11. ———, Letter to the author 1976.

12. C. Goffman and D. Waterman, Functions whose Fourier series converge for every change of variables, Proc. Amer. Math. Soc., 19 (1968) 80–86.

13. M. Iosifescu, Conditions that the product of two derivatives be a derivative, Rev. Math. Pures Appl., 4 (1959) 641–649 (In Russian).

14. M. Laczkovich and G. Petruska, On the transformers of derivatives, to appear.

15. I. Maximoff, Sur la transformation continue de fonctions, Bull. Soc. Phys. Math. Kazan, (3) 12 (1940) 9–41 (Russian, French summary).

16. ———, Sur la transformation continue de quelques fonctions en dérivées exactes, Bull. Soc. Phys. Math. Kazan, (3) 12 (1940) 57–81 (Russian, French summary).

17. A. P. Morse, Dini derivatives of continuous functions, Proc. Amer. Math. Soc., 5 (1954) 126–130.

18. S. Saks, Theory of the integral, Monographie Matematyczne 7, Warszawa-Lwów, 1937.

19. G. Tolstov, Parametric differentiation and the restricted Denjoy integral (in Russian), Mat. Sbornik, 53 (95) (1961) 387–392.

20. W. Wilkosz, Some properties of derivative functions, Fund. Math., 2 (1921) 145–154.

21. Z. Zahorski, Sur la première dérivée, Trans. Amer. Math. Soc., 69 (1950) 1–54.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CA 93106.

A CIRCLE-OF-LIGHTS ALGORITHM FOR THE "MONEY-CHANGING PROBLEM"

HERBERT S. WILF

I. Introduction. The classical "money-changing problem" asks the following question: If we have coins of k different values, namely $a_1,\ldots,a_k$ units respectively, then what sums of money can we change, assuming that an infinite supply of each of the k denominations is available?

For example, if we have only 3-cent coins and 5-cent coins, then we can change 0, 3, 5, 6 cents and any amount $\geqslant 8$ cents.

In general, we are given integers $0<a_1<a_2<\cdots<a_k$ and we suppose that g.c.d.$(a_1,\ldots,a_k)=1$. We ask for a description of the set (semigroup) of integers n which can be written in the form

$$n=x_1a_1+x_2a_2+\cdots+x_ka_k \qquad (x_i\geqslant 0,\quad i=1,\ldots,k). \tag{1}$$

It is well known that there is a least positive integer χ, called the *conductor* of $a_1,\ldots,a_k$, such that $n=\chi-1$ is not representable as in (1), but *every* $n\geqslant\chi$ is representable. Sylvester showed that for $k=2$ the conductor is $\chi=(a_1-1)(a_2-1)$, and more general results may be found in **[1]**, **[5]**.

Our concern here is with algorithms for finding the conductor, for determining whether or not a given integer is representable, for finding a representation of a given integer, and for determining the number of n which are not representable ("omitted values").

Consider first the calculation of the conductor. A. Brauer **[1]** suggested the following procedure: For each $r=0,1,\ldots,a_1-1$ let n_r denote the least value of n such that $n\equiv r \pmod{a_1}$ and n is representable in the form (1). Then we have

$$\chi=1-a_1+\max_r(n_r). \tag{2}$$

The author received his Ph.D. in Applied Mathematics from Columbia University in 1958, after several years in industrial computing. He has taught at the University of Illinois and the University of Pennsylvania, with visiting positions at Imperial College (University of London), Rockefeller University, and the University of Paris. He was a Guggenheim Fellow in 1973–74. His interests are in combinatorics, spectral theory, and numerical analysis; his books include Mathematical Methods for Digital Computers, 1960 (edited jointly with A. Ralston); Mathematics for the Physical Sciences, 1962; Calculus and Linear Algebra, 1966; Mathematical Methods for Digital Computers, vol. II, 1967; Programming for a Digital Computer in the Fortran Language, 1969; Finite Sections of Some Classical Inequalities, 1970; Combinatorial Algorithms (with A. Nijenhuis), 1975; and Statistical Methods for Digital Computers (with K. Enslein and A. Ralston), in press.—*Editors*

The question of precisely how the n_r are to be found was left open.

Heap and Lynn ([3], [4]) have proposed another algorithm for finding χ. One would define a matrix C by

$$C_{ij}=\begin{cases} 1 \text{ if } i-j=a_p-1 & \text{for some } p \\ 1 \text{ if } i-j=-1 \\ 0 \text{ otherwise} \end{cases} \tag{3}$$

for $i,j=1,\ldots,N$, where $N=a_k$. They showed that if γ denotes the least power of C all of whose entries are positive then $\chi=\gamma-a_k+1$. The index γ is found by bisection of some interval which is known to contain it. This algorithm needs $O(a_k^3(\log\chi)^2)$ time and about $2a_k^3$ bits of array storage, and so, while quite elegant, it would not be preferred for large problems.

