Magic Dice

Bernard D. Flury, Robert Irving, and M. N. Goria

1. INTRODUCTION. A magician offers her audience a betting game with two dice. With X and Y denoting the numbers shown by the first and the second die, respectively, the magician wins one ruble for 12 of the 36 possible outcomes (x, y), and loses 1 ruble for another set of 12 outcomes, as indicated in Table 1. No payment is made in the remaining cases. This seems to be a fair game, but in fact the two dice are not independent, as seen from their joint distribution displayed in Table 1. Soon enough the audience realizes that every time a ruble is paid it is in

TABLE 1. Joint Probabilities for six-sided magic dice.

Columns correspond to values of X; rows to values of Y. Entries are probabilities in multiples of $1/36$. The audience wins if $(X, Y) = (1,3), (1,5), (2,3), (2,5), (3,3), (3,6), (4,1), (4,4), (5,2), (5,4), (6,2)$, or $(6,4)$. The magician wins for 12 other (arbitrarily chosen) outcomes.

	1	2	3	4	5	6
6	1	2	0	1	1	1
5	0	0	2	1	2	1
4	3	1	2	0	0	0
3	0	0	0	2	1	3
2	1	2	1	2	0	0
1	1	1	1	0	2	1

the magician's favor. This happens despite the fact that two observers who tally the frequencies of X and Y, respectively, find that both dice show each side with exactly the required relative frequency of $1/6$.

Now as almost everybody knows, marginal probabilities do not determine joint probabilities, and therefore the audience asks for a third observer. The magician agrees and lets someone tally the frequencies with which $X + Y$ takes values 2, $3, \ldots, 12$. Sure enough, these are found to be $1/36$, $2/36$, etc, just as expected if X and Y were independent fair dice. Hence a fourth observer is admitted who tallies $X - Y$, and finally a fifth observer who tallies $X + 2Y$. When asked to admit a sixth observer, however, the magician stops the game.

As can be verified from Table 1, none of the five observers studying the distributions of X, Y, $X + Y$, $X - Y$, and $X + 2Y$ is able to detect that something is wrong with the pair of dice. Indeed, all five observers find exactly what they expect if X and Y are independent regular dice, and the deviations of the joint probabilities from their fair value $1/36$ remains undetected.

The obvious question is, how many different observers can the magician admit without giving away the secret? To make this question clear, we formulate the rules of the game more precisely. Each time the magician is asked to admit another observer, she chooses a linear combination $aX + bY$ (with real coefficients a and b) that is not proportional to any of the previously assigned linear combinations. She constructs her dice such that she can admit as many observers as possible, yet be able to offer unfair bets. The maximum number of observers

that can be admitted is called the *magic number*. We investigate magic numbers for k–sided dice, $k \geq 2$. For six–sided dice the magic number is 5, and Table 1 gives a particular example where five observers can be admitted. It is straightforward (but tedious) to verify in Table 1 that any further linear combination would indeed reveal that some joint probabilities are not $1/36$. Showing that it is impossible to construct an unfair pair of dice that would admit more than five observers is somewhat more laborious; Theorem 6 gives us a final answer.

2. DEFINITION OF MAGIC NUMBERS. For a fixed integer $k \geq 2$, let (X, Y) denote a bivariate random variable taking values in the set $\{1, 2, \ldots, k\} \times \{1, 2, \ldots, k\}$ with probabilities p_{ij}.

Definition 1. A linear combination $Z = aX + bY$ is *proper* if its distribution is unchanged by setting all $p_{ij} = 1/k^2$.

For any linear combination $Z = aX + bY$ we have

$$\Pr[Z = m] = \sum_{(i,j) \in \mathcal{J}_m(a,b)} p_{ij},$$

where

$$\mathcal{J}_m(a, b) = \{(i, j) \in \mathbb{N}^2 : 1 \leq i \leq k, 1 \leq j \leq k, ai + bj = m\}.$$

Hence $Z = aX + bY$ is proper exactly if, for all integers m,

$$k^2 \cdot \Pr[Z = m] = \#(\mathcal{J}_m(a, b)),$$

where $\#(\mathcal{J})$ is the number of elements in the set $\mathcal{J}$.

Two linear combinations Z_1 and Z_2 are considered identical if $Z_1 = cZ_2$ for some $c \in \mathbb{R}$. The trivial linear combination $0 \cdot X + 0 \cdot Y$ is always excluded.

Definition 2. For $k \in \mathbb{N}$, $k \geq 2$, let $m(k)$ denote the maximum number of different linear combinations such that the following condition holds: It is possible to find joint probabilities p_{ij}, where not all p_{ij} are equal to $1/k^2$, such that all $m(k)$ linear combinations are proper. The number $m(k)$ is called the *magic number* for k–sided dice.

For $k \leq 4$, $m(k)$ can be found by hand, but for larger k a more systematic approach is needed.

3. COMPUTATION OF MAGIC DICE, AND PRELIMINARY RESULTS. For $k \geq 2$ there are only finitely many linear combinations that map the points $(i, j) \in \{1, \ldots, k\} \times \{1, \ldots, k\}$ into fewer than k^2 different points on the real line (which, in turn, would determine all p_{ij}). For instance, for $k = 3$ the only linear combinations to be considered are X, Y, $X + Y$, $X - Y$, $X + 2Y$, $X - 2Y$, $2X + Y$, and $2X - Y$. Only linear combinations with integer coefficients need to be considered, and a linear combination $Z = aX + bY$ can therefore be represented as a pair of integers (a, b). For each $k \geq 2$ the set of linear combinations to be considered is as follows.

Definition 3. The set of feasible linear combinations, or *feasible set*, for k–sided dice is the set $\mathcal{F}_k$ of pairs of integers (a, b) such that

(i) $0 \leq a \leq k - 1$, $-(k - 1) \leq b \leq k - 1$.
(ii) $ab = 0$ implies $a = 1$ or $b = 1$.
(iii) If both a and b are nonzero, then a and b are relatively prime.

