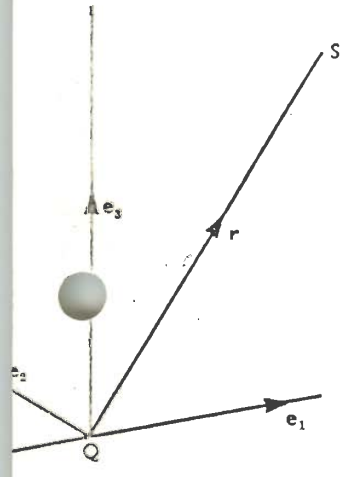
$_3 + a\omega e_2$.

the situation in which a seagull
, it appears to move on a helix.
rc of a circle of radius b, what is
to the Earth?



hich defines the frame f. Then
centre of the circle on which the
en if the position vector of the
xpressed parametrically as

$e_2 + \phi \tan\alpha\, e_3$),

$\cos\phi\, e_2 + \tan\alpha\, e_3$).

to the Earth (F) is then

$\dot{\phi}(\beta_1 e_2 - \beta_2 e_1)$

s ϕ, $\beta_2 = a \sin\phi$; after a little

$+ \dot{\phi})\cos\phi)e_2 + a\dot{\phi}\tan\alpha\, e_3$.

MARGARET E. RAYNER

HOW MANY DIFFERENT KEYS?

BY C. A. COULSON

The profile of a familiar type of key is shown in Fig. 1a. The shape of the key profile is determined by the depths of successive

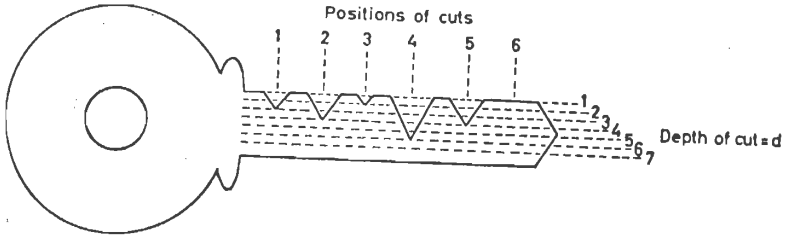


FIG. 1a. The key with successive cuts $d = 3,4,2,6,4,1$ and for which $N = 6$, $D = 7$.

cuts. Each cut is of wedge shape. The centres of the cuts lie at N regular well-defined positions. In the key shown there are 6 cuts ($N = 6$). The depths d of these cuts, which distinguish one key from another, must have one of a set D of well-defined values. If we regard a cut of zero depth as defined by $d = 1$, the key shown may have values $d = 1, 2, \ldots, 6, 7$ ($D = 7$).

If the depths of all the N cuts were independent, there would clearly be a total number N^D of possible distinct keys. A few of those would, in practice, be undesirable, such as the key where each $d = 1$. There are not many of these, and it is easy to weed them out. We shall therefore neglect them in what follows.

The real problem arises because, on account of the wedge shape of each cut, a deep cut in one position would obliterate the space required for a shallow cut in the positions on either side. Figure 2

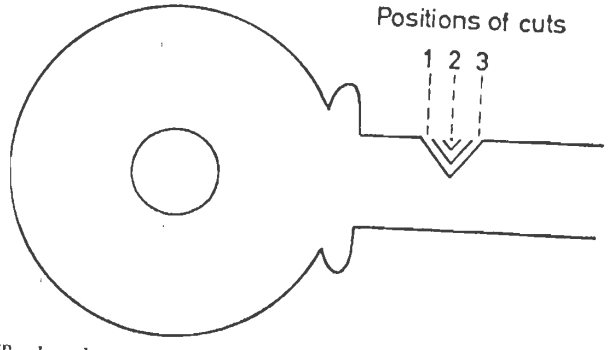


FIG. 2. To show how $d = 4$ at position 2 prevents $d = 1$ at positions 1 and 3.

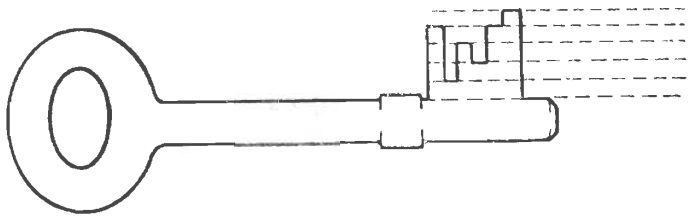


FIG. 1b. A conventional mortice lock key. There are no restrictions on the depths of successive cuts.

shows a situation where a cut $d = 4$ in position 2 prevents our choosing $d = 1$ in position 3. The difference $4 - 1 = 3$ is called the tolerance T. In general therefore, for an acceptable key, we must have

$$|d_{n+1} - d_n| < T \tag{1}$$

This condition, which clearly does not apply to a mortice lock key of the more familiar type as shown in Fig. 1b, restricts the depth of any one cut to not more than $2T - 1$ values. If d_n is small, or large, the number of possible depths d_{n+1} is less than $2T - 1$. Our problem now is: how many different keys are possible for given N, D, T?

