Magic N-Cubes Form a Free Monoid

Allan Adler
P.O. Box 20276, Cherokee Station, New York, NY 10021

Abstract

In this paper we prove a conjecture stated in an earlier paper [A-L]. The conjecture states that with respect to a rather natural operation, the set of N-dimensional magic cubes forms a free monoid for every integer $N > 1$. A consequence of this conjecture is a certain identity of formal Dirichlet series. These series and the associated power series are shown to diverge. Generalizations of the underlying ideas are presented. We also prove variants of the main results for magic cubes with remarkable power sum properties.

(1980) AMS Classifications: 05A15, 05A17, 05A19, 05B15, 08A02, 08A05, 08B20, 10A05, 10A25, 10A50, 10H40, 10M20, 15A30, 15A33, 15A51, 20M05

Key Words: array, estimate, free monoid, generating function, inescapable submonoid, infinite dimensional variety, irreducible, left prime, magic N-cube, monoid, persuasive submonoid, semidirect product

§0 Introduction

According to the book of W.S.Andrews [An], the study of magic squares is quite old and dates back to ancient Tibet, to 12th century China, to 9th century Arab astrologers and perhaps much further. Indeed, Andrews speculates that magic squares might even be prehistoric. Despite their antiquity, they have often been regarded by serious mathematicians as a waste of time, although many of the great mathematicians of the past, such as Euler [E1],[E2], Ramanujan [R1],(cf. [R2]) and Fermat [F], found it to their liking to waste quite a lot of time on them. One possible reason for this double standard is that although magic squares are a lot of fun, no one believes that it is possible to prove general theorems about them. Indeed, until recently all work on magic squares consisted in presenting methods of constructing magic N-cubes or of examining the properties of particular magic N-cubes, with most attention being devoted to the case $N = 2$. Since no explicit method has ever been given for constructing all magic N-cubes, the work of past researchers has necessarily been limited to special classes of magic N-cubes. Even so, their work has in some cases also drawn on interesting mathematics such as the related studies of Latin squares and finite geometries. One can also mention the paper [A-L], which used Prouhet sequences[1] to construct an infinite class of

[1] Prouhet sequences have as a special case a sequence used by Morse [Mo1] (cf. [Mo2], [M-H 1]) to give a counterexample to the Poincaré-Bendixson theorem in higher genus and by Morse and Hedlund [M-H 2] to give an example of unending chess.

magic cubes with remarkable power sum properties, and the recent papers [A1],[A-W], in which p-adic L-functions [Iw] are used to construct an infinite class of magic p-dimensional cubes.[2]

In recent times, mathematicians concerned with areas quite different from magic squares have been pleased and amused when they could report that their researches have led them to objects which, if not actually magic squares, at any rate exhibit some of the properties of magic squares. Thus it was that Ax [Ax1], in his studies of quantum mechanics [Ax2], enjoyed referring to doubly stochastic matrices as "magic squares"; that André Weil [W1] was able to point out properties of the period matrices of Fermat curves [W2] which made them like "magic squares"; and that I.M. Gelfand in his lectures on generalized hypergeometric functions [Ge] was happy to report that some of the objects of his theory are described by "magic squares". Some such "magic squares" then become legitimate objects of study in their own right. For example, in his work on magic graphs, Richard Stanley [S1],[S2] used the Hilbert syzygy theorem to study the growth as $k \to \infty$ of the number of arrays of positive integers with entries less than k and having many of the properties of magic squares. Nevertheless, the study of magic N-cubes themselves remains disreputable and probably always will.

It is not the purpose of this article, however, to survey the subject of magic N-cubes nor to create enthusiasm for the topic where it does not already exist. It is instead to report on a theoretical development in the subject of magic N-cubes, and here I mean genuine magic N-cubes, not the imitations which were mentioned in the previous paragraph. The simple fact is that until the paper [A-L] appeared in 1977, no theorem had ever been published concerning the set of all magic N-cubes as a whole. What was new in [A-L], apart from a new construction of a remarkable class of magic N-cubes, was the introduction ([A-L], p. 624) of an operation on the set of all magic squares. This operation is associative and has an identity element and therefore makes the set of magic squares into a monoid. Furthermore, it was conjectured that with respect to this operation, the set of magic squares is a free monoid. It was also remarked in [A-L], but not explicitly proved, that the operation makes sense for magic N-cubes for all N and the conjecture was expected to hold for all $N > 1$. In this paper, we show that the conjecture is true.[3] By adapting the techniques of the proof, we show that magic N-cubes satisfying certain remarkable power sum properties also form a free monoid. We then consider various generating functions for the number of magic N-cubes and show that they diverge. Although pleasant to know, the real significance of their divergence lies in the estimates that one uses. For, what one really wants to know, either exactly or approximately, is how many magic N-cubes there are of a given size. We therefore summarize the estimates we obtain at the end of the article. Undoubtedly one can get much better estimates even from the constructions we have used. Whether one can get accurate asymptotic estimates for the number of magic N-cubes is another question. It is conceivable that the "sporadic" magic squares which do not arise from general constructions form an infinite set larger in the sense of its growth than the set of magic squares that do arise from such constructions. If this is the case, then the approach we have taken to obtaining estimates cannot, even in principle, be made accurate through more careful study of general constructions. In order to test for this possibility, it seems reasonable to suggest that in addition to using computers to enumerate the magic squares of various sizes, as many people are doing, one should also be trying to see whether the magic squares produced by these searches have natural generalizations to new infinite families.

The contents of the paper are as follows. In §1, we prove (Theorem 1.26) that magic squares form a free monoid. These ideas apply as well in the case of magic N-cubes, but since they only involve trivial modifications of the proof for magic squares, the details are left to the reader. In §2, which is devoted to generalizations, we note that the frames of the magic N-cubes form a monoid, as do the summation conditions to which they are subjected, and we formulate these observations

[2] One can view this result as saying that one can use the Riemann zeta function and certain Dirichlet L-functions to construct magic p-cubes.

[3] For $N = 1$, every permutation of the interval $[1, r]$ is a magic 1-cube, since there is only one "side" and that side is also the only "diagonal". In this case, the monoid is definitely not free, since for example, the magic 1-cubes $\boxed{1}\boxed{2}\boxed{3}$ and $\boxed{1}\boxed{2}$ are irreducible and commute with each other under the monoid operation, the product being $\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}$. The generators of the monoid are the irreducible elements of the monoid, but I don't know the relations among them.

in a very general setting, motivated by the desire to understand the monoids $\mathcal{S}_N(t,g)$ (see §3) from an abstract point of view. In earlier draft of this article [A2], these generalizations were worked out in considerable detail including some discussion of infinite dimensional varieties. In the present article, for reasons of space, the discussion is reduced to a brief sketch. In §3, we consider classes of magic N-cubes that have certain remarkable power sum properties for their entries. We denote these monoids $\mathcal{S}_N(t,g)$ and prove in Theorem 3.1 that they are free on infinitely many generators. In §4, we take up the question of the convergence of the generating functions and, after showing that they diverge, conclude the article with a summary of the estimates we obtained. These estimates can undoubtedly be greatly improved by a more careful application of the methods we are using. However they are all based on the observation that certain methods of constructing magic N-cubes are compatible with many permutations. More desirable than merely having better estimates would be to have another observation of an essentially different nature.

