A COMBINATORIAL PROBLEM ASSOCIATED WITH A FAMILY OF COMBINATION LOCKS

G. SIMMONS, Sandia Corporation

This paper discusses an interesting combinatorial problem which arises in the analysis of a family of electrical combination locks. These devices, unlike mechanical combination locks, have the sequential codes (positions of the tumblers) introduced by switch closures. Obviously a great many restrictions could be imposed on the choice of codes, their sequence of insertion etc., which would lead to functionally different types of locks. However, all of these electronic combination locks have some features in common. The operator is presented with n switches (the dial and tumbler), each of which may be set to an "on" or "off" position. The arrangement of settings of these switches constitutes a code for insertion into the lock, corresponding to the rotation of the tumbler to one of the code positions in the mechanical analog. The direction of rotation of the tumbler is reversed when the code position is reached to "enter" the code into the mechanical lock. By direct analogy, once the desired code is set into the n switches by the operator, he presses an entry button to cause the code to be entered in the lock.

The family of locks which are the origin of the problems considered in this paper have some special restrictions imposed on the code sequences allowed to the operator. The n switches are independent, i.e., they may be closed individually or in any combination whatsoever. If a switch is on when an entry is made, it is removed from further consideration. It may be useful to think of this switch being deactivated by a latching mechanism which was actuated by the initial closure of the switch and the entry button. At any rate it is not available to the operator for further code construction. There is no meaning to an ordering of the switches which are closed to form a code at the time of entry. Thus AB means the same thing as BA if the product symbol pairing is used to represent an entry code of switch A and switch B closed. The sequencing of discrete entries constitutes the "combination" of the lock. For an example A—BC would symbolize the entry of switch A in the on position followed by the entry of switches B and C in the on position. This would be a specific combination, and would be recognized as different from AB—C, etc. The locks considered here differ from their mechanical analogs in only one particular: the concept of limited try. After the operator has entered some combination, sequence of codes, he presses a "test" button. If the correct combination has been entered the lock is operated, or opens. If the combination is an incorrect one, however, the lock is disabled, temporarily or permanently, so that further combinations may not be tried.

The obvious question, in view of the foregoing description of the operation of the lock, is the security which a particular lock affords, i.e., a lock with n switches. Since the system is designed to allow only a single combination trial, the security is the probability of an unauthorized person's finding the correct code sequence by accident on the first attempt. This is $1/P_n$, where P_n is the

total number of combinations for an n switch lock. P_n and several of its interesting relations are developed in the following sections.

It is possible to determine P_n directly by enumeration of the possible groupings for small n; however, this quickly proves to be an impractical technique for locks which are still of feasible size; $n=10$ for an example. The first few values of P_n are:

$$P_1 = 1 \qquad P_2 = 5 \qquad P_3 = 25.$$

The actual enumeration of the combinations for $n=1$, 2, and 3 are as follows, with the null combination, corresponding to no switches being closed, being included for logical consistency. This arrangement is of no practical interest, since it corresponds to the lock being ready to open all the time and is not considered to be an acceptable combination code for a lock. The entries in the table are grouped into columns according to the number of distinct entries involved. Thus the simultaneous entry of any number of switches is interpreted as a single distinct code entry for the purposes of this classification.

	0	1	2	3
P_1	$-$	$-a-$		
P_2	$-$	$-a-$	$-a-b-$	
		$-b-$	$-b-a-$	
		$-ab-$		
P_3	$-$	$-a-$	$-a-b-$	$-a-b-c-$
		$-b-$	$-b-a-$	$-b-c-a-$
		$-c-$	$-b-c-$	$-c-a-b-$
		$-ab-$	$-c-b-$	$-a-c-b$
		$-bc-$	$-a-c-$	$-c-b-a-$
		$-ac-$	$-c-a-$	$-b-a-c-$
		$-abc-$	$-a-bc-$	
			$-bc-a-$	
			$-ab-c-$	
			$-c-ab-$	
			$-ac-b-$	
			$-b-ac-$	