To solve this problem it is convenient to replace it by an equivalent one. We set up a pattern of small boxes as in Fig. 3, in which each

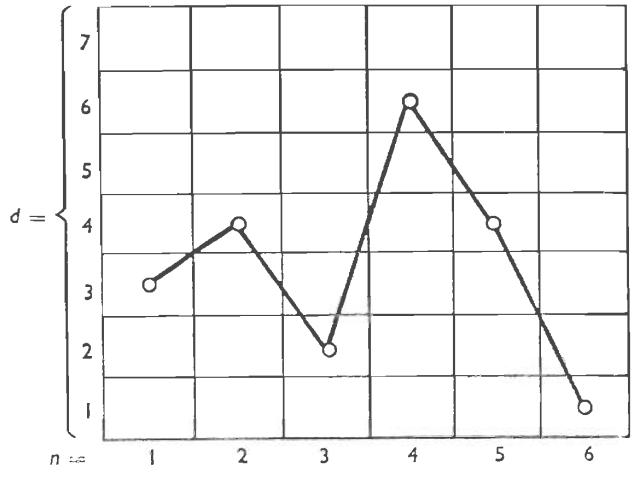


FIG. 3. Schematic representation of key shown in Fig. 1a. In order that the cuts at positions $n = 3$ and 4 do not obliterate each other, it is necessary for this key that $T > 6 - 2 = 4$.

box is labelled by the number of a cut ($n = 1, 2, \ldots, N$) plotted horizontally, and the depth of this cut ($d = 1, 2, \ldots, D$) plotted vertically. Each shape of key is represented by an array of dots: each vertical column will have one dot, corresponding to the depth of cut in that column. But in successive columns the dots must not be as much as T units apart. The dot pattern of Fig. 3 represents the key profile of Fig. 1.

We now use a recurrence relation to calculate how many different dot patterns there can be, starting on the left of Fig. 3 and moving to the right.

Let $u_{n,d}$ be the number of permitted keys for which there are n cuts and the last cut is of depth d. If the nth cut is of depth d, the $n-1$th cut must have been at any one of the depths d, $d \pm 1$, $d \pm 2$, $\ldots$, $d \pm (T - 1)$, and so

$$u_{n,d} = \sum_{\alpha=d-T+1}^{\alpha=d+T-1} u_{n-1,\alpha} \tag{2}$$

where, since no cut can have depth $d > D$ or $d < 1$, we suppose that all $u_{n-1,\alpha}$ for which $\alpha > D$ or $\alpha < 1$ are identically zero.

The relation (2) is conveniently put in matrix form. We introduce the column matrix $\mathbf{u}_n$ defined by

$$\mathbf{u}_n = \begin{bmatrix} u_{n1} \\ u_{n2} \\ \cdot \\ \cdot \\ \cdot \\ u_{nD} \end{bmatrix}, \text{ where } \mathbf{u}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix} \tag{3}$$

The transposed matrices are

$$\mathbf{u}_n{}^{\dagger} = (u_{n1}, u_{n2}, \ldots, u_{nD}), \qquad \mathbf{u}_1{}^{\dagger} = (1, 1, \ldots, 1) \tag{4}$$

The fact that $\mathbf{u}_1$ is the unit column matrix merely means that when we start cutting there is just one key possible for each of the D possible depths of this cut. The set of equations (2) take the matrix form

$$\mathbf{u}_n = \mathbf{C}\mathbf{u}_{n-1} \tag{5}$$

where $\mathbf{C}$ is the bordered matrix

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & 1 & & & 0 \\ 1 & 1 & 1 & 1 & & \\ 1 & 1 & 1 & 1 & 1 & \\ & 1 & 1 & 1 & 1 & 1 \\ & & 1 & 1 & 1 & 1 & 1 \\ & & & 1 & 1 & 1 & 1 \\ & 0 & & & 1 & 1 & 1 \end{bmatrix} \tag{6}$$

in which the entries in the leading diagonal are all unity, and this diagonal is bordered on each side by $T - 1$ unit entries. All other elements are zero. The maximum number of non-zero elements in each row is $2T - 1$ (where we have supposed that $2T - 1 < D$). Equation (6) illustrates the particular case in which $T = 3$, $D = 7$.