Throughout this article, N will denote an integer greater than 1 and $\mathbf{Z}$ will denote the ring of integers. We will often regard $\mathbf{Z}$ as a monoid either under addition or under multiplication, as the situation requires. If a and b are integers, we will denote by $[a,b]$ the set of integers which are $\geq a$ and $\leq b$. If S is a monoid, we will denote the identity element of S by 1_S.

The author wishes to thank C.Cowsik for his help in proving the crucial Lemma 1.25 and P.Szüsz for his help in proving the divergence of the generating functions. The author is also grateful to Roger Howe and Walter Feit for making it possible for him to use facilities at Yale University. Finally, the author is grateful to Michel Broué for making it possible to use a computer at the École Normale Supérieure in Paris, where final changes were made in the manuscript.

§1 Magic Squares

Definition (1.1): By a **magic square of order n**, also called an $\mathbf{n \times n}$ **magic square**, we mean an $n \times n$ square array $A = (a_{ij})$, $0 \leq i, j \leq n-1$, of positive integers such that

(i) each of the integers from 1 to n^2 inclusive occurs exactly once among the entries of A;

(ii) for $0 \leq i \leq n-1$, the sum $\sum_{j=0}^{n-1} a_{ij}$ is independent of i;

(iii) for $0 \leq j \leq n-1$, the sum $\sum_{i=0}^{n-1} a_{ij}$ is independent of j;

(iv) the sums $\sum_{i=0}^{n-1} a_{ii}$ and $\sum_{i=0}^{n-1} a_{i,n-i-1}$ are equal to the sums given in (ii) (and therefore to those in (iii) as well).

For example,

$$\begin{array}{|c|c|c|}\hline 8 & 1 & 6 \\ \hline 3 & 5 & 7 \\ \hline 4 & 9 & 2 \\ \hline \end{array}\ ,\ \begin{array}{|c|}\hline 1 \\ \hline \end{array} \quad \text{and} \quad \begin{array}{|r|r|r|r|}\hline 1 & 15 & 14 & 4 \\ \hline 12 & 6 & 7 & 9 \\ \hline 8 & 10 & 11 & 5 \\ \hline 13 & 3 & 2 & 16 \\ \hline \end{array}$$

Figure 1

are magic squares.

We let let $\mathcal{M}_2$ denote the set of all magic squares. We will define an operation on $\mathcal{M}_2$. The operation will be denoted by $*$ and will be referred to as **multiplication**. Before defining our operation on $\mathcal{M}_2$ formally, let us illustrate it with an example. Let A be the 3×3 magic square in Figure 1 above and let B be the 4×4 magic square in Figure 1. To form the magic square $A * B$, note that B is 4×4 in this case and make a big, empty 4×4 frame, as in Fig.2 below.

Fig. 2

8	1	6									
3	5	7									
4	9	2									

Fig. 3

Now locate the square in B which contains the number 1 and place a copy of A in the corresponding square of the frame we have just constructed, as in Fig.3 above. We can view this as a way of counting out 9 consecutive numbers. Now locate the square in B containing 2 and in the corresponding square of Fig. 3, count out the next 9 numbers in the same pattern. It is the same to say that one adds 9 to all of the entries of A and places the result in the box corresponding to the position of the 2 in B, as in Fig.4 below.

8	1	6									
3	5	7									
4	9	2									
						17	10	15			
						12	14	16			
						13	18	11			

Fig. 4

8	1	6	134	127	132	125	118	123	35	28	33
3	5	7	129	131	133	120	122	124	30	32	34
4	9	2	130	135	128	121	126	119	31	36	29
107	100	105	53	46	51	62	55	60	80	73	78
102	104	106	48	50	52	57	59	61	75	77	79
103	108	101	49	54	47	58	63	56	76	81	74
71	64	69	89	82	87	98	91	96	44	37	42
66	68	70	84	86	88	93	95	97	39	41	43
67	72	65	85	90	83	94	99	92	40	45	38
116	109	114	26	19	24	17	10	15	143	136	141
111	113	115	21	23	25	12	14	16	138	140	142
112	117	110	22	27	20	13	18	11	139	144	137

Fig. 5

Next one finds the 3 of B and counts out the next 9 numbers in the corresponding place in the frame. Continuing in this way, we eventually get the magic square in Fig.5 above.

The product square $A * B$ has order 12, the product of the orders of A and B. It is convenient to have an analytic expression for this operation and for that purpose we can work in somewhat greater generality.

Let $\mathcal{G}$ be an abelian group and choose an element u of $\mathcal{G}$ once and for all. Denote by $\mathcal{A}(\mathcal{G})$ the set of all square arrays of elements of $\mathcal{G}$, the size of the arrays being arbitrary. If $A = (a_{ij})$, $0 \leq i, j \leq m-1$, and $B = (b_{kl})$, $0 \leq k, l \leq n-1$ are elements of $\mathcal{A}(\mathcal{G})$ of sizes $m \times m$ and $n \times n$ respectively, their product $A * B$ will be the $mn \times mn$ matrix $E = (e_{\alpha\beta})$ whose (α, β)-th entry is given by

$$e_{\alpha\beta} = m^2 \cdot (b_{kl} + u) + a_{ij} \tag{1.2}$$

where

$$(\alpha, \beta) = m \cdot (k, l) + (i, j). \tag{1.3}$$

Here one should note that as i, j run over the integers from 0 to $m-1$ and k, l run over the integers from 0 to $n-1$, the numbers α, β will run over the integers from from 0 to $mn-1$. So we have defined all the entries of E. A moment's thought will show that if we take $\mathcal{G}$ to be the group $\mathbf{Z}$ of rational integers and $u = -1$ and if we let A and B be magic squares, then we recover the operation we have defined for magic squares. It is also easy to see that in general the 1×1 array $\boxed{u}$ is a 2-sided identity element for the operation $*$. Furthermore, the reader will easily verify that the operation $*$ is associative (see for example [A-L]). A set S closed under an associative operation is called a **semigroup**. A semigroup with an identity element is called a **monoid**. We therefore have the following result.

Lemma (1.4): *Let $\mathcal{G}$ be an abelian group. The set $\mathcal{A}(\mathcal{G})$ of all square arrays with entries in $\mathcal{G}$ is a monoid with identity element $\boxed{u}$ with respect to the operation $*$ defined by equations (1.2) and (1.3).*

If S is a monoid with identity element s with respect to an associative operation $\circ$ then a subset T of S is called a **submonoid** of S if T contains the identity element s of S and is closed under the operation $\circ$. Returning to the original construction involving magic squares, we have the following result, whose straightforward proof is left to the reader (cf.[A-L]).