The above display contains the key to the solution of the problem. To form any combinatory element for the columns of P_n it suffices to note that only one new symbol is being introduced, x_n, $x=a, b, c, \cdots$. If the column elements being investigated have j distinct code entries, then it is obvious that only the columns devoted to j and $j-1$ code entries in the preceding classification of P_{n-1} can affect these elements. For an example, the new symbol, $-x_n-$, may be introduced in place of any occurrence of $-$ in the $j-1$ entry elements for P_{n-1} to produce combinations of j distinct entries. If $G(n, j)$ is defined to be the number of elements for j distinct closures under P_n, then the foregoing rule may be written symbolically as $jG(n-1, j-1)$. If one now considers the elements for P_{n-1} which involved j distinct entries, it is obvious that the introduction of the new symbol must be made in such a manner that no new entries are introduced. This can be accomplished either by including the new symbol with any product

symbol grouping, code, in these combinatory elements, i.e., enter the associated switch in combination with one of the other distinct code entries, or else by not using it at all. The number of such options is expressed by $(j+1)G(n-1, j)$. These are the only ways in which combinations of j distinct entries can be generated using n symbols, given the combinations for $(n-1)$ symbols classified according to the number of entries. This result is expressed by the partial difference equation

$$G(n, j) = jG(n-1, j-1) + (j+1)G(n-1, j). \tag{1}$$

This equation is descriptive of the system being studied, and its solution and an investigation of the properties of these solutions is the object of this paper. The number P_n which is desired as a solution for the combination lock problem is given by

$$P_n = \sum_{j=1}^{n} G(n, j). \tag{2}$$

A tabular display of the numbers generated by (1) is helpful in visualizing some of the relations to be developed in the following analysis:

n/j	0	1	2	3	4	5
0	1					
1	1	1				
2	1	3	2			
3	1	7	12	6		
4	1	15	50	60	24	
5	1	31	180	390	360	120

Equation (1) can be reduced to a simpler form by the change of variable:

$$G(n, j) = j!G'(n, j). \tag{3}$$

The substitution of (3) into (1) yields the following linear partial difference equation:

$$G'(n, j) = G'(n-1, j-1) + (j+1)G'(n-1, j). \tag{4}$$

To allow symbolic manipulation this is best expressed in terms of the partial displacement operators, $\mathbf{E}_n$ and $\mathbf{E}_j$, defined by the relation $\mathbf{E}_n G(n, j) = G(n+1, j)$, [1]. Equation (4) may then be written as:

$$\left(\mathop{\mathbf{E}}_{n} \mathop{\mathbf{E}}_{j} - 1 - (j+2) \mathop{\mathbf{E}}_{j} \right) G'(n, j) = 0. \tag{5}$$

This type of linear partial difference equation, i.e., one in which one of the variables does not appear explicitly, may be treated by Boole's method. Consider the operator $\mathbf{E}_n$ to be a constant k and solve the resulting linear difference equation in the single variable j. Equation (5) now assumes the form

$$(k - j - 2) \mathop{\mathbf{E}}_{j} G(n, j) - G'(n, j) = 0. \tag{6}$$

If the variable change

$$u(n, j) = v(j)G'(n, j) \tag{7}$$

is made, where $v(j)$ is defined to be

$$v(j) = (k - 1)(k - 2) \cdots (k - j - 1), \tag{8}$$

(6) may be reduced to the simple system

$$u(n, j + 1) - u(n, j) = 0. \tag{9}$$

Equation (9) has as a solution

$$u(n, j) = c \tag{10}$$

which may be rewritten in the following form using (8):

$$[k - 1][k - 2] \cdots [k - (j + 1)]G'(n, j) = c. \tag{11}$$

This may then be expanded into the following operator ($\mathbf{E}_n$) equation:

$$\sum_{i=0}^{j} k^i \mathrm{S}_{j+1}^{i+1} G'(n, j) = c, \tag{12}$$

where S_{j+1}^{i+1} is a Stirling number of the first kind.

This equation, (12), may be treated by the method of characteristic equations. The characteristic equation associated with (12) is

$$\sum_{i=0}^{j} \mathrm{S}_{j+1}^{i+1} r^{j-1} = 0. \tag{13}$$

The roots of this equation are 1, 2, 3, $\cdots$, $j+1$, so that the general solution of (12) is of the form

$$G'(n, j) = c_0(j)(j + 1)^n + c_1(j)j^n + \cdots + c_{j-1}(j)2^n + c_j, \tag{14}$$

where the $c_i(j)$ are arbitrary, and as yet undetermined, functions of j.