II. The circle of lights. Suppose $1<a_1<\cdots<a_k$ are given relatively prime integers. For each $n=0,1,2,\ldots$, let x_n denote the proposition that the integer n is representable in the form (1). Then we have

$$\begin{aligned} &\text{(a)} \quad x_m=\text{false } (m<0) \\ &\text{(b)} \quad x_0=\text{ true} \\ &\text{(c)} \quad \text{For } m>0: \\ &\qquad x_m=x_{m-a_1} \text{ or } x_{m-a_2} \text{ or} \cdots \text{ or } x_{m-a_k}. \end{aligned} \tag{4}$$

Now imagine that we are calculating the x_m recursively from (4). Observe that if at any time we encounter a_1 consecutive values of m for which x_m is true, then all succeeding x_m are true, and so the calculation can halt and the conductor will be 1 greater than the last m such that x_m was false.

Further, since each x_m is found from only its $N=a_k$ predecessors, we can over-write x_{m-N} with x_m as soon as the latter is computed. Thus the array x requires only a_k bits of storage as a circular list.

The whole procedure can be visualized as a circle of N lights, numbered $0,1,\ldots,N-1$. Initially light 0 is on, the others off. We sweep around the circle in a clockwise direction, and as we encounter each light, we will turn it on if any of the k lights which are situated $a_1,a_2,\ldots,a_k$ lights back (counterclockwise) from the present are on, we leave it on if it was already on, otherwise we leave it off. The process halts as soon as any a_1 consecutive bulbs are "on."

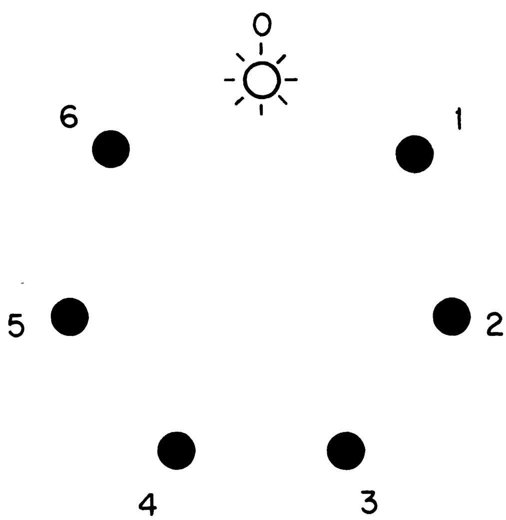

FIG. 1

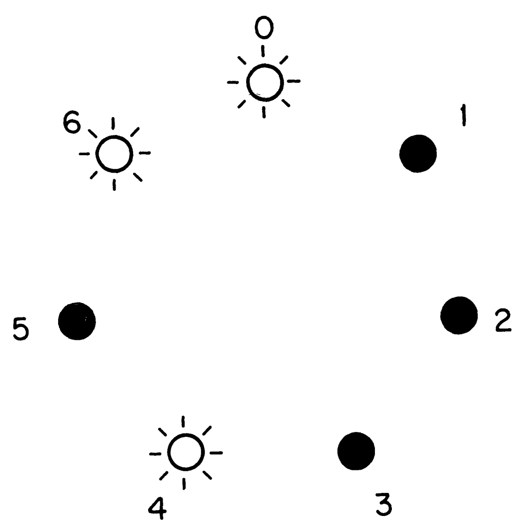

FIG. 2

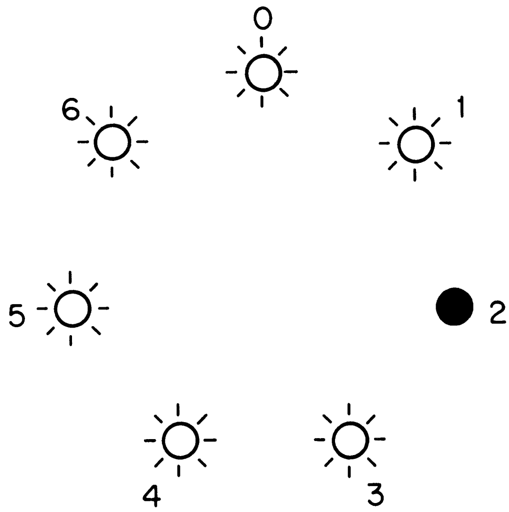

FIG. 3

As an example, consider the integers $(a_1, a_2, a_3) = (4, 6, 7)$. We have a ring of 7 lights which is initially as shown in Figure 1. After one full sweep around the circle the situation is as shown in Figure 2.