Proposition (1.5): *Let $\mathcal{M}_2$ denote the set of all magic squares. Let $\mathcal{A}(\mathbf{Z})$ denote the monoid obtained by taking G to be the additive group of integers and $u = -1$ in Lemma (1.4). Then $\mathcal{M}_2$ is a submonoid of $\mathcal{A}(\mathbf{Z})$.*

If we modify condition (i) of Definition 1.1 so that the entries of a magic square of order n run from 0 to $n^2 - 1$ instead of from 1 to n^2 and modify the product $*$, as given in Figures 2-6, accordingly, then the analytic expression for the product becomes simpler. It is the product inherited from $\mathcal{A}(\mathbf{Z})$ when we take $u = 0$ instead of $u = -1$.
The notation $\mathcal{M}_2$ and $\mathcal{A}(\mathbf{Z})$ introduced in Proposition (1.5) will be retained throughout this section.

Definition (1.6): Let S be a monoid with identity element s with respect to an operation $\circ$. We say that S is is **left cancellative** if for any elements a, b, c of S, the identity

$$a \circ b = a \circ c \tag{1.7}$$

implies $b = c$. Similarly we say that S is **right cancellative** if for any elements a, b, c of S, the identity

$$a \circ c = b \circ c \tag{1.8}$$

implies $a = b$.

Lemma (1.9): *Let $\mathcal{G}$ be an abelian group and let u be an element of $\mathcal{G}$. Then the monoid $(\mathcal{A}(\mathcal{G}), *, u)$ is right cancellative.*

Proof: Let A, B and C be elements of $\mathcal{A}(\mathcal{G})$. Suppose that A is $m \times m$, B is $n \times n$ and C is $p \times p$. If $A * C = B * C$ then we must have $mp = np$ and therefore $m = n$. We therefore have

$$m^2 \cdot (c_{kl} - 1) + a_{ij} = m^2 \cdot (c_{kl} - 1) + b_{ij} \tag{1.10}$$

for $0 \leq i, j \leq m - 1$ and $0 \leq k, l \leq n - 1$, which implies that $a_{ij} = b_{ij}$ for all i, j. Therefore $A * C = B * C$ implies $A = B$ and we are done.

Lemma (1.11): *Let $\mathcal{G}$ be an abelian group and let u be an element of $\mathcal{G}$. Then the monoid $(\mathcal{A}(\mathcal{G}), *, u)$ is left cancellative if and only if the group $\mathcal{G}$ is torsion-free.*

Proof: Let A, B, C be elements of $\mathcal{A}(\mathcal{G})$ and suppose that A is $m \times m$, B is $n \times n$ and C is $p \times p$. If $A * B = A * C$ then we must have $mn = mp$ and therefore $n = p$. It follows that

$$m^2 \cdot (b_{kl} - 1) + a_{ij} = m^2 \cdot (c_{kl} - 1) + a_{ij} \tag{1.12}$$

for $0 \leq i, j \leq m - 1$ and $0 \leq k, l \leq n - 1$, which implies that $m^2 \cdot (b_{kl} - c_{kl}) = 0$ for all k, l. Since the group G is torsion free, it follows that $b_{kl} = c_{kl}$ for all k, l. Therefore, the equation $A * B = A * C$ implies $B = C$ and we are done.

Definition (1.13): Let S be a monoid with identity element s with respect to the law of composition $\circ$. Let T be a submonoid of S. We say that T is **persuasive** in S if the following condition is satisfied: for any elements a, b, c of S such that $a \circ b = c$, if two of the elements a, b, c belong to T then so does the third. We say that T is **inescapable** in S if whenever the identity $a \circ b = c$ holds in S with c in T, the elements a, b must also belong to T. It is easy to see that an inescapable submonoid is persuasive.

Lemma (1.14): *The submonoid $\mathcal{M}_2$ of $\mathcal{A}(\mathbf{Z})$ is persuasive. The arrays which satisfy conditions (ii),(iii) of Definition 1.1 form an inescapable submonoid of $\mathcal{A}(\mathbf{Z})$*

Proof: Let A, B, C be elements of $\mathcal{A}(\mathbf{Z})$, where A is $m \times m$, B is $n \times n$ and C is $mn \times mn$, and suppose that $A * B = C$. Then we have

$$\begin{aligned} \sum_{r=0}^{mn-1} c_{rs} &= \sum_{i=0}^{m-1} \sum_{k=0}^{n-1} \left(m^2 \cdot (b_{kl} - 1) + a_{ij}\right) \\ &= \left(m^3 \sum_{k=0}^{n-1} b_{kl}\right) - m^3 n + \left(n \sum_{i=0}^{m-1} a_{ij}\right), \end{aligned} \tag{1.15}$$

where $(r, s) = m \cdot (k, l) + (i, j)$. If in the above equations, we replace the row or column of A we are using by another and keep the row or column of B fixed, we do not change the value of the expression. That is because C belongs to $\mathcal{M}_2(\mathbf{Z})$ and all we are doing is choosing another row or column of C. Since we have kept the row or column of B fixed, its contribution is also unchanged. It follows that the sum over the row or column of A is likewise unchanged, which proves that A satisfies conditions (ii) and (iii) of Definition 1.1. Similarly, if one fixes the row or column of A and varies the row or column of B, one proves that B satisfies conditions (ii) and (iii) of Definition 1.1. This proves that arrays satisfying conditions (ii) and (iii) form an inescapable submonoid. As for condition (iv), the sum $\sum c_{ii}$ over the main diagonal of C is $m^2 \sum (b_{jj} - 1)$ plus $\sum a_{kk}$. If we change to the other diagonal, the sum for C doesn't change and therefore it doesn't change for A if and only if it doesn't change for B. This shows that condition (iv) is persuasive. It remains to verify condition (i) of Definition (1.1). If A and B are magic squares then by Proposition (1.5) so is C. Therefore if two of A, B, C are magic squares then C is a magic square and therefore satisfies condition (i) of Definition (1.1). We can write

$$c_{rs} = m^2 \cdot (b_{kl} - 1) + a_{ij} \tag{1.16}$$

where

$$(r, s) = m \cdot (k, l) + (i, j) \tag{1.17}$$

and $0 \leq i, j \leq m - 1$ and $0 \leq k, l \leq n - 1$. If A satisfies condition (i) of Definition (1.1) then in equation (1.16) the elements a_{ij} are determined by the condition that $c_{rs} - a_{ij}$ must be divisible by m^2 and therefore we have

$$b_{kl} = \left[\frac{c_{rs} + m^2 - 1}{m^2}\right] \tag{1.18}$$

which implies that

$$1 \leq b_{kl} \leq n^2. \tag{1.19}$$

Since the $(mn)^2$ numbers c_{rs} in equation (1.16) must be distinct, the same must be true of the n^2 numbers b_{kl}. Therefore, B satisfies condition (i) of Definition (1.1). Conversely, suppose that B satisfies condition (i) of Definition (1.1). By equation (1.16), the m^2 elements a_{ij} must be a full set of representatives for the residue classes modulo m^2 and for each c_{rs} there is a unique a_{ij} such that