A single value of the function P_n will involve $n(n+1)/2$ of the functions, $c_i(j)$, or rather functional values. In order to determine these functions it is necessary to refer to the defining relationship (4). Examination of (4) allows the following boundary conditions to be stated:

$$\begin{aligned} G'(n, j) &= 0 \qquad \text{if } j > n \\ G'(n, j) &= 1 \qquad \text{if } j = n. \end{aligned} \tag{15}$$

If these restrictions are imposed on (14) the following family of simultaneous equations is obtained:

$$\left.\begin{aligned} \sum_{i=0}^{j} c_i(j)(j + 1 - i)^n &= 1 \\ \sum_{i=0}^{j} c_i(j)(j + 1 - i)^{n-k} &= 0 \qquad \text{for } 1 \leqq k \leqq n \end{aligned}\right\} \tag{16}$$

The determinant of this system is

$$\begin{vmatrix} (j+1)^n & j^n & \cdots & 2^n & 1 \\ (j+1)^{n-1} & j^{n-1} & \cdots & 2^{n-1} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ (j+1) & j & \cdots & 2 & 1 \\ 1 & 1 & \cdots & 1 & 1 \end{vmatrix} = D \tag{17}$$

which is Vandermonde's determinant. n appears as a dummy variable in (17) as may be seen by examining the restraints of (15) and the equations (16) from which D is derived. The system is defined only for $0 \leqq j \leqq n$, i.e., in solving for the $c_i(j)$ only $(j+1)$ equations of the form given by (14) are considered of degrees $(j+1), (j), \cdots, (2),(1)$. Thus (17) is a square $(j+1)\times(j+1)$ determinant.

D is given by

$$D = j!(j-1)! \cdots 2!\,1! \tag{18}$$

Since the constant column to be introduced into D for the solution for the $c_i(j)$ is a unique one, i.e., a one in the highest order position and zero in all other entries, a very simple solution is possible, based on an expansion of D by minors along the upper row. If one denotes the numerator matrices by N_i, then they may be written in the following form:

$$N_i = \frac{(j-1)!(j-2)! \cdots 2!1!}{i!(j-1-i)!}(-1)^i, \tag{19}$$

where i obviously ranges from 0 to j. The $c_i(j)$ may now be determined:

$$c_i(j) = \frac{N_i}{D} = (-1)^i \binom{j}{i} \frac{1}{j!}. \tag{20}$$

Thus the arbitrary functions $c_i(j)$ are determined and the solution may be written for (14) with the $c_i(j)$ replaced by the appropriate functions of j.

$$G'(n,j) = \sum_{i=0}^{j} (-1)^i \binom{j}{i} \frac{1}{j!} (j+1-i)^n \tag{21}$$

or

$$G(n,j) = \sum_{i=0}^{j} (-1)^i \binom{j}{i} (j+1-i)^n. \tag{22}$$

The form assumed by the $G'(n,j)$ is a well-known expression for the Stirling numbers of the second kind, [2]. The solutions (21) and (22) may be conveniently written in a simpler form by the introduction of S_{n+1}^{j+1}.

$$G'(n,j) = \mathrm{S}_{n+1}^{j+1} \tag{21a}$$

$$G(n,j) = j!\mathrm{S}_{n+1}^{j+1}. \tag{22a}$$

This completes the solution of the original partial difference equation (1) and incidentally of the problem from which it was derived. Equation (2) may be used with either (22) or (22a) to give as a final result

$$P_n = \sum_{j=1}^{n} \sum_{i=0}^{j} (-1)^i \binom{j}{i} (j+1-i)^n \tag{23}$$

or

$$P_n = \sum_{j=1}^{n} j! S_{n+1}^{j+1}. \tag{23a}$$

The generating function for the P_n is simply obtained from the latter form, (23a), and is found to be:

$$P_n = \frac{d^n}{du^n}\left(\frac{1}{2e^{-u}-1}\right)_{u=0} - 1, \tag{24}$$

where the nth derivative of the parenthetic term is to be evaluated at $u=0$.

It is of interest to tabulate some of the values of P_n derived by use of (23a), since they are the measure of security achieved by the family of combination locks on which this problem is based.

	1	2	3	4	5	6	7	8	9	10
P_n	1	5	25	149	1,081	9,366	94,586	1,091,670	14,174,522	204,495,125

2050

References

1. Charles Jordan, Calculus of finite differences, Chelsea, New York, 1950.
2. John Riordan, An introduction to combinatorial analysis, Wiley, New York, 1958.

Reprinted from the MATHEMATICS MAGAZINE
Vol. 37, No. 3, May, 1964

No A47782 = 2nd version