Our reasons for introducing the matrix $\mathbf{u}_n$ are twofold. In the first place, by repeated application of (5) it follows that

$$\mathbf{u}_n = \mathbf{C}^{n-1}\mathbf{u}_1 \tag{7}$$

In the second place, since the last cut on the key must have depth $d_N = 1, 2, \ldots, D$, it follows that the total number $\mathscr{N}_{N,D}$ of keys with N cuts is

$$u_{N1} + u_{N2} + \cdots + u_{ND}$$

But from (4) and (7) this can be written

$$\mathscr{N}_{N,D} = \mathbf{u}_1{}^{\dagger}\mathbf{u}_N = \mathbf{u}_1{}^{\dagger}\mathbf{C}^{N-1}\mathbf{u}_1 \tag{8}$$

This is the answer, and for any chosen N, D, T it is possible to complete the matrix multiplication and calculate the required number $\mathscr{N}$. But the result may be simplified as follows.

The real symmetric matrix C may be diagonalized by means of a unitary orthogonal matrix $\mathbf{V}$, so that

$$\mathbf{C} = \mathbf{V}^{\dagger}\mathbf{\Lambda}\mathbf{V} \tag{9}$$

where

$$\mathbf{V}^{\dagger}\mathbf{V} = \mathbf{1}$$

Λ is a diagonal matrix, with elements $\lambda_1, \lambda_2, \ldots, \lambda_D$. The λ_i are, of course, merely the D latent roots of the matrix $\mathbf{C}$. Then

$$\mathscr{N}_{N,D} = \mathbf{u}_1{}^{\dagger}\mathbf{V}^{\dagger}\mathbf{\Lambda}^{N-1}\mathbf{V}\mathbf{u}_1 \tag{10}$$

The matrix $\mathbf{\Lambda}^{N-1}$ is also diagonal, with elements $\lambda_1^{N-1}, \lambda_2^{N-1}, \ldots$. If we now put $\mathbf{V}\mathbf{u}_1$ equal to a column matrix $\mathbf{v}$, so that

$$\mathbf{v} = \mathbf{V}\mathbf{u}_1, \tag{11}$$

it follows that

$$\mathscr{N}_{ND} = \mathbf{v}^{\dagger}\mathbf{\Lambda}^{n-1}\mathbf{v} \tag{12}$$

In any particular situation, we start by writing down the matrix $\mathbf{C}$. The simplest procedure then is to evaluate $\mathbf{C}^{N-1}$ and so, from (8), determine $\mathscr{N}$. But this is rather clumsy, and so we should, if practicable, fall back on the analysis of (9)-(12). With an electronic computer it is easy to find the latent roots λ_i, and then the columns of $\mathbf{V}$ are normalized multiples of the corresponding latent vectors. The rest of the analysis is then straightforward. When N is fairly large (greater than about $N = 5$) the quantity (12) is dominated

Table 1. *The case of* $d = 7$, $T = 2$

$d = 7$	1	2	5	13	35	96	267	749	2113	5982
6	1	3	8	22	61	171	482	1364	3869	10991
5	1	3	9	26	75	215	615	1756	5009	14279
4	1	3	9	27	79	229	659	1889	5401	15419
3	1	3	9	26	75	215	615	1756	5009	14279
2	1	3	8	22	61	171	482	1364	3869	10991
1	1	2	5	13	35	96	267	749	2113	5982
$\mathscr{N}_{N,7}$ (exact)	7	19	53	149	421	1193	3387	9627	27383	77923
$\mathscr{N}_{N,7}$ (eqn. 20)	6	16	45	129	368	1050	2990	8516	24251	69060

by $\lambda_{\max}$, the largest of the λ_i, so that $\mathscr{N}_{N,D}$ varies approximately as $\lambda_{\max}^{N-1}$. It is easy to show that $\lambda_{\max} < 2T - 1$ and tends towards this value as D increases.

The following numerical example is interesting, since it represents a situation for which a closed form can be provided for the final value $\mathscr{N}_{N,D}$. Consider a key for which $N = 10$ so that there are 10 cuts; and for which each cut may have depth $1, 2, \ldots, 7$, so that $D = 7$. Further let the tolerance be $T = 2$. This compels successive depths to differ by not more than one unit.