Consider the matrix $\mathbf{U} = [u_{ij}]$, where $u_{ij} = k^2 p_{ij}$. For a given $(a, b) \in \mathcal{F}_k$, the linear combination $aX + bY$ generates a number $N_k(a, b)$ of linear equations in the variables u_{ij}. For example, for $k = 3$ and $(a, b) = (1, 1)$, the five equations

$$\begin{aligned} u_{11} &= 1 \\ u_{12} + u_{21} &= 2 \\ u_{13} + u_{22} + u_{31} &= 3 \\ u_{23} + u_{32} &= 2 \\ u_{33} &= 1 \end{aligned}$$

are generated. In the $N_k(a, b)$ equations generated by $(a, b) \in \mathcal{F}_k$ each of the variables u_{ij} occurs exactly once, and the right-hand side of each equation is the number of variables on the left hand side. Using the vec-operator that stacks the columns of a matrix on top of each other, and writing $\mathbf{1}_n$ for the n-vector with 1 in each position, the equations generated by $(a, b) \in \mathcal{F}_k$ can be written as

$$\mathbf{C}(a, b)\text{vec}(\mathbf{U}') = \mathbf{C}(a, b)\mathbf{1}_{k^2}.$$

For $k = 3$ and $(a, b) = (1, 1)$, we obtain

$$\mathbf{C}(1,1) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The matrix $\mathbf{C}(a, b)$ is binary, of dimension $N_k(a, b) \times k^2$, and has full row rank. For a subset $\mathcal{S} = \{(a_1, b_1), \ldots, (a_p, b_p)\} \subset \mathcal{F}_k$, let

$$\mathbf{C}_{\mathcal{S}} = \begin{bmatrix} \mathbf{C}(a_1, b_1) \\ \vdots \\ \mathbf{C}(a_p, b_p) \end{bmatrix}.$$

We refer to

$$\mathbf{C}_{\mathcal{S}}\text{vec}(\mathbf{U}') = \mathbf{C}_{\mathcal{S}}\mathbf{1}_{k^2} \tag{1}$$

as the *system of equations generated by* $\mathcal{S}$. Defining $\mathbf{V} = \mathbf{U} - \mathbf{1}_k\mathbf{1}'_k$, we can write (1) as

$$\mathbf{C}_{\mathcal{S}}\text{vec}(\mathbf{V}') = \mathbf{0}. \tag{2}$$

For a given subset $\mathcal{S} \subset \mathcal{F}_k$ we have to solve (2). If $\text{rank}(\mathbf{C}_{\mathcal{S}}) = k^2$, then $\text{vec}(\mathbf{V}') = \mathbf{0}$ is the only solution, so $\mathbf{U} = \mathbf{1}_k\mathbf{1}'_k$, and $p_{ij} = 1/k^2$ for all (i, j). If $\text{rank}(\mathbf{C}_{\mathcal{S}}) < k^2$, then multiple solutions exist, and since $\text{vec}(\mathbf{V}') = \mathbf{0}$ is always a solution, we can then obtain another solution for which the p_{ij} are probabilities. The magic number $m(k)$ is the largest cardinality of all subsets $\mathcal{S} \subset \mathcal{F}_k$ such that $\text{rank}(\mathbf{C}_{\mathcal{S}}) < k^2$.

In preliminary calculations for k up to 24, Gaussian elimination was used to determine the rank of of $\mathbf{C}_{\mathcal{S}}$ exactly. In all cases considered, whenever $\mathcal{S}$ was a maximum cardinality subset it was possible to generate integer-valued solutions for $\mathbf{U}$, as in Table 1. (This is always possible, as we will see at the end of Section 5). The computational problem was huge for the larger values of k, and it was necessary to program the Gaussian elimination algorithm in integer arithmetic to retain full precision. Results obtained in this way are summarized in Table 2. Note that the choice of a new linear combination to be included is not always unique. For example, when going from $k = 5$ to $k = 6$, we have a choice of including one

TABLE 2. Magic Numbers and Related Quantities for k–sided dice, $2 \le k \le 24$.

$\mathscr{S}$ = largest subset of $\mathscr{T}_k$ such that rank$[\mathbf{C}_{\mathscr{S}}] < k^2$; $\mathbf{C}_{\mathscr{S}}$ = coefficient matrix generated by $\mathscr{S}$; $m(k)$ = magic number for k–sided dice. In the column labelled $\mathscr{S}$, each row shows only the linear combination introduced in addition to the ones already present in the preceding rows. *Note*: Magic dice for $k = 23$ and $k = 24$ can also be constructed using the linear combinations $(1, 4)$ and $(4, 1)$ instead of $(2, 3)$ and $(3, 2)$.

k	$\mathscr{S}$	rows($\mathbf{C}_{\mathscr{S}}$)	rank($\mathbf{C}_{\mathscr{S}}$)	$m(k)$
2	(1, 0) (0, 1)	4	3	2
3	(1, 1)	11	8	3
4	(1, −1)	22	15	4
5		28	21	4
6	(1, 2)	50	34	5
7	(2, 1)	78	48	6
8		90	60	6
9	(1, −2)	127	79	7
10	(2, −1)	170	99	8
11		188	117	8
12		206	135	8
13	(1, 3)	273	166	9
14	(3, 1)	348	195	10
15		374	221	10
16		400	247	10
17	(1, −3)	491	286	11
18	(3, −1)	590	323	12
19		624	357	12
20		658	391	12
21	(2, 3)	791	439	13
22		830	478	13
23	(3, 2)	978	528	14
24		1022	572	14

of the four linear combinations $(1, 2)$, $(2, 1)$, $(1, -2)$, and $(2, -1)$. For all values of k up to 24 it was possible to find k–sided magic dice with a set of linear combinations that contains the set of linear combinations used for $k - 1$ as a subset. We return to this point in Section 4. Table 3 shows joint probabilities for an example of 14–sided magic dice, admitting ten proper linear combinations.

TABLE 3. Joint Probabilities for 14–sided magic dice.

Columns correspond to values of X; rows to values of Y. Entries are probabilities in multiples of $1/196$. The set $\mathscr{S}$ of proper linear combinations has elements $(1, 0)$, $(0, 1)$, $(1, 1)$, $(1, -1)$, $(1, 2)$, $(2, 1)$, $(1, -2)$, $(2, -1)$, $(1, 3)$, and $(3, 1)$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
14	1	1	1	1	2	0	1	1	1	1	1	1	1	1
13	1	1	0	1	1	1	1	1	2	1	1	1	1	1
12	1	2	1	1	2	1	1	1	0	1	0	1	1	1
11	1	1	1	1	0	0	2	0	2	1	1	2	1	1
10	0	1	0	2	1	1	1	2	1	1	1	1	1	1
9	2	1	1	2	1	1	1	0	1	1	0	2	0	1
8	1	1	1	0	1	1	1	1	2	0	2	1	1	1
7	1	1	1	2	0	2	1	1	1	1	0	1	1	1
6	1	0	2	0	1	1	0	1	1	1	2	1	1	2
5	1	1	1	1	1	1	2	1	1	1	2	0	1	0
4	1	1	2	1	1	2	0	2	0	0	1	1	1	1
3	1	1	1	0	1	0	1	1	1	2	1	1	2	1
2	1	1	1	1	1	2	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1	0	2	1	1	1	1

Our first Lemma proves two intuitively reasonable aspects of magic numbers.

Lemma 1. *For the magic numbers $m(k)$ the following holds*:

(i) $m(k+1) \geq m(k)$.
(ii) $\lim_{k\to\infty} m(k) = \infty$.

Proof: Part (i) follows by taking a matrix $\mathbf{U}$ of dimension $k \times k$ that generates k–sided magic dice, and appending a column of 1's and a row of 1's. For part (ii), we prove a stronger result that implies (ii), namely: for any set of linear combinations $\mathcal{S} = \{(a_1, b_1), \ldots, (a_p, b_p)\}$ with integer coefficients there exists a $k \in \mathbb{N}$ such that $\text{rank}[\mathbf{C}_{\mathcal{S}}] < k^2$. For any two positive integers a and b, the linear combination $aX + bY$ applied to k–sided dice can take integer values from $a + b$ to $k(a + b)$. Thus such a linear combination generates at most $(k-1)(a+b)+1$ equations. Similarly for arbitrary integers a and b, at most $(k-1)(|a| + |b|) + 1$ equations are generated. Let $N_i = |a_i| + |b_i|$ $(i = 1, \ldots, p)$, and $N = \sum_{i=1}^{p} N_i$. Then, for k–sided dice, the set $\mathcal{S}$ generates at most

$$\sum_{i=1}^{p} [(k-1)N_i + 1] = (k-1)N + p$$

equations. Choosing k such that $k^2 > (k-1)N + p$ gives a coefficient matrix with k^2 columns and fewer than k^2 rows, which cannot have full column rank. ■

4. FINDING MAGIC NUMBERS. We now describe a simple way to compute magic numbers. Throughout this section we refer to the first and k–th rows and columns of the matrix $\mathbf{U}$ as the *margins* of $\mathbf{U}$.

Lemma 2. *For fixed k and for any $\mathcal{S} \subset \mathcal{F}_k$ the following two conditions are equivalent*:

(*a*) *rank*$(\mathbf{C}_{\mathcal{S}}) = k^2$.
(*b*) *At least one of the margins is uniquely determined.*

Proof: Clearly (a) implies (b). To show the reverse, let $\mathbf{u}_j$ be the j–th column of $\mathbf{U}$, and suppose (b) holds for the first column. Define a $k \times k$ matrix $\mathbf{U}_{-1} = (\mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{1}_k)$, and notice that $\mathcal{S}$ generates the system of equations

$$\mathbf{C}_{\mathcal{S}}\text{vec}(\mathbf{U}'_{-1}) = \mathbf{C}_{\mathcal{S}}\mathbf{1}_{k^2}. \tag{3}$$

To see why this is true, represent the k^2 variables as grid points with coordinates $(i, j), 1 \leq i, j \leq k$, in the plane. (This is similar to the approach to be used later in the proof of Lemma 3). Each of the equations generated by $\mathcal{S}$ may be represented by a straight line that hits one or several points that correspond to variables. Formally, we may associate grid points outside the square with variables whose value is set to be 1. Then (1) holds as well if we shift the square by one unit to the right, which implies (3). By assumption, the first column vector of $\mathbf{U}_{-1}$ must be $\mathbf{1}_k$. By induction all columns of $\mathbf{U}$ must be equal to $\mathbf{1}_k$. ■

Lemma 2 shows that it is important to understand the conditions under which the margins are determined. In fact, as soon as at least one linear combination (a, b) with $ab \neq 0$ enters the equation system, some entries in the corners of $\mathbf{U}$ are determined (must take the value 1). In the next lemma, which is central to the theory, we describe the way in which the corners of $\mathbf{U}$ "fill up" as the number of linear combinations increases.

Lemma 3. *Let* $\mathscr{S}^+$ *be a set of* $r \geq 1$ *linear combinations* (a_h, b_h) *such that both* $a_h \geq 1$ *and* $b_h \geq 1$. *Let* $a^+ = \sum_{h=1}^{r} a_h$ *and* $b^+ = \sum_{h=1}^{r} b_h$. *If* **U** *solves the system of equations* (1) *generated by* $\mathscr{S}^+$, *then*

(i) $u_{1j} = 1$ *for* $j = 1, \ldots, a^+$, *and* $u_{i1} = 1$ *for* $i = 1, \ldots, b^+$.
(ii) *If* r *is even, then* $u_{1,\,a^+ + 1} = u_{b^+ + 1,\,1}$. *If* r *is odd, then* $u_{1,\,a^+ + 1} + u_{b^+ + 1,\,1} = 2$.
(iii) *The* u_{1j} *for* $j > a^+$, *and the* u_{i1} *for* $i > b^+$, *are not determined.*

Proof: Let $\mathscr{S}^+ = \{(a_1, b_1), \ldots, (a_r, b_r)\}$. In the real plane, consider the grid given by all points with positive integer coefficients, and identify the grid point (i, j) with the corresponding variable u_{ij}. For the current purposes we may think of the number of grid points as unlimited. The linear combinations in $\mathscr{S}^+$ determine 1 to be the value of some of the variables associated with grid points near the origin. Let $m_h = a_h / b_h$ for $h = 1, \ldots, k$, and assume without loss of generality that $m_1 > m_2 > \cdots > m_r$. For $h = 0, \ldots, r$, let

$$\alpha_h = \sum_{i=h+1}^{r} a_i \quad \text{and} \quad \beta_h = \sum_{i=1}^{r} b_i,$$

define $r + 1$ points

$$P_h = (\beta_h + 1, \alpha_h + 1), \quad h = 0, \ldots, r,$$

and call them the *characteristic points* of $\mathscr{S}^+$. In particular, we have $P_0 = (1, a^+ + 1)$ and $P_r = (b^+ + 1, 1)$. Conversely, let $P_h = (x_h, y_h)$, $h = 0, \ldots, r$, denote $r + 1$ grid points in $\mathbb{N}^2$ such that $x_0 = 1$, $y_r = 1$, and the sequence $m_h = (y_{h-1} - y_h)/(x_h - x_{h-1})$ is monotonically decreasing. Then the P_h determine an associated set $\mathscr{S}^+$ with elements (a_1, b_1) to (a_r, b_r) uniquely by $P_h - P_{h-1} = (-b_h, a_h)$. Thus there is a one-to-one relationship between sets $\mathscr{S}^+$ and their characteristic points.

For a set $\mathscr{S}^+$ with characteristic points $P_0, \ldots, P_r$ let l_h be the line segment connecting points P_{h-1} and P_h, and denote by $\mathscr{L}$ the polygon obtained by joining the r line segments. We now show that all variables associated with grid points inside the area bounded by $\mathscr{L}$ and the coordinate axes are determined ($= 1$) by the equations generated by $\mathscr{S}^+$. This implies part (i) of Lemma 3. See Figure 1 for a graphical illustration.

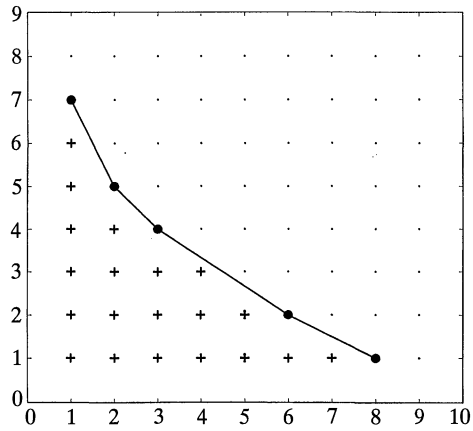

Figure 1. Illustration of the Proof of Lemma 3. Grid points whose associated variables are determined by the linear combinations in the set $\mathscr{S}^+ = \{(2, 1), (1, 1), (2, 3), (1, 2)\}$ are marked by plus-signs. The characteristic points of $\mathscr{S}^+$ are shown as large dots, and connected by the polygon $\mathscr{L}$.

We show first that the above statement implies part (ii) of Lemma 3. Denote the variables associated with the characteristic points $P_0, \ldots, P_r$ by $\xi_0, \ldots, \xi_r$. The line segment l_h corresponds to an equation $\xi_{h-1} + \xi_h = 2$ because all other grid points in $\mathbb{N}^2$ hit by the line of which l_h is a segment are determined. Thus we have an equation system

$$\begin{aligned} \xi_0 + \xi_1 &= 2 \\ \xi_1 + \xi_2 &= 2 \\ &\vdots \\ \xi_{r-1} + \xi_r &= 2 \end{aligned}$$

Successive elimination of intermediate variables gives $\xi_0 + \xi_r = 2$ if r is odd, and $\xi_0 = \xi_r$ if r is even. This proves part (ii) of Lemma 3. Note also that if we set *any* of the ξ_h equal to 1, then by the above equation system all other ξ_h are automatically 1 as well.

We now prove that all variables in the area below $\mathscr{L}$ are determined. For each real s with $1 \le s \le a^+ + 1$ let $\mathscr{L}(s)$ be the polygon obtained by translating $\mathscr{L}$ down to start at $(1, s)$ instead of at $(1, a^+ + 1)$. Let $1 = s_1 < \cdots < s_m = a^+ + 1$ be the sequence of distinct values of s such that $\mathscr{L}(s)$ passes through a grid point in the area bounded by $\mathscr{L}$ and the axes. Then, by induction on i for $i = 1$ to $i = m$, all variables are determined in the interior of the area bounded by $\mathscr{L}(s_i)$ and the axes. In passing from i to $i + 1$ it has to be shown that each grid point P on $\mathscr{L}(s_i)$ is determined. If P is the only grid point on a segment of $\mathscr{L}(s_i)$, this is obvious. If P and Q are two grid points on the same segment of $\mathscr{L}(s_i)$, they must be at the ends of the segment, s_i must be an integer, and there is a chain of grid points along $\mathscr{L}(s_i)$, one at each corner. The lowest of this chain of grid points is determined, hence so are all the others by working along the chain.

To prove part (iii), we proceed by induction on r. Assume that (iii) hold true for some $r \ge 1$, and notice that no variable associated with a grid point (i, j), where $j > a^+$, is determined. Adding a new linear combination (a_{r+1}, b_{r+1}) to the previous set $\mathscr{S}^+$ of r linear combinations, we get a new set $\mathscr{S}^+_{r+1} = \mathscr{S}^+ \cup \{(a_{r+1}, b_{r+1})\}$, whose initial characteristic point is $(1, a^+ + a_{r+1} + 1)$. The only way the variable associated with this characteristic point could be determined is that the variable associated with the point $(b_{r+1} + 1, a^+ + 1)$ is determined, which is not the case. Similarly, the variable associated with the final characteristic point of $\mathscr{S}^+_{r+1}$ is not determined. ■

By Lemma 3, the system of equations generated by $\mathscr{S}^+$ imposes exactly $a^+ + b^+$ linearly independent constraints on the variables associated with points on the left and bottom margins: the first a^+ points are determined vertically, the first b^+ points in the margin are determined horizontally, which means that $a^+ + b^+ - 1$ points are determined around the corner, plus the additional constraint of part (ii). For fixed k, consider similarly the three remaining corners of the matrix **U**. Exactly the same result as Lemma 3 is established for the corner with coordinates (k, k). For the two remaining corners, consider a set $\mathscr{S}^-$ of linear combinations (a_h, b_h) where $a_h > 0$ and $b_h < 0$, and put $a^- = \Sigma a_h$, $b^- = \Sigma |b_h|$, both sums extending over all $(a_h, b_h) \in \mathscr{S}^-$. The same arguments as in Lemma 3 show that the first a^- points are determined vertically, and the first b^- points are determined horizontally. Finally, let $\mathscr{S}^0$ be a set of linear combinations where

either $a_h = 0$ or $b_h = 0$; there are at most two elements in $\mathscr{S}^0$, each imposing a constraint on the rows and columns, respectively. Put $a^0 = \Sigma a_h$ and $b^0 = \Sigma b_h$, both sums extending over all elements in $\mathscr{S}^0$. Both a^0 and b^0 can only take values 0 and 1.

Finally, for a given set $\mathscr{S} \subset \mathscr{F}_k$, we can write $\mathscr{S}$ as the union of three disjoint sets $\mathscr{S}^0$, $\mathscr{S}^+$, and $\mathscr{S}^-$, as above. Let

$$a^* = a^0 + a^+ + a^- = \sum_{(a_h, b_h) \in \mathscr{S}} a_h$$

and

$$b^* = b^0 + b^+ + b^- = \sum_{(a_h, b_h) \in \mathscr{S}} |b_h|.$$

By the previous considerations, exactly a^* constraints exist on the first column of $\mathbf{U}$, and b^* constraints on the first row of $\mathbf{U}$. By Lemma 2, all variables in $\mathbf{U}$ are determined exactly if $a^* \geq k$ or $b^* \geq k$. If $\max\{a^*, b^*\} < k$, then $\mathbf{U}$ is not completely determined. Thus we have the following main result.

Theorem 4. *The magic number $m(k)$ is the number of elements in a largest set $\mathscr{S} \subset \mathscr{F}_k$ such that*

$$\sum_{(a_h, b_h) \in \mathscr{S}} a_h < k \quad \text{and} \quad \sum_{(a_h, b_h) \in \mathscr{S}} |b_h| < k. \qquad \blacksquare$$

For example, the set $\mathscr{S}$ consisting of linear combinations $(1, 0)$, $(0, 1)$, $(1, \pm 1)$, $(1, \pm 2)$, $(2, \pm 1)$, $(1, \pm 3)$, $(3, \pm 1)$, $(2, \pm 3)$, $(3, \pm 2)$, $(1, \pm 4)$, $(4, \pm 1)$, and $(3, 4)$, has 21 elements, with $\Sigma a_h = 40$, $\Sigma |b_h| = 41$. This is a largest set such that $\max\{\Sigma a_h, \Sigma |b_h|\} < 42$, and therefore $m(42) = 21$. The set is not unique because the linear combination $(3, 4)$ may be replaced by any of $(3, -4)$, $(4, 3)$, or $(4, -3)$. Let $\mathscr{S}^*$ be the set obtained by taking $(3, 4)$ out of $\mathscr{S}$ and adding the two linear combinations $(1, 5)$ and $(5, 1)$; then $\mathscr{S}^*$ has 22 elements, with $\Sigma a_h = \Sigma |b_h| = 43$. This is a largest set such that $\max\{\Sigma a_h, \Sigma |b_h|\} < 44$, and therefore $m(44) = 22$. This shows that the linear combinations contained in magic k-sided dice are not necessarily all contained in magic $(k + 1)$-sided dice. See the discussion following the proof of Theorem 6.

We now show how the magic number $m(k)$ can be expressed in terms of the classical Euler totient (or phi) function. For a positive integer n, $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. For convenience, we define $\phi(1)$ to be 1. Also define

$$\Phi(n) = \sum_{i=1}^{n} \phi(i),$$

and

$$\Psi(n) = \sum_{i=1} i\phi(i),$$

and put $\mathscr{F} = \bigcup_{k \geq 2} \mathscr{F}_k$, where $\mathscr{F}_k$ is the feasible set for k–sided dice. For a subset $\mathscr{S}$ of $\mathscr{F}$, let $\sigma_{\mathscr{S}} = \max(\Sigma a, \Sigma |b|)$, where the sums are taken over all pairs $(a, b) \in \mathscr{S}$, and call $\mathscr{S}$ *k–bounded* if $\sigma_{\mathscr{S}} < k$. It is convenient to view $\mathscr{F}$ as an ordered

sequence of pairs in which (a, b) precedes (p, q) if

(i) $a + |b| < p + |q|$, or
(ii) $a + |b| = p + |q|$ and $|b| - a| > ||q| - p|$.

Further, if $0 < a < b < k$, with a and b relatively prime, then the pairs $(a, -b)$, $(b, -a)$, (a, b), and (b, a) appear in that order in the sequence. The first few pairs in $\mathcal{F}$, represented as an ordered sequence, are $(0,1)$, $(1,0)$, $(1,-1)$, $(1,1)$, $(1,-2)$, $(2,-1)$, $(1,2)$, $(2,1)$, $(1,-3)$, $(3,-1)$, $(1,3)$, $(3,1)$, $(1,-4)$, $(4,-1)$, $(1,4)$, $(4,1)$, $(2,-3)$, $(3,-2)$, $(2,3)$, $(3,2)$, $(1,-5)$, $(5,-1)$, ...

For $r > 0$, define

$$\sigma_{2r} = \sum a = \sum |b|,$$

where the sums are taken over the first $2r$ pairs in the ordered sequence $\mathcal{F}$. Note that $\sigma_{2r} = \sigma_{\mathcal{S}}$ when $\mathcal{S}$ is the set of the first $2r$ elements in the ordered sequence.

Verification of the following lemma is straightforward.

Lemma 5. *If* $\Phi(n) \le r < \Phi(n+1)$, *then*

(i) $\sigma_{2r} = \Psi(n) + [r - \Phi(n)](n+1)$.
(ii) *Any* $2r$*-subset* $\mathcal{S}$ *of* $\mathcal{F}$ *must have* $\sigma_{\mathcal{S}} \ge \sigma_{2r}$, *and, for* $r > 1$, *any* $(2r+1)$*-subset* $\mathcal{S}$ *of* $\mathcal{F}$ *must have* $\sigma_{\mathcal{S}} \ge \sigma_{2r} + \lfloor (n+3)/2 \rfloor$. ■

Trivially, $m(2) = 2$ and $m(3) = 3$. For $k > 3$, Lemma 5 enables us to establish the value of $m(k)$.

Theorem 6. *For* $k > 3$, *suppose* $\Psi(n) < k \le \Psi(n+1)$, *and let* $p = k - \Psi(n) - 1$.

(i) *If* $p \bmod (n+1) < \lfloor (n+3)/2 \rfloor$, *then*

$$m(k) = 2\Phi(n) + 2\lfloor p/(n+1) \rfloor,$$

and a maximum cardinality k*-bounded subset of* $\mathcal{F}$ *can be obtained by taking the first* $m(k)$ *pairs in the ordered sequence.*

(ii) *If* $p \bmod (n+1) \ge \lfloor (n+3)/2 \rfloor$, *then*

$$m(k) = 2\Phi(n) + 2\lfloor p/(n+1) \rfloor + 1,$$

and a maximum cardinality k*-bounded subset of* $\mathcal{F}$ *can be obtained by taking the first* $m(k) - 1$ *pairs in the ordered sequence together with the pair* $(\lfloor (n+3)/2 \rfloor, \lfloor (n+1)/2 \rfloor)$.

Proof: (i) If $r = \Phi(n) + \lfloor p/(n+1) \rfloor$, then by Lemma 5(i),

$$\sigma_{2r} = \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor \le \Psi(n) + p = k - 1,$$

so we have a k-bounded set of the claimed size. On the other hand, by Lemma 5(ii), any subset $\mathcal{S}$ of $\mathcal{F}$ of size $\ge 2r+1$ has

$$\begin{aligned} \sigma_{\mathcal{S}} &\ge \sigma_{2r} + \lfloor (n+3)/2 \rfloor \\ &= \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + \lfloor (n+3)/2 \rfloor \\ &> \Psi(n) + p - \lfloor (n+3)/2 \rfloor + \lfloor (n+3)/2 \rfloor \\ &= k - 1, \end{aligned}$$

and so it cannot be k-bounded.

(ii) If $r = \Phi(n) + \lfloor p/(n+1) \rfloor$, then, if $\mathscr{S}$ is the set described, Lemma 5(i) gives

$$\begin{aligned}\sigma_{\mathscr{S}} &= \sigma_{2r} + \lfloor (n+3)/2 \rfloor \\ &= \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + \lfloor (n+3)/2 \rfloor \\ &\le \Psi(n) + p - \lfloor (n+3)/2 \rfloor + \lfloor (n+3)/2 \rfloor \\ &= k - 1,\end{aligned}$$

so again we have a k–bounded set of the claimed size. On the other hand, it is easy to verify that

$$\sigma_{2r+2} \ge \sigma_{2r} + n + 1,$$

so that, by Lemma 5(ii), any subset $\mathscr{S}$ of $\mathscr{F}$ of size $\ge 2r+2$ has

$$\begin{aligned}\sigma_{\mathscr{S}} &\ge \sigma_{2r+2} \\ &\ge \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + n + 1 \\ &\ge \Psi(n) + p - (p \bmod (n+1)) + n + 1 \\ &> k - 1,\end{aligned}$$

and so cannot be k–bounded. ∎

As seen from Theorem 6, a set of k–sided magic dice can not always be constructed such as to contain the same linear combinations as magic $(k-1)$–sided dice. Theorem 6 allows us also to establish the asymptotic behavior of the function $m(k)$, based on the growth rate of the function Φ. First we need another preliminary lemma.

Lemma 7. *For the functions* $\Phi(n)$ *and* $\Psi(n)$, *the following holds*:

(i) $\Phi(n) = 3n^2/\pi^2 + O(n\log n)$.
(ii) $\Psi(n) = 2n^3/\pi^2 + O(n^2\log n)$.

Proof: For part (i), see [**3**, pp. 448–449]. For part (ii), by summation of parts, $\Psi(n) = n\Phi(n) - \sum_{i=1}^{n-1} \Phi(i)$. Thus

$$\Psi(n) = \frac{3}{\pi^2}n^3 + O(n^2\log n) - \frac{3}{\pi^2}\sum_{i=1}^{n-1}\left[i^2 + O(i\log i)\right],$$

and the result follows. ∎

Theorem 8. *The asymptotic behavior of* $m(k)$ *is*

$$m(k) = ck^{2/3} + O\left(k^{1/3}\log k\right), \quad \text{where } c = 6/(2\pi)^{2/3} \approx 1.7621.$$

Proof: Given k, choose n such that

$$\Psi(n) < k \le \Psi(n+1),$$

and hence

$$2\Phi(n) = m(\Psi(n)+1) \le m(k) < m(\Psi(n+1)+1) = 2\Phi(n+1).$$

From Lemma 7(ii) we have

$$k = \frac{2}{\pi^2}n^3 + O\left(n^2\log n\right),$$

and from Lemma 7(i),

$$m(k) = \frac{6}{\pi^2}n^2 + O(n\log n).$$

It follows that

$$n = (\pi^2/2)^{1/3}k^{1/3} + O(\log n)$$

and so

$$m(k) = \frac{6}{\pi^2}\left[(\pi^2/2)^{1/3}k^{1/3} + O(\log n)\right]^2 + O(n\log n).$$

Using $n = O(k^{1/3})$ leads to the stated result. ■

Figure 2 shows a graph of exact values of $m(k)$ along with the approximation $\hat{m}(k) = 6k^{2/3}/(2\pi)^{2/3}$, for $2 \le k \le 100$. As can be seen from the graph, the approximation is excellent.

Before you ask, the magic number for 1998–sided dice is 280.

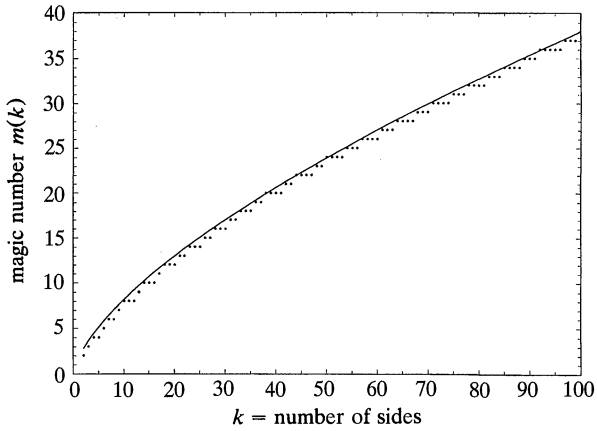

Figure 2. Exact values of the magic function $m(k)$ (dots) and approximation $\hat{m}(k) = 6k^{2/3}/(2\pi)^{2/3}$ (solid line).

5. THE RANK OF THE COEFFICIENT MATRIX. The theory of Section 4 allows us to find the magic number $m(k)$ as well as an associated set $\mathcal{S} \subset \mathcal{F}$ without solving the equation system of Section 3. For generating actual magic dice we still have to solve the equation system. As a byproduct of the Gauss–Jordan algorithm we obtain the rank of the coefficient matrix $\mathbf{C}_{\mathcal{S}}$. In the current section we give a simplified method for computing the rank of $\mathbf{C}_{\mathcal{S}}$ that does not require solving the equation system.

The idea is to study how the rank increases for a given set $\mathcal{S}$ of linear combinations if we go from $(k-1)$–sided dice to k–sided dice. Let $\mathbf{U}$ be the $(k-1) \times (k-1)$ matrix of variables for $(k-1)$–sided dice, and write $\mathbf{A}$ (instead of $\mathbf{C}_{\mathcal{S}}$ as before) for the coefficient matrix generated by the linear combinations in $\mathcal{S}$. Going from $k-1$ to k, we add a row and a column to the matrix $\mathbf{U}$, thus introducing $2k-1$ new variables to get a new matrix $\mathbf{U}^*$ of dimension $k \times k$. Instead of writing the equation system for k–sided dice in terms of vec($\mathbf{U}^{*\prime}$) as before, consider the variables contained in $\mathbf{U}$ as the $(k-1)^2$ first ones, and the

$2k - 1$ new variables as the last ones. The coefficient matrix for k–sided dice can then be written in partitioned form as

$$\mathbf{A}^* = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix}.$$

If $\mathbf{A}$ has s rows, then $\mathbf{B}$ has dimension $s \times (2k - 1)$. That is, the entries of $\mathbf{B}$ are coefficients of the newly introduced variables, but only for equations that involve entries from $\mathbf{U}$. The matrix $\mathbf{C}$ contains the coefficients of all equations that involve only newly introduced variables; it has $2k - 1$ columns and $\Sigma(a_h + |b_h|)$ rows. We will now show how $r(k - 1; \mathscr{S}) = \text{rank}(\mathbf{A})$ and $r(k; \mathscr{S}) = \text{rank}(\mathbf{A}^*)$ are related.

Perform Gauss–Jordan type row operations on the matrix $\mathbf{A}^*$, based on the first $(k - 1)^2$ columns, until as many rows as possible have zeros in the first $(k - 1)^2$ entries. That is, transform $\mathbf{A}^*$ into

$$\begin{bmatrix} \mathbf{A}_1 & \mathbf{B}_1 \\ \mathbf{O} & \mathbf{B}_2 \\ \mathbf{O} & \mathbf{C} \end{bmatrix},$$

where $\mathbf{A}_1$ has full row rank $r(k - 1; \mathscr{S})$. Because $\mathbf{A}_1$ has full row rank, we get

$$\text{rank}(\mathbf{A}^*) = \text{rank}(\mathbf{A}_1) + \text{rank}\begin{bmatrix} \mathbf{B}_2 \\ \mathbf{C} \end{bmatrix}.$$

Thus the rank of the coefficient matrix increases by $\delta = \text{rank}\begin{bmatrix} \mathbf{B}_2 \\ \mathbf{C} \end{bmatrix}$ when going from $(k - 1)$–sided dice to k–sided dice. But δ is the number of linearly independent constraints imposed on the newly introduced variables, i.e., the number of constraints imposed by $\mathscr{S}$ on the variables in the first row and first column, say, of the matrix $\mathbf{U}^*$.

In the notation and terminology of Section 4, consider the lower left corner of a $k \times k$ grid, and assume $\max\{\Sigma a_h, \Sigma|b_h|\} < k$, where both sums extend over all elements in $\mathscr{S}$. By Lemma 3, the variables associated with $a^+ + b^+ - 1$ grid points around the corner $(1, 1)$ are determined. In addition, there is a linear constraint between one of the variables in the first column and one of the variables in the first row, making the total number of constraints due to $\mathscr{S}^+$ equal to $a^+ + b^+$. The linear combinations in $\mathscr{S}^-$ determine another a^- variables vertically and b^- variables horizontally, and the linear combinations in $\mathscr{S}^0$ add a^0 and b^0 constraints vertically and horizontally, respectively. Thus the total number of constraints is $\Sigma(a_h + |b_h|)$, where the sum extends over all elements in $\mathscr{S}$. The rank increase is therefore $\delta = \Sigma(a_h + |b_h|)$, independent of k, as long as k is large enough.

If either $\Sigma a_h \geq k$ or $\Sigma|b_h| \geq k$, then Lemma 2 ensures that $\text{rank}(\mathbf{A}) = (k - 1)^2$ and $\text{rank}(\mathbf{A}^*) = k^2$; that is, the rank increase is $\delta = 2k - 1$. Finally, notice that for $k = 1$ the rank of the coefficient matrix is always 1, regardless of how many linear combinations are in $\mathscr{S}$.

This is summarized in the following theorem.

Theorem 9. *Let $r(k; \mathscr{S})$ denote the rank of the coefficient matrix of the equation system generated by the linear combinations (a_h, b_h) in the set $\mathscr{S}$, for k–sided dice. Then, for $k \geq 2$,*

$$r(k; \mathscr{S}) = \begin{cases} r(k - 1; \mathscr{S}) + \Sigma(a_h + |b_h|) & \text{if } \max\{\Sigma a_h, \Sigma|b_h|\} < k, \\ k^2 & \text{otherwise.} \end{cases}$$

■

For a given set $\mathcal{S}$ of linear combinations, Theorem 9 provides a simple recursion to compute the rank of the coefficient matrix. In particular, if $\mathcal{S}$ is a largest set of proper linear combinations, then $r(k; \mathcal{S}) = (k-1)^2 + \Sigma(a_h + |b_h|)$, and the number of free variables in the equations system is $2k - \Sigma(a_h + |b_h|) - 1$. For instance, in Section 4 we gave a set $\mathcal{S}$ of linear combinations for 42–sided magic dice and found $m(42) = 21$. Theorem 9 gives $r(42; \mathcal{S}) = 1762 = 42^2 - 2$. For all sets of 1998–sided magic dice, the rank is $3992003 = 1998^2 - 1$.

Finally, we return to a question raised in Section 3: Is it always possible to find an integer–valued solution to the system of equations generated by $\mathcal{S}$? The answer is yes, by the following argument. If the coefficient matrix has rank r, then the values of $f = k^2 - r$ variables can be chosen. Identify a free variable associated with a characteristic point. Set the remaining (if any) $f - 1$ free variables equal to 1, and assign the value 0 or 2 to the chosen free variable. Then, working along chains like the polygon in Figure 1, variables are assigned values of 2 and 0 in an alternating pattern.

6. EPILOGUE. "Magic Dice" originated in the first author's attempts to teach undergraduate students that marginal distributions do not determine joint distributions. It is natural to ask how much more information needs to be given (in addition to the marginal distributions) such that a joint distribution is completely determined. Although the story about the magician is flawed (in the sense that it appears physically impossible to construct such dice), students can relate to it and find it entertaining. In fact, it would take a TRUE magician to make the numbers shown by two dice depend on each other! This distinguishes our magic dice (or "pseudo dice," as suggested by a reviewer), from tricks with dice as described in [2]. The term "magic" may also be justified by the similarities with magic squares [6].

The idea of defining a joint distribution of two or several random variables by conditions imposed on linear combinations of the variables is not new; for example, a common definition of the multivariate normal distribution states that $\mathbf{X}$ is multivariate normal if every linear combination of $\mathbf{X}$ is univariate normal or constant. Melnick and Tenenbein give a nice example to illustrate that for any finite k, normality of k linear combinations does not imply multivariate normality [4]. For the discrete case, Rényi shows that a distribution of n strictly positive masses located at n distinct points in the plane, where both the sizes and locations of the masses are unknown, is determined by any $n + 1$ distinct projections, but not necessarily by n distinct projections [5]. Bélisle et al. study related questions for non–discrete probability distributions [1].

Finally, it is not difficult to see that the same results hold as well for arbitrary distributions on a $k \times k$ grid, as long all k^2 probabilities are strictly positive. Up to Theorem 4, results also generalize easily to the situation of distributions on a rectangular grid of size $k_1 \times k_2$. It is natural to ask related questions in higher dimension, but to our knowledge no results have appeared in the literature.

REFERENCES

1. Bélisle, C., Massé, J.–C., and Ransford, T., When is a probability measure determined by infinitely many projections? *Ann. Prob.* **25** (1997) 767–786.
2. Gardner, M., *Mathematics, Magic and Mystery*, Dover, New York, 1956.
3. Graham, R. L., Knuth, D. E., and Patashnik, O., *Concrete Mathematics*, Addison–Wesley, 1989.

4. Melnick, E. L., and Tenenbein, A., Misspecifications of the normal distribution. *Amer. Statist.* **36** (1982) 372–373.
5. Rényi, A., On projections of probability distributions. *Acta Math. Hungar.* **3** (1952) 131–142.
6. Ward, J. E., Vector spaces of magic squares. *Math. Mag.* **53** (1980), 108–111.

BERNARD D. FLURY studied statistics and mathematics at the University of Berne, Switzerland. After a random walk around the world he became Professor of Statistics in the Department of Mathematics, Indiana University. His research focuses on theoretical, practical, and computational aspects of multivariate statistics, mostly related to problems in classification and principal component analysis. Other research interests include beer and frequent trips to Italy.
Indiana University, Bloomington, IN 47405
flury@indiana.edu

ROBERT IRVING completed his BSc and PhD degrees in mathematics at the University of Glasgow in Scotland. After periods as a communications specialist and as a lecturer in mathematics and computer science at Salford University in Manchester, he returned to the Computing Science Department at Glasgow where he is now a Senior Lecturer. His research interests are in the areas of algorithms and complexity theory, including combinatorial optimization, graph theory, and "stringology."
Computing Science Department, University of Glasgow, Glasgow G12 8QQ, Scotland
rwi@dcs.gla.ac.uk

M. N. GORIA completed his MA in statistics at the University of Punjab (Lahore, Pakistan), and his PhD in statistics at the University of California in Berkeley. He is now Professor of Statistics at the University of Trento. His research focuses on parametric and nonparametric statistical inference.
Istituto di Statistica e Ricerca Operativa, Università degli Studi di Trento, Via Inama, 38100 Trento, Italy
mgoria@gelso.unitn.it

It's a kind of transitive law, isn't it?
when, in a house of growing children
two people who pet the same cat are petting each other.
Especially if one of them is holding the cat.
Especially if both of them are holding the cat.
And if Devin gets under the blanket with Mirage
and lets only their heads stick out
and smiles up in that way
if the pug of his nose is close to that spot between Mirage's ears
and if I grab hold of it all
and kiss it all...

well, Devin also knows
and Mirage also knows
that something is necessary
something is sufficient
and something else is scared.

Contributed by Marion Cohen, Drexel University, Philadelphia, PA