)\,(n-2)\ \ldots\ (n-m+1)$$

$$= \left(\frac{n}{m}\right) (m-1)!\,(-1)^{m-1} (m-1)! \bmod n$$

$$= \left(\frac{n}{m}\right) ((m-1)!)^2 \bmod n$$

$$\not\equiv 0 \bmod n$$

since m is a prime; and the second term is $0 \bmod n$ because

$\left\{ {m-1 \atop i} \right\}$, $\frac{(m-1)!}{i+1}$, and $\frac{(n-1)!}{(n-i-1)!}$ are all integral. Thus $\sigma(m-1)! \not\equiv 0 \bmod n$, and hence $\sigma \not\equiv 0 \bmod n$.

We can now prove the desired result. Suppose there exists a set of $k = \frac{m+1}{2}$ independent permutations $\{P_1, P_2, \ldots, P_k\}$ over D_n . We wish to obtain a contradiction from this.

First, let S_p denote the set of all vectors $\langle s_1, \ldots, s_p \rangle$ where each s_i equals 1 or -1 (s stands for "sign"). Consider the sum

$$A_k = \sum_{\langle s_1,\ldots,s_k\rangle \in S_k} \ \sum_{0 \le x \le n-1} (s_1 P_1(x) + s_2 P_2(x) + \ldots + s_k P_k(x))^{m-1}$$

$$= \sum_{0 \le x \le n-1} \ \sum_{\langle s_1,\ldots,s_k\rangle \in S_k} (s_1 P_1(x) + \ldots + s_k P_k(x))^{m-1} \ .$$

On expansion, terms in which any P_i appears with an odd power are cancelled out, and the coefficients of terms in which all P_i's appear with even powers add up, to give

$$A_k = \sum_{0 \le x \le n-1} 2^k \Bigg[\sum_{1 \le i_1 \le k} (P_{i_1}(x))^{m-1}$$

$$+ \sum_{\substack{1 \le i_1 < i_2 \le k \\ 0 \le j_1, j_2 \\ j_1, j_2 \text{ even} \\ j_1 + j_2 = m-1}} \binom{m-1}{j_1\ j_2} (P_{i_1}(x))^{j_1} \cdot (P_{i_2}(x))^{j_2}$$

$$+ \sum_{\substack{1 \le i_1 < i_2 < i_3 \le k \\ 0 \le j_1, j_2, j_3 \\ j_1, j_2, j_3 \text{ even} \\ j_1 + j_2 + j_3 = m+1}} \binom{m-1}{j_1\ j_2\ j_3} (P_{i_1}(x))^{j_1} \cdot (P_{i_2}(x))^{j_2} \cdot (P_{i_3}(x))^{j_3}$$

$$+ \; . \; . \; .$$

$$+ \sum_{\substack{1 \le i_1 < \ldots < i_{k-1} \le k \\ 0 \le j_1, \text{[illegible]} \\ j_1, \ldots, j_{k-1} \text{ even} \\ j_1 + \ldots + j_{k-1} = m-1}} \binom{m-1}{j_1\, j_2 \cdots j_{k-1}} (P_{i_1}(x))^{j_1} \ldots (P_{i_{k-1}}(x))^{j_{k-1}}$$

(i.e., all j's are 2)

where $\binom{m-1}{j_1\ j_2}$, $\binom{m-1}{j_1\ j_2\ j_3}$ etc., represent multinomial coefficients. We use the following notation:

$$T_1(x) = \sum_{1 \le i_1 \le k} (P_{i_1}(x))^{m-1}$$

$$T_2(x) = \sum_{\substack{1 \le i_1 < i_2 \le k \\ 0 \le j_1, j_2 \\ j_1, j_2 \text{ even} \\ j_1 + j_2 = m-1}} \binom{m-1}{j_1\ j_2} (P_{i_1}(x))^{j_1} (P_{i_2}(x))^{j_2}$$

etc.