$c_{rs} - a_{ij}$ is divisible by m^2. If some a_{ij} is less than 1, choose (r, s) such that $c_{rs} - a_{ij}$ is divisible by m^2 and such that c_{rs} is as large as possible. Then we have

$$c_{rs} - a_{ij} \geq c_{rs} \geq (mn)^2 \tag{1.20}$$

which by equation (1.16) implies that

$$b_{kl} \geq n^2 + 1, \tag{1.21}$$

contradicting the fact that B satisfies condition (i) of Definition (1.1). Therefore we must have $a_{ij} \geq 1$ for all i, j. A similar argument, which we leave to the reader, shows that $a_{ij} \leq m^2$ for all i, j. Since the a_{ij} represent all of the m^2 residue classes modulo m^2, it follows that A satisfies condition (i) of Definition (1.1). This proves the lemma.

Remark (1.22): I don't know whether $\mathcal{M}_2$ is an inescapable submonoid of $\mathcal{A}(\mathbf{Z})$.

The following definition is motivated by the corresponding notions from elementary number theory.

Definition (1.23): Let S be a monoid with identity element s with respect to an operation $\circ$. We will say that element t of S is **irreducible** if $t \neq s$ and if for any elements u, v of S such that $t = u \circ v$ we have either $u = s$ or $v = s$. An element t of S is said to be **left prime** if for any elements u, v, w of S such that $t \circ u = v \circ w$, there is an element x of S such that $v = t \circ x$. This definition of irreducibility is more restrictive than the one generally accepted. However since the monoids in which we wish to study irreducible elements have no units other than the identity element, our definition will in practice coincide with the usual one.

The following lemma follows by an obvious induction on the order of the order of the magic square.

Lemma (1.24): *The set of all irreducible magic squares generates the monoid $\mathcal{M}_2$ of all magic squares. In other words, every magic square can be written as a product of irreducible magic squares.*

In order to prove that the monoid $\mathcal{M}_2$ is free, we only have to prove that every magic square is *uniquely* a product of magic squares. Indeed, a monoid is free if and only if it is freely generated by its irreducible elements. That this is the case for $\mathcal{M}_2$ follows, in analogy with the proof of the fundamental theorem of arithmetic, by a simple induction as soon as one has proved that an irreducible magic square is left prime. Therefore, the freeness of $\mathcal{M}_2$ is a consequence of the following simple lemma.

Lemma (1.25): (Irreducible Implies Prime) *Let A, B, C, D be magic squares such that $A * B = C * D$. Suppose A is $m \times m$, B is $n \times n$, C is $p \times p$ where $m \leq p$. If A is irreducible then there is a magic square E such that $C = A * E$.*

Proof: We will first show that m must divide p. Here we prefer to give a geometric argument since the key insight is geometrical and is lost in analytic formulations of the proof. We will therefore refer to the geometric description of the operation on magic squares, as illustrated in Figures 2-6. Let $F = A * B = C * D$. If we view F is the product $C * D$ then F is partitioned into $p \times p$ squares. Let C_1 denote the $p \times p$ square which contains the number 1 in F. Then C_1 is an exact replica of the magic square C and in particular contains all of the entries of F which are ≥ 1 and $\leq p^2$ and none of the entries of F which are $> p^2$. If we now view F as the product $A * B$ then F is instead partitioned into $m \times m$ squares. The first such square contains the numbers from 1 to m^2 and is denoted A_1. The second such square contains the numbers from $m^2 + 1$ to $2m^2$ and is denoted A_2 and so on. If m does not divide p then in particular $m < p$ and m^2 does not divide p^2. Let h be the smallest integer such that $h \cdot m^2 \geq p^2$. Then the square A_h lies partly in the square C_1 and partly outside of it. Let $g > 0$ be an integer. If $g < h$ then the square A_g lies entirely inside C_1 and if $g > h$ then A_g lies entirely outside of C_1. Since A_h is $m \times n$ and C_1 is $p \times p$ with $m < p$, there must be a column of C_1 which does not meet the square A_h. Since that column must be covered by disjoint squares A_g lying entirely inside of C_1, it follows that m does divide p after all. Retaining the definition of h, we see that $h \cdot m^2 = p^2$ and therefore $h = t^2$ for some positive integer t. The square C_1 is therefore covered by squares A_g and is therefore of the form $A * E$ where E is a $t \times t$ array of nonnegative integers. Since A and C are magic squares, it now follows from Lemma (1.14) that E is a magic square and we are done.

Theorem (1.26): *The monoid $\mathcal{M}_2$ of all magic squares is freely generated by the set of all irreducible magic squares.*

Proof: In view of the Irreducibility Implies Prime Lemma and the remarks preceding it, the proof may safely be entrusted to the reader.

§2 Generalizations

In the preceding section, we have stated our result in the case of magic squares because of the highly geometric and visual nature of the operation and proof and the comparatively simple notation in that case. One can also define **magic N-dimensional cubes** (also known as **magic N-cubes**) in a similar way to that given in Definition 1.1 and the reader is invited to provide the definition herself, the only caution being that the condition (iv) on the sum over the diagonals is generalized in N dimensions to the sum over the *longest* diagonals, the ones joining opposite corners of the N-cube. Similarly one can, with only minor changes, define the operation $*$ on the set $\mathcal{M}_N$ of all magic N-cubes. The same arguments then apply with only minor modifications to prove that the set $\mathcal{M}_N$ of all magic N-cubes forms a free monoid. We omit the details of this generalization, whose only complications are notational.

One can in fact generalize much further with no essential difficulty. Since some of these generalizations might be of independent interest, and since to some extent they facilitate the discussion of §3, we will indicate some of them briefly, leaving the verification of the elementary details to the reader.

(1) Let S, H be monoids and suppose that H is an S-module, i.e. we have a homomorphism from S into the monoid of endomorphisms of the monoid S. Denote by $\mathcal{F}(S,H)$ the set of all pairs (F,σ) consisting of a finite subset F of H and an element σ of S. The pair (F,σ) is called a **frame**, F is called the **turf** of the frame and σ is called the **nominal order** of the frame. Then $\mathcal{F}(S,H)$ forms a monoid in which the product of (F_1,σ_1) and (F_2,σ_2) is the frame $(F_3,\sigma_1\sigma_2)$, where F_3 is the set of all elements of the form $\sigma_1(f_2)f_1$ with $f_1 \in F_1$ and $f_2 \in F_2$. If we view a magic N-cube as an array, hence a function defined on a certain cubical subset of $\mathbf{Z}^N$, this definition allows us to consider domains which instead are finite subsets F of arbitrary monoids H. It should be clear that the monoid $\mathcal{F}(S,H)$ is simply the semidirect product of S and the monoid $\mathcal{P}(H)$ of finite subsets of H.