After a portion of one more sweep, going only as far as light number 5, the lights are as shown in Figure 3.

Now we have $\geqslant 4$ consecutive lights on, so the process can halt. The conductor is one more than the number represented by the most recent "off" bulb, i.e., it is $1 + 9 = 10$.

It is interesting that the algorithm provides a proof of its own complexity:

THEOREM. *Let $1 < a_1 < a_2 < \cdots < a_k$ be relatively prime, and let x be their conductor. Then $\chi \leqslant a_k^2$.*

Proof. After each full sweep of the circle of lights, at least one more light must be "on," or else, since all subsequent sweeps would be identical, the conductor would be infinite. (Professor M. Koren has shown (p.c.) that actually every sweep interval of length a_1 produces a new light on.) After a_k sweeps they will all be on. ■

We state a formal algorithm which is based on these ideas. Input are $1 < a_1 < \cdots < a_k$, relatively prime. Output are the conductor χ, and Ω, the number of omitted values. The counter q counts consecutive assumed values and is reset to zero at each omitted value.

(A) $q \leftarrow 0$; $N \leftarrow a_k$; $x_0 \leftarrow$true; $x_\mu \leftarrow$false $(\mu = 1, N-1)$; $m \leftarrow a_1$; $\Omega \leftarrow 0$
(B) [m is representable] $r \leftarrow m \pmod{N}$; $x_r \leftarrow$true
(C) $q \leftarrow q+1$; if $q \neq a_1$, go to (D); $\Omega \leftarrow m - a_1 - \Omega$; $\chi \leftarrow m - a_1 + 1$; exit.
(D) [next m] $m \leftarrow m+1$; $i \leftarrow k$.
(E) [Is $m - a_i$ representable?] $r \leftarrow m - a_i \pmod{N}$; if x_r is true, go to (B); if $i = 1$, go to (F); $i \leftarrow i-1$; go to (E).
(F) [m is omitted] $\Omega \leftarrow \Omega + q$; $q \leftarrow 0$; go to (D). ■

The algorithm requires a_k bits of array storage and $O(ka_k^2)$ time. A Fortran program of 28 instructions found the conductor $x = 13023$ of the set 271, 277, 281, 283 in 1,2 seconds of IBM 370/168 time, along with the number $\Omega = 6533$ of values omitted by the form. Less than 75 words of array storage were used.

When the same algorithm was written for a little programmable calculator with 20 words of memory, the same problem was solved in about six hours!

To discover if a given n is representable, we would incorporate Brauer's suggestion: In addition to the array x we carry an array y of length a_1 words which stores the first occurrence of each residue class mod a_1. A given n is then representable if and only if $n \geqslant y_q$ where $q \equiv n \pmod{a_1}$.

To construct an explicit representation of a given n we would generate and store explicit representations of the y_j defined above.

We raise the following questions: (a) Is it true that for fixed k the fraction Ω/χ of omitted values is at most $1-(1/k)$ with equality only for the generators $k, k+1, \ldots, 2k-1$? (b) Let $f(n)$ be the number of semigroups whose conductor is n. What is the order of magnitude of $f(n)$ for $n \to \infty$?

I am pleased to thank Professor Nijenhuis for interesting discussions of this problem.

This research was supported by the National Science Foundation.

References

1. A. Brauer, On a problem of partitions, Amer. J. Math., 64 (1942) 299–312.

2. A. Brauer and B. M. Seelbinder, On a problem of partitions, II, Amer. J. Math., 76 (1954) 343–346.

3. B. R. Heap and M. S. Lynn, A graph-theoretic algorithm for the solution of a linear diophantine problem of Frobenius, Num. Math., 6 (1964) 346–354.

4. ———, On a linear Diophantine problem of Frobenius, Num. Math., 7 (1965) 226–231.

5. A. Nijenhuis and H. S. Wilf, Representations of integers by linear forms in nonnegative integers, J. Number Theory, 4 (1972) 98–106.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA 19174.

DISCUSSION ON THE PROGRESS OF PURE ANALYSIS

ÉVARISTE GALOIS

Editorial note. The story of Galois' life (1811–1832) is rather well known. (See, for example, E. T. Bell, *Men of Mathematics*, Simon and Schuster, New York, 1937; L. Infeld, *Whom the Gods Love: The Story of Evariste Galois*, Whittlesey House, New York, 1948.) The essay that follows (and has apparently not previously appeared in English) was written in 1832 as an introduction to a projected series of articles. You should keep in mind that what Galois meant by *Analysis* is not what we mean by the same word today: it included not only algebra but everything that involved calculation (rather than verbal or geometric reasoning).

We know that of all the bodies of human knowledge pure analysis is the most abstract, the most supremely logical, the only one which borrows nothing