Thus

$$A_k \quad 2^k \sum_{0 < x < n-1} T_1(x) + T_2(x) + \ldots + T_{k-1}(x)$$

In general, for $1 \le p < k$, consider the sum

$$A_p = \sum_{1 \le \ell_1 < \ell_2 < \cdots < \ell_p \le k} \; \sum_{\langle s_1, \ldots, s_p \rangle \in S_p} \; \sum_{0 \le x \le n-1} (s_1 P_{\ell_1}(x) + \cdots + s_p P_{\ell_p}(x))^{m-1}$$

$$= \sum_{0 \le x \le n-1} \left[\sum_{1 \le \ell_1 < \cdots < \ell_p \le k} \; \sum_{\langle s_1, \ldots, s_p \rangle \in S_p} (s_1 P_{\ell_1}(x) + \cdots + s_p P_{\ell_p}(x))^{m-1} \right].$$

When we expand the summations shown in brackets above, all terms in which any P_i appears with an odd power are cancelled out, and terms like $(P_{i_1}(x))^{m-1}$ appear $2^p \binom{k-1}{p-1}$ times, terms like $\binom{m-1}{j_1\ j_2}(P_{i_1}(x))^{j_1}(P_{i_2}(x))^{j_2}$ appear $2^p \binom{k-1}{p-2}$ times, and so on, to yield

$$A_p = 2^p \sum_{0 \le x \le n-1} \binom{k-1}{p-1} T_1(x) + \binom{k-2}{p-2} T_2(x) + \cdots + \binom{k-p}{0} T_p(x)$$

We now form the sum

$$A = \sum_{1 \le p \le k} (-1)^p \, 2^{k-p} A_p$$

$$= 2^k \sum_{0 \le x \le n-1} \Bigg[T_1(x) \sum_{1 \le p \le k} (-1)^p \binom{k-1}{p-1}$$

$$+ T_2(x) \sum_{2 \le p \le k} (-1)^p \binom{k-2}{p-2}$$

$$+ \cdots$$

$$+ T_{k-1}(x) \sum_{k-1 \le p \le k} (-1)^p \binom{1}{p-k+1} \Bigg]$$

$$= 0 \quad .$$

We can also form the same sum in another way. Noting that

$$\sigma = \sum_{0 \le x \le n-1} x^{m-1}$$

and using the additive property of independent permutations we see that

$$A_p = \binom{k}{p} 2^p \sigma \mod n$$

i.e.,

$$A = \sum_{1 \le p \le k} (-1)^p 2^{k-p} A_k$$

$$= 2^k \cdot \sigma \cdot \sum_{1 \le p \le k} (-1)^p \binom{k}{p} \mod n$$

$$= - 2^k . \sigma \mod n \ .$$

But n is odd, and $\sigma \not\equiv 0 \mod n$, hence $A \not\equiv 0 \mod n$. This is the desired contradiction.

<u>Corollary.</u> Let m be the smallest prime factor of n $(n > 1)$. Then if n is prime or $m \le 5$, then $S(n) = \lfloor \log_2(m) \rfloor$.

The smallest values of n for which $S(n)$ is not given by this corollary are 49 , 77 , and 91 .

4. Relation to Moser's Problem

Let $M(n,d)$ denote the set of all vectors $\langle x_1,\ldots,x_d \rangle$ where each x_1 is an element of D_n, and let $f(n,d)$ denote the size of the largest subset $S \subset M(n,d)$ containing no n collinear points. Obviously, $f(n,1) = n-1$, and $f(n,d+1) \le nf(n,d)$, so that

$$f(n,d) \leq n^d - n^{d-1}$$

Moser conjectured that $f(n,d) = o(n^d)$ for each fixed n ; this conjecture has not been proved or disproved yet, though, of course, $f(2,d) = 1$ for all d . It has-been shown, however, that $f(3,d) > c3^d/\sqrt{d}$ (s e e [2]), and $f(3,3) = 16$, $f(3,4) = 43$ (s e e [1]). Also, $f(4,2) = 12$, $f(4,3) = 48$. These can be shown by the set $S \subset M(4,3)$ represented by squares marked x in Figure 2 which represents four parallel planes of a cube of side four.

<u>Theorem 4</u>. Given any n and d such that $1 \leq d \leq S(n)$,

$$f(n,d) = n^d - n^{d-1} .$$

<u>Proof.</u> Given a set of independent permutations $\{P_1,\ldots,P_d\}$ on a domain D_n , we wish to show that

$$f(n,d) = n^d - n^{d-1} .$$

Let S be the set of all $\langle x_1,\ldots,x_d\rangle \in M(n,d)$ such that

$$P_1(x_1) + P_2(x_2) + \ldots + P_d(x_d) \not\equiv 0 \bmod n .$$

Clearly S contains $n^d - n^{d-1}$ nodes because for every $x_1,x_2,\ldots,x_{d-1}$ in D_n there is exactly one x_d for which $\langle x_1,x_2,\ldots,x_d\rangle$ is not in S . To see that S contains no n collinear points, observe that any line passing through n points may be represented as:

$$x_1 = a_1 + b_1 \cdot z , \; x_2 = a_2 + b_2 \cdot z , \; \ldots, \; x_d = a_d + b_d \cdot z$$

where z is a parameter that takes on values $0,1,\ldots,n-1$, and for each i either

	x	x	x
x	x	x	
x		x	x
x	x		x

x	x	x	
	x	x	x
x	x		x
x		x	x

x		x	x
x	x		x
	x	x	x
x	x	x	

x	x		x
x		x	x
x	x	x	
	x	x	x

Figure 2

(i) $b_i = 0$ and $a_i \epsilon D_n$, i.e., x_i is constant

(ii) $b_i = 1$ and $a_i = 0$, or

(iii) $b_i = -1$ and $a_i = n-1$,

and not all b_i's are zero. Then by-the definition of independent permutations, the function of z defined by

$$P_1(a_1 + b_1 \cdot z) + \ldots + P_d(a_d + b_d \cdot z)$$

is a permutation and hence for some value of z it equals 0 , and by the definition of the set S the corresponding node is not in S . This completes the proof.

Corollary. Given any d there is an n > 1 for which $f(n,d) = n^d - n^{d-1}$

This follows from the above theorem and from the fact that S(n) can be made arbitrarily large by a suitable choice of n .

5. Relation to Pólya's Theorem

We return, now, to the problem motivated in the introduction, that is, the question of the existence of a configuration of n noncapturing superqueens on an $n \times n$ board. We shall relate the existence of such configurations to our concept of independent permutations.

Theorem 5. If n is any integer n > 1 , then n noncapturing superqueens can be placed on an $n \times n$ board if and only if $S(n) \geq 2$. Furthermore, the number of ways in which n superqueens can be so placed equalsthe number of permutations P over D_n such that $\{I,P\}$ is independent.

Proof. All arithmetic below is modulo n . And we use the words "square" (in an $n \times n$ board), "node", and "vertex" interchangeably.

(a) If $S(n) \geq 2$ there exists a set $\{P_1, P_2\}$ of independent permutations over D_n. Consider the configuration in which superqueens are placed on exactly those nodes $\langle x,y\rangle$ where $P_1(x) + P_2(y) = 0$. Now, clearly, there is exactly one superqueen in every row and column. Furthermore, two superqueens cannot be on the same diagonal (with wrap around) because any diagonal can be represented as $y = a+bx$ where b is 1 or -1, and $a \in D_n$, then as $P_1(x) + P_2(a+bx)$ must be a permutation (as P_1, P_2 are independent) there can be only one point on the diagonal where it is zero, i.e., there cannot be two superqueens on the diagonal.

(b) On the other hand, if there is a configuration for noncapturing superqueens then for each $y \in D_n$ there is a unique $x \in D_n$ such that there is a superqueen at $\langle x,y\rangle$. Let Q denote the set of nodes on which superqueens are placed. We define the permutation P by $P(y) = -$(the unique x for which $\langle x,y\rangle \in Q$) . P is a permutation because for any x there is a unique y for which $\langle x,y\rangle \in Q$. Now, the set $\{I, P\}$ where I is the identity permutation, is independent, because if not there exist $a_1, a_2 \in D_n$, $b_1, b_2 \in \{0,1,-1\}$ not both zero, and $x_1, x_2 \in D_n$, $x_1 \neq x_2$ such that

$$I(a_1+b_1 \cdot x_1) + P(a_2+b_2 \cdot x_1) = I(a_1+b_1 \cdot x_2) + P(a_2+b_2 \cdot x_2) .$$

Thus

$$P(a_2+b_2 \cdot x_1) - P(a_2+b_2 \cdot x_2) = b_1 \cdot (x_2 - x_1) .$$

Now, $b_2 \neq 0$ because if $b_2 = 0$ then b_1 too would have to be 0 . By the definition of P , there are superqueens on nodes

$v_1 = \langle -P(a_2+b_2 \cdot x_1), a_2+b_2 \cdot x_1 \rangle$ and on $v_2 = \langle -P(a_2+b_2 \cdot x_2), a_2+b_2 \cdot x_2 \rangle$ which is the same as $\langle -P(a_2+b_2 \cdot x_1) + b_1(x_2-x_1), a_2+b_2 \cdot x_2 \rangle$. Since $b_2 \neq 0$ and $x_1 \neq x_2$ the nodes v_1 and v_2 are distinct. Now consider the line of nodes $\langle x,y \rangle$ given by

$$-b_2 \cdot x + b_1 \cdot y = b_2 \cdot P(a_2+b_2 \cdot x_1) + a_2 \cdot b_1 + b_1 \cdot b_2 \cdot x_1$$

(this is a valid line since both b_1, b_2 are not zero). But both nodes v_1 and v_2 fall on this line and hence in the original arrangement, one superqueen can capture another -- a contradiction.