(2) Let S, H be as in (1) and let G be a commutative S-module. Let u be an element of G which will be fixed throughout the discussion. If $(F,\sigma) \in \mathcal{F}(S,H)$, then by an **array of type** (F,σ) **with entries in** G, we mean a triple (F,σ,λ) where λ is a function from F to G. If we do not wish to specify the type (F,σ) of the array, we will refer to it as an **array framed in** $\mathcal{F}(S,H)$. We call σ the **order** of the array (F,σ,λ). We denote by $\mathcal{A}(S,H,G)$ the set of all arrays framed in $\mathcal{F}(S,H)$. Then $\mathcal{A}(S,H,G)$ is naturally a semigroup in which the product of (F_1,σ_1,λ_1) and (F_2,σ_2,λ_2) is the array (F_3,σ_3,λ_3), where (F_3,σ_3) is the product of (F_1,σ_1) and (F_2,σ_2) in $\mathcal{F}(S,H)$ and where the function λ_3 is defined by

$$\lambda_3(h_3) = \sum{}' (\sigma_1(\lambda_2(h_2) + u) + \lambda_1(h_1))$$

where the summation runs over all elements $(h_1,h_2) \in F_1 \times F_2$ such that $h_3 = \sigma_1(h_2)h_1$. If g is an element of G, we will denote by $\boxed{g}$ the framed array $\boxed{g} = (\{e\}, s, \lambda : \{e\} \to G)$ defined by $\lambda(e) = g$, where e is the identity element of H. This notation generalizes and supersedes the notation $\boxed{u}$ introduced in §1. If g is taken to be an element of G such that $g + u = 1_G$, where 1_G is the identity element of G, then $\mathcal{A}(S,H,G)$ is actually a monoid whose identity element is $\boxed{g}$. Assume that such an element g exists. The monoid $\mathcal{A}(S,H,G)$ may then be described as the semidirect product of S with the monoid $\mathcal{P}(H;G)$ of all finite partial functions from H to G, this being the kernel of the homomophism $(F,\sigma,\lambda) \mapsto \sigma$ of $\mathcal{A}(S,H,G)$ onto S.

(3) In order to introduce the notion of a magic frame, we have to be able to specify the summation conditions. To do so in our present generality, we observe that the summation conditions traditionally considered in the study of magic N-cubes also form a monoid and use that insight in order to formulate our generalization. More precisely, let S, H, G be as in (1) and let n be a positive integer. We introduce the following monoids.

$$\begin{aligned} M_1^{(1)} &= \mathcal{F}(S,H) & M_1^{(n)} &= \prod_{i=1}^{n} M_1^{(1)} \\ M_2^{(1)} &= \mathcal{F}(S,\mathcal{P}(H)) & M_2^{(n)} &= \prod_{i=1}^{n} M_2^{(1)}. \end{aligned}$$

In the definition of $M_1^{(n)}$ and $M_2^{(n)}$ we use the product notation to denote the fibre product over S, not the cartesian product. In practice, an element of $M_1^{(1)}$ will be a subset of H over which we wish to sum the entries of an array. In the case of magic N-cubes, such a subset might be an orthogonal or a great diagonal of the N-cubes, but one considers other subsets as well. In general, we will want to sum over various subsets and we wish to handle all such subsets simultaneously. For example, if N is fixed and $H = \mathbf{Z}^N$, we can let $n = 2^{N-1}$ and view the set of n great diagonals of the N-cube as an element of $M_1^{(n)}$. In that case, if (F_i, σ_i) is an N-cube for $i = 1, 2$ and if A_i is the element of $M_1^{(n)}$ corresponding to the set of great diagonals of (F_i, σ_i), then the product in $M_1^{(n)}$ of A_1 and A_2 will be the set of great diagonals of the product of (F_1, σ_1) and (F_2, σ_2). This is quite satisfying but does not suffice to describe the orthogonals. The reason is that the number of orthogonals of an N-cube depends on the size of the N-cube and not just on N. For this reason we introduced the monoid $M_2^{(1)}$. The orthogonals parallel to a particular axis of an N-cube form an element of $M_2^{(1)}$. If for $i = 1, 2$, B_i is the element of $M_2^{(1)}$ corresponding to the orthogonals of an N-cube (F_i, σ_i) parallel to a particular axis (the same axis for $i = 1, 2$), then the product in $M_2^{(1)}$ of B_1 and B_2 is the element corresponding to the set of orthogonals in that same direction in the product of (F_1, σ_1) and (F_2, σ_2). This is also satisfying, but since there are N directions in which to choose the orthogonals, the system of all orthogonals is described by an element of $M_2^{(N)}$. Thus, the set of summation conditions which a magic N-cube is expected to satisfy is an element of the monoid

$$M_1^{(n)} \times M_2^{(N)},$$

where $n = 2^{N-1}$. In order to simplify the notation, we observe that the monoid $M_1^{(1)}$ may be embedded in the monoid $M_2^{(1)}$ by associating to a subset F of H the singleton $\{F\}$. Therefore, we may regard the set of summation conditions as an element of $M_2^{(d)}$ where $d = N + 2^{N-1}$. These considerations motivate the following definition: let (F, σ, λ) be an element of $\mathcal{A}(S, H, G)$, let d be a positive integer and let $C = (C_1, \ldots, C_d)$ be an element of $M_2^{(d)}$ such that for $1 \leq i \leq d$, every element of C_i is a subset of F. We say that the array (F, σ, λ) is **C-stochastic** if for $1 \leq i \leq d$ and for E in C_i, the summation $\sum_{h \in E} \lambda(h)$ is independent of i and E. Suppose that ϕ is a homomorphism from a submonoid $\mathcal{F}$ of the monoid $\mathcal{F}(S, H)$ to the monoid $M_2^{(d)}$ such that for every (F, σ, λ) in $\mathcal{F}$ the order of $\phi(F, \sigma, \lambda)$ is σ. We will say that an array (F, σ, λ) is **phi-stochastic** if (F, σ) belongs to $\mathcal{F}$ and if (F, σ, λ) is $\phi(F, \sigma)$-stochastic. If $\mathcal{F}$ and ϕ are such, we denote by $\mathcal{M}(\phi)$ the subset of $\mathcal{A}(S, H, G)$ consisting of all ϕ-stochastic arrays. Then $\mathcal{M}(\phi)$ is a submonoid of $\mathcal{A}(S, H, G)$. Now suppose that the only pair $(\sigma, g) \in S \times G$ with $\sigma(g) = 1_G$ is $(1_S, 1_G)$, where 1_S is the identity element of S. Then then the monoid $\mathcal{M}(\phi)$ is a persuasive submonoid of $\mathcal{A}(S, H, G)$.