We now set up the tableau of values of $u_{n,d}$ shown in Table 1. To write down this table we proceed, column by column, from the left to the right. According to (2) each entry in column n is the sum of three entries in column $n - 1$, except for the top and bottom entries as shown by the arrows in the table. At the foot of each column is given the total of all the entries in this column. This is

the value of $\mathcal{N}_{n,d}$. Thus, with 10 cuts there are 77,923 possible keys (including the "undesirables" with which we are not concerned). The arithmetic is simple, and can be extended easily to larger n or d.

The matrix $\mathbf{C}$ of (6) now takes the form

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & & & & & \\ 1 & 1 & 1 & & & & \\ & 1 & 1 & 1 & & & \\ & & 1 & 1 & 1 & & \\ & & & 1 & 1 & 1 & \\ & & & & 1 & 1 & 1 \\ & & & & & 1 & 1 \end{bmatrix} \tag{13}$$

The latent roots of this matrix can be shown to be

$$\lambda_j = 1 + 2\cos j\pi/8 \ (j = 1, 2, \ldots, 7) \tag{14}$$

so that

$$\lambda_{\max} = 1 + 2\cos \pi/8 = 2{\cdot}8478 \tag{15}$$

Further the normalized latent vector corresponding to λ_j has components

$$\frac{1}{2}\sin\frac{jr\pi}{8} \ (r = 1, 2, \ldots, 7) \tag{16}$$

Hence the matrix $\mathbf{V}$ of (9) is a symmetrical matrix whose elements $V_{r,j}$ are given by (16). It can soon be verified that $\mathbf{V}^\dagger\mathbf{V} = \mathbf{1}$. Then, from (11)

$$\mathbf{v} = \mathbf{V}\mathbf{u}_1$$

is a column matrix whose rth element is

$$v_r = \frac{1}{2}\sum_{j=1}^{7}\sin\frac{rj\pi}{8} = \sin 3\alpha \sin 4\alpha \Big/ 2\sin\frac{\alpha}{2} \text{ where } \alpha = \frac{r\pi}{8} \tag{17}$$

Finally, from (12)

$$\mathcal{N}_{N,7} = \sum_{r=1}^{7} v_r^2 \lambda_r^{N-1} \tag{18}$$

The combination of (17) and (18) gives the complete analytical form of the answer. For different N it gives the values $\mathcal{N}_{\text{exact}}$ at the foot of Table 1.

The series (18) should be dominated by $\lambda_{\max}^{N-1}$. From (15) this is λ_1, and then from (17) $\alpha = \pi/8$ and

$$v_1 = \sin(3\pi/8)/2\sin(\pi/16) \tag{19}$$

Thus for large N, the number of keys is dominated by the term

$$\frac{\sin^2\frac{3\pi}{8}}{4\sin\frac{\pi}{16}}\left(1 + 2\cos\frac{\pi}{8}\right)^{N-1} \tag{20}$$

Values of this expression for $N = 1, 2, \ldots, 10$ are shown, to the nearest integer, on the bottom line of the table, where they may be compared with the exact values in the line above. Considering that $\lambda_{\max}$ is not very much greater than some of the other λ_j the agreement is not bad (the error is about 12%). But the ratios of successive values of $\mathcal{N}_{N,D}$ are even more impressive. Table 1 shows that the ratio $\mathcal{N}_{N,7}/\mathcal{N}_{N-1,7}$ has the values 2·8337, 2·8391, 2·8423, 2·8444, 2·8456 when $N = 6, 7, 8, 9, 10$ respectively. According to (20) the asymptotic value of this ratio should be

$$1 + 2\cos\pi/8 = 2{\cdot}8478$$

It is surprising how rapidly this asymptotic value is approached.

I would like to thank Mr Brian Greaves, of Keyways, Hale Barnes, Cheshire, for bringing this problem to my attention, and for telling me that Mr Clifford Jones, B.Sc., and some of the boys at Leigh Grammar School had obtained a purely numerical way of solving this problem.

Mathematical Institute,
24–29 St Giles,
Oxford OX1 3LB

C. A. COULSON

THE MATHEMATICS OF AGMs

HAZEL PERFECT

This evening, on the occasion of our Annual General Meeting*, I propose that we look at the following problem, which I shall call "the AGM problem."

A certain organisation is made up of several departments and, in general, any member of the organisation may belong to more than one department. (We may, for instance, think of a Church with its Choir, Sunday School, Youth Club, etc.) At its AGM, the organisation wishes to receive a report from each of the departments. Thus, each department needs to appoint a spokesman. Furthermore,

* This is the text of a lecture given to the Sheffield and District Branch of the Mathematical Association at the Annual General Meeting on October 4th 1967.