It should be noted that in this construction the set of nodes Q where superqueens are placed is given by those $\langle x,y \rangle$ for which $I(x) + P(y) = 0$. Comparing with part (a) of the proof we have a 1-1 correspondence between superqueen solutions and independent permutations of the form $\{I,P\}$.

From our earlier results (Theorems 1, 3) we see that (for $n > 1$) $S(n) \geq 2$ if and only if n is not a multiple of two or three. We say a superqueens solution is <u>regular</u> if it corresponds to an independent set $\{I, a \cdot I+b\}$, otherwise it is <u>nonregular</u>. The smallest nonregular solution is for n = 13 (see Section 3.1). Incidentally, Pólya's theorem can also be used to solve the related problem for super nite-queens. A <u>nite-queen</u> is a piece that can move like a chess queen or a chess knight (two squares in a horizontal or vertical direction and one square in an orthogonal direction). A super nite-queen is a nite-queen with wrap-around moves allowed. The problem of placing n noncapturing super nite-queens on an $n \times n$ board has been mentioned several times in the literature (see, for example, Golomb [3]). There exists a solution if and only if $n \geq 11$ and n is not a multiple of two or three. We can show this by using independent permutations as follows. Clearly a solution can exist only if n is not a multiple of two or three. From the construction in the proof of Theorem 5 we see that if the independent pair $\{I, P\}$ in which P has the form $P = a \cdot I+b$, corresponds to a solution to the super nite-queens problem, then the knight's-move constraint requires that $a \neq 2, n-2, (n-1)/2, (n+1)/2 \bmod n$. But, for $n = 5$ or 7 the only independent pairs $\{I,P\}$ are those for which P has the form $a \cdot I+b$, and $a=2$ or 3 if $n = 5$, and $a = 2,3,4$ or 5 if $n = 7$ (see Section 3.1), none of which corresponds to a solution. Hence there is no solution for $n = 5$ or 7. But we can easily get a solution if $n \geq 11$ from the independent pair $\{I,3I\}$ if, if course, n is not a multiple of two or three. Also, the example of the independent set $\{I,P\}$ for D_{13} in Section 3.3 corresponds to a nonregular solution for the super nite-queens problem. There is another interesting piece which we call a <u>super K-queen</u>. It moves like the super nite-queen except that in one move it can take any number of knight steps in any <u>one</u> direction, whereas the super nite-queen could take only one step. A proof somewhat similar to the proof for Theorem 3 can be used to show that n non-capturing super K-queens can be placed on an $n \times n$ board if and only if n is not a multiple of 2,3,5, or 7 (by showing that if m, the least prime factor of n, is 5 or 7 then no solution exists, and if $m \geq 11$ then $\{I,3I\}$ corresponds to a solution). The smallest nonregular solution of super K-queens is unknown, but a computer search shows that only regular solutions exist for $n \leq 23$.

Acknowledgment

The author is pleased to acknowledge several helpful discussions with Prof. V. Chvátal of Stanford University.

References

[1] A. K. Chandra, "On the solution of Moser's problem in 4 dimensions," in Report No. CS-286, Computer Science Dept., Stanford University, June 1972.

[2] V. Chvátal, "Remarks on a problem of Moser", Canad. Math. Bull., Vol. 15 (i), 1972.

[3] S. W. Golomb, "Sphere packing, coding metrics, and Chess puzzles," in the Proceedings of the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications, May 1970, pp. 176-189.

[4] D. E. Knuth, The Art of Computer Programming, Vol. 1, Addison-Wesley, 1968.

[5] L. Moser, "Problem 21," Proceedings of 1963 Number Theory Conference, University of Colorado, mimeographed, 79.

[6] L. Moser, "Problem P.170," Canad. Math. Bull., Vol. 13, pg. 268 (1970).

[7] G. Pólya, "Uber die 'doppelt-periodischen' Losungen des n-Damen-Problems," in Mathematische Unterhaltungen und Spiele, by W. Ahrens, Verlag und Druck von B. G. Teubner in Leipzig 1918, pp. 364-374.