By placing some restrictions on the monoid G, one can generalize further the notions of stochasticity introduced in (3). More precisely, one assumes that G is the additive group of an algebraically closed field k. In that case, one can introduce monoids of summation conditions by means of certain classes of infinite dimensional varieties over k and prove that they are free. Space does not permit the detailed description of this general construction and we presently know only one interesting example of it, namely in connection with the monoids $\mathcal{S}_N(t,g)$ defined in the next section. So we will confine our attention to that example, which we describe in the next section without reference to infinite dimensional varieties.

§3 Magic N-cubes with remarkable power sum properties

Let $n \in [1,N]$. An n-cube contained in an N-dimensional cubical array f of order d is then the intersection of that array with a certain number of hyperplanes parallel to the faces of the array. As such it is completely described by selecting a subset J of cardinality $N-n$ of $[1,N]$ and prescribing a function $h: J \to [0,d-1]$. Two n-cubes having the same set J are said to be **conjugate**.

Let $g: [1,N] \to \mathbf{Z}$ be any nonnegative function and let $t > 1$ be an integer. We denote by $\mathcal{S}_N(t,g)$ the set of all magic N-cubes A satisfying the following two conditions:

(a) The order of A is a power of t, say t^s.

(b) For $1 \leq n \leq N$, conjugate n-dimensional subcubes have equal sums of the r-th powers of their entries, for $0 \leq r \leq g(n)$.

We also denote by $\mathcal{M}_N(t)$ the monoid of all magic N-cubes satisfying only condition (a) above. In the proof, we will use notation introduced in (1) and (2) of §2.

Theorem (3.1): *Let t, g be as above. Then $\mathcal{S}_N(t,g)$ is an inescapable submonoid of the monoid $\mathcal{M}_N$ of all magic N-cubes. Furthermore, $\mathcal{S}_N(t,g)$ is a free monoid on infinitely many generators.*

Proof: Let A, B be elements of $\mathcal{S}_N(t,g)$ and let C be their product. Any n-dimensional subcube K of C is the product in $\mathcal{F}(\mathbf{Z},\mathbf{Z}^N)$ of the corresponding subcubes K', K'' of A and B respectively. Normally we think of the n-subcubes as subsets of A, B and C but we can view them as elements of $\mathcal{F}(\mathbf{Z},\mathbf{Z}^N)$ by replacing, e.g. K' by the pair (K', t^s), where t_s is the order of C. Here the action of $\mathbf{Z}$ on $\mathbf{Z}^N$ is the usual $\mathbf{Z}$-module structure on $\mathbf{Z}^N$. Since we care about the *entries* of these n-cubes, we are concerned with the elements of $\mathcal{A}(S,\mathbf{Z}^N,G)$, where S, G are $\mathbf{Z}$ under multiplication and addition respectively and where G is viewed as an S-module via $(s,g) \mapsto s^N g$. Denote by f, f', f'' the functions that give the entries of the subcubes K, K', K'' respectively. We then have

$$\begin{aligned}\sum_{v\in K} f(v)^r &= \sum_{v'\in K'}\sum_{v''\in K''} (t^{sN} f''(v'') + f'(v'))^r \\ &= \sum_{j=0}^{r} \binom{r}{j} \left(\sum_{v'\in K'} f'(v')^{r-j}\right) \cdot \left(\sum_{v''\in K''} t^{jsN} f''(v'')^j\right)\end{aligned} \tag{3.2}$$

Since the sums over K' and K'' are independent of the choices of the n-cubes K', K'' within their conjugacy classes, the sum over K is independent of the choice of the n-cube K within its conjugacy class. This proves that $\mathcal{S}_N(t,g)$ is a submonoid of $\mathcal{M}_N$. Furthermore, the submonoid $\mathcal{S}_N(t,g)$ is an inescapable submonoid of $\mathcal{M}_N$. Indeed, suppose A, B, C are magic N-cubes such that $A * B = C$ and suppose that C belongs to $\mathcal{S}_N(t,g)$. Choose K, K', K'' as before and use the above identity for the sum of the r-th powers of the entries of K, which we know is independent of the choice of the n-cube K within its conjugacy class. If we fix the n-cube K'' and allow the n-cube K' to vary in its conjugacy class, it follows by an easy induction on r that, for $1 \leq r \leq g(n)$, the sum of the r-th powers of the entries of the entries of K' are independent of the choice of K' within its conjugacy class. Similarly, by fixing K' and letting K'' vary in its conjugacy class we see that the sum of the r-th powers of the entries of K'' is independent of the choice of the n-cube K'' within its conjugacy class. This proves that $\mathcal{S}_N(t,g)$ is an inescapable submonoid of $\mathcal{M}_N$. It follows that an irreducible element of $\mathcal{S}_N(t,g)$ is also irreducible when viewed as an element of $\mathcal{M}_N$. To see that $\mathcal{S}_N(t,g)$ is free, it suffices to prove the analogue of the Irreducibility Implies Prime Lemma for this situation. So suppose that A, B, C, D are elements of $\mathcal{S}_N(t,g)$ of orders m, n, p, q where $m \leq p$, and suppose that $A * B = C * D$ with A irreducible. In the proof of the freeness of $\mathcal{M}_N$, which we left to the reader, one proves along the way that $\mathcal{M}_N$ satisfies the analogue of the Irreducibility Implies Prime Lemma. Since A is also irreducible as a magic N-cube, it follows that we can write C as the product $A * E$ of A and another magic N-cube E. It then follows that E belongs to $\mathcal{S}_N(t,g)$. Therefore, $\mathcal{S}_N(t,g)$ is free. Finally, to see that $\mathcal{S}_N(t,g)$ has infinitely many generators, we will show that it contains infinitely many irreducible magic N-cubes. In Theorem 1 on p.620 of [A-L], it is shown how to construct a magic N-cube of order t^M for every positive integer M such that t divides MN and such that $M > 1$ when t is even. We will call that construction the **method of Prouhet sequences**. Hence infinitely many elements of $\mathcal{M}_N(t)$ are constructed by the method of Prouhet sequences. Furthermore, in Theorem 5 on p.626 of [A-L] it is shown that for $1 \leq n \leq N$ every magic N-cube A constructed in this way has the following property: for all n, conjugate n-dimensional subcubes of A have equal sums of the k-th powers of their entries for $k = 0, 1, \ldots, nr-1$. It follows that all but finitely many of the magic N-cubes in $\mathcal{M}_N(t)$ constructed by the method of Prouhet sequences belong to $\mathcal{S}(t, g)$. Therefore we will be done as soon as prove the following lemma.

Lemma (3.3): *If $M+1$ is divisible by t then the magic N-cube of order t^M constructed by the method of Prouhet sequences is irreducible.*

Proof: We refer the reader to Theorem 1 of [A-L] or to [A1], pp.16-18, for details of the method of Prouhet sequences. Let $A = (a_{i_1,\ldots,i_N})$ be a magic N-cube of order t^M constructed by the method of Prouhet sequences. Let $(i) = (i_1, \ldots, i_N)$ and $(j) = (j_1, \ldots, j_N)$ be the N-tuples such that $a_{(i)} = 0$, $a_{(j)} = 1$. Then we have $(i) = (0, \ldots, 0)$ and $(j) = (t^M - 1, \ldots, t^M - 1, 0)$. It follows that the entries 0 and 1 are on opposite faces of the N-cube and cannot lie in any proper subcube of dimension N. Therefore A is irreducible.

§4 Divergence of generating functions

It is well known that the freeness of these monoids implies identities of formal Dirichlet series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \left(1 - \sum_{n=3}^{\infty} \frac{b_n}{n^s}\right)^{-1}$$

where a_n denotes the number of elements of size n in the monoid and b_n denotes the number of irreducible elements of size n of the monoid. We will now consider the convergence properties of these formal Dirichlet series and their associated power series.

Theorem (4.1): *Let N, a_n (resp. b_n) be the number of magic N-cubes (resp. irreducible magic N-cubes) of order n. Then the formal power series*

$$\sum_{n=1}^{\infty} a_n t^n, \ \sum_{n=3}^{\infty} b_n t^n$$

both have radius of convergence equal to 0. In particular, the formal Dirichlet series introduced above are everywhere divergent for this monoid.

Proof: Let $X = (X_{k\ell})$, $0 \leq k, \ell \leq N-1$ denote the $N \times N$ matrix whose (k, ℓ)-th entry is $1 + N\delta_{k\ell}$. If M is a positive integer relatively prime to $(2N-1)!$ and if we view X as having entries in the ring $\mathbf{Z}/M\mathbf{Z}$ then X satisfies the following conditions: (1) X is invertible; (2) Every entry of X is a unit of $\mathbf{Z}/M\mathbf{Z}$; (3) If e is a vector whose entries are all ± 1 then the entries of the vector Xe are units of $\mathbf{Z}/M\mathbf{Z}$.

For every such M, we can construct a magic N-cube

$${}_M A = ({}_M A_{i_1,\ldots,i_N})$$

of order M whose entries are defined by

$${}_M A_{i_1,\ldots,i_N} = \sum_{k=0}^{N-1} j_k M^k,$$

where the digits j_k are determined by the conditions $0 \leq j_k \leq M-1$ and

$$j_k \equiv \sum_{k=0}^{N-1} X_{k\ell} i_\ell \pmod{M}.$$

For a discussion of the ideas behind this construction, see §1 of the author's paper [A1]. We will merely remark that:

(I) condition (1) guarantees that each of the numbers $0, 1, \ldots, M^N - 1$ occurs exactly once in ${}_MA$;

(II) condition (2) guarantees that for any fixed k, the k-th digits of the entries of any orthogonal of ${}_MA$ are $0, 1, \ldots, M-1$ in some order;

(III) condition (3) guarantees that for any fixed k, the k-th digits of the entries of any diagonal of ${}_MA$ are $0, 1, \ldots, M-1$ in some order.

Peter Szüsz pointed out to the author that the observations (I),(II),(III) imply that if σ is any permutation of the numbers $0, 1, 2, \ldots M-1$ then the array ${}_MA^\sigma$ defined by

$$ {}_MA^\sigma_{i_1,\ldots,i_N} = \sigma({}_MA_{i_1,\ldots,i_N}) $$

is also a magic N-cube. Therefore $a_M \geq M!$ whenever M is relatively prime to $(2N-1)!$, and that already suffices to prove that the summation $\sum_{n=1}^\infty a_n t^n$ diverges for $t \neq 0$. To show that $\sum_{n=3}^\infty b_n t^n$ also diverges, we first prove that the magic N-cube ${}_MA$ is irreducible. Indeed, the number 0 is placed in the center of ${}_MA$ and the number 1 is placed in the box indexed by $(i) = (i_0, \ldots, i_{N-1})$ where (i) satisfies $0 \leq i_k \leq M-1$ and

$$ \sum_{\ell=0}^{N-1} (1 + N\delta_{k\ell}) \cdot i_k \equiv \delta_{0k} \pmod{M} \tag{4.2} $$

for $0 \leq k \leq N-1$. It follows that $i_1 = i_2 = \ldots = i_{N-1}$ and

$$ \begin{aligned} (N+1) \cdot i_0 + (N-1) \cdot i_1 &\equiv 1 \pmod{M} \\ i_0 + (2N-1) \cdot i_1 &\equiv 0 \pmod{M}. \end{aligned} $$

Solving these equations modulo M we obtain

$$ i_0 \equiv \frac{2N-1}{2N^2} \pmod{M} \text{ and } i_1 \equiv \frac{-1}{2N^2} \pmod{M}. $$

In particular, since M is relatively prime to $(2N-1)!$, both i_0 and i_1 are units modulo M. If ${}_MA$ were reducible, we could tile it with subcubes of order R with 0 and 1 lying in a common N-cube B of order R. Here $R < M$ is a factor of M. The N cube B would have to contain all of the nonnegative integers less than R^N. For $0 \leq \nu \leq R-1$, the integer ν occurs at the point $\nu \cdot (i)$. Therefore, for $0 \leq \nu \leq R-1$ the N-cube B would contain the multiple $\nu \cdot (i)$ of (i). In particular, for $0 \leq \nu \leq R-1$, both νi_0 and νi_1 must lie among the elements $0, 1, \ldots, R-1$ of $\mathbf{Z}/M\mathbf{Z}$. Since i_0 and i_1 are units modulo M, they cannot be divisible by R. Therefore the only way all the multiples νi_0 and νi_1 with $0 \leq \nu \leq R-1$ can be $< R$ is if $i_0 = i_1 = 1$. But then $1/N \equiv i_0 - i_1 \equiv 0$ modulo M, which is impossible. Therefore 0 and (i) cannot lie in a common subcube, which proves that ${}_MA$ is irreducible. Furthermore, the proof that ${}_MA$ is irreducible depends only on the locations of the numbers $0, 1, \ldots, D-1$, where D is the largest divisor of M other than M itself. Therefore any permutation σ that fixes these numbers will map ${}_MA$ to an irreducible magic N-cube ${}_MA^\sigma$. Since M is relatively prime to $(2N-1)$, we have $D = M/p$, where p is the smallest prime dividing M and $p \geq (2N+1)$. Therefore, we have

$$ b_M \geq (M-D)! > \Gamma\left(\frac{2MN}{2N+1}\right) \geq \Gamma(4M/5) $$

which implies that the series $\sum_{n=3}^\infty b_n t^n$ diverges for $t \neq 0$.

We have a similar result for the monoids $\mathcal{S}_N(t, g)$, but unfortunately somewhat weaker: we can only prove that the Dirichlet series diverge.

Theorem (4.3): *Let $N > 1$ be an integer and let $g : [1, N] \to S$ be any function. For every positive integer n denote by c_n (resp. d_n) the number of magic N-cubes (resp. irreducible magic N-cubes) of order n belonging to the monoid $S_N(t, g)$. Then the Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s}, \sum_{n=1}^{\infty} \frac{d_n}{n^s}$$

diverge for every complex number s.

Proof: Let n run over all positive integers M such that t divides MN and such that $M > 1$ if t is even. If σ is a permutation on the integers $0, 1, \ldots, M-1$ and if x is an integer such that $0 \le x \le t^M - 1$, then we write $\sigma(x)$ to denote the integer obtained by permuting the digits of x in the base t according to the permutation σ. If $(i) = (i_1, \ldots, i_N)$ is an N-tuple of integers such that $0 \le i_\nu \le t^M - 1$ for $1 \le \nu \le N$ then we write $\sigma \cdot (i)$ to denote the N-tuple obtained from (i) by replacing i_N by $\sigma(i_N)$. Let $A = (a_{i_1,\ldots,i_N})$ be the magic N-cube of order t^M constructed by the method of Prouhet sequences (cf. [A-L],Theorem 1). As noted in the proof of Theorem 3.1, for all but at most finitely many M such that t divides MN, the magic N-cube lies in $\mathcal{S}_N(t, g)$. If σ is a permutation on $0, \ldots, M-1$ then we define the array $A^\sigma = (a^\sigma_{i_1,\ldots,i_N})$ by the rule

$$a^\sigma_{(i)} = a_{\sigma \cdot (i)}.$$

It is easy to see that for $1 \le k \le N$ the mapping $(i) \mapsto \sigma \cdot (i)$ maps k-subcubes to k-subcubes and preserves the relation of conjugacy of subcubes. It follows that A^σ also belongs to $\mathcal{S}_N(t, g)$. This shows that for $n = t^M$ with M sufficiently large and such that t divides MN, we have $c_n \ge M!$. Furthermore, since the proof of Lemma 3.3 shows that A^σ is also irreducible, we actually have $d_n \ge M!$. Therefore we have, letting M run over sufficiently large multiples of t,

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s} \ge \sum_{n=1}^{\infty} \frac{d_n}{n^s} \ge \sum \frac{M!}{t^{Ms}}$$

and the summation on the right diverges by the ratio test.

Since the problem of determining the numbers a_n, b_n, c_n, d_n, and others like them, or at least giving good estimates for them, is a matter of independent interest, we summarize in the following theorem the estimates we have obtained. Undoubtedly one can easily do much better.

Theorem (4.4): *We have the following inequalities.*
(i) $a_M \ge M!$ if M is relatively prime to $(2N-1)!$.
(ii) $b_M \ge (M-D)!$ if M is relatively prime to $(2N-1)!$, where D is the largest proper divisor of M;
(iii) $c_n \ge d_n \ge M!$ if $n = t^M$.

The estimates (i) and (ii) could be improved by studying the question of how many matrices one could have used instead of the matrix X we actually chose for the proof of Theorem 4.1. This would only improve the estimate by at most a factor which is polynomial in M. We haven't investigated this in any detail since we believe that the actual growth of b_M is much larger than any polynomial multiple of $M!$.

References

[A1] Allan Adler, "Magic Cubes and the 3-adic Zeta Function," Mathematical Intelligencer **14** (1992) 14-23
[A2] Allan Adler, "Magic N-cubes form a free monoid," preprint
[A-L] Allan Adler and S.-Y. Robert Li, "Magic N-Cubes and Prouhet Sequences," American Mathematical Monthly **84** (1977) 618-627
[A-W] Allan Adler and Lawrence C. Washington, "p-adic L-functions and p-dimensional magic cubes," J.Number Theory **52** (1995) 179-197
[An] W.S.Andrews, *Magic Squares and Cubes*, Dover, New York, 1960

[Ax1] James Ax, Private Conversation, 1974

[Ax2] James Ax, "Group-theoretic treatment of the axioms of quantum mechanics," Found. Phys. **6** (1976) 371-399

[E1] Leonhard Euler,"Recherches sur une nouvelle espece de quarres magiques," *Commentationes arithmeticae* **2** (1849) 302-361, *Opera Omnia*, Series I^a, Vol. VII, pp.290-392 Leipzig and Berlin, B.G.Teubner 1923 [#530 in Enestrom's list]

[E2] Leonhard Euler, "De carris magicis," *Commentationes arithmeticae* **2** (1849) 593-602, *Opera Postuma* **1** (1862) 140-151 [#795 in Enestrom's list]

[F] Pierre de Fermat, Letter to Mersenne, April 1, 1640,*Oeuvres de Fermat,* Vol.II,p.191

[Ge] I.M. Gelfand, Silliman Lectures, part III, Yale University, Nov.29, 1989

[Iw] Kenkichi Iwasawa, *Lectures on p-adic L-functions*, Princeton University Press and University of Tokyo Press, Princeton, NJ 1972

[K] Maurice Kraitchik, *Traité des Carrées Magiques*, Paris, Gauthier-Villars C$^{\text{ie}}$

[Me] Jerome S. Meyer, *Fun With Mathematics*, World Publishing Company, Cleveland and New York, 1952

[Mo1] Marston Morse, "Recurrent geodesics on a surface of negative curvature," Transactions of the American Mathematical Society **22** (1921) 84-100 [*Collected Papers*, vol. 2, pp.24-40]

[Mo2] Marston Morse, *Symbolic Dynamics*, Lectures by Marston Morse, 1937-1938 Notes by Rufus Oldenburger, edition with preface, 1966, Institute for Advanced Study, Princeton

[M-H 1] Marston Morse and G.A. Hedlund, "Symbolic Dynamics," American Journal of Mathematics **60** (1938) 815-866

[M-H 2] Marston Morse and G.A. Hedlund, "Unending Chess, Symbolic Dynamics and a Problem in Semigroups," Duke Math. Journal **11** (1933) 1-7

[R1] S. Ramanujan, *Notebooks of Srinivasa Ramanujan*, vol.II, Chapter 2, Facsimile Edition, Tata Institute, Bombay 1957

[R2] S. Ramanujan, *Ramanujan's Notebooks*, Part I, edited by Bruce C. Berndt Springer-Verlag, NY 1985

[S1] Richard Stanley, "Linear homogeneous Diophantine equations and magic labelings of graphs," Duke Math. J. **40** (1973) 607-632

[S2] Richard Stanley, "Magic labelings of graphs, symmetric magic squares, systems of parameters and Cohen-Macaulay rings," Duke Math. J. **43** (1976) 511-531

[W1] André Weil, Private Conversation, 1976

[W2] André Weil, "Sur les périodes des intégrales abéliennes," Comm. Pure and Applied Math. XXIX (1976) 813-819, *Collected Papers*, vol. 3, [1976b], pp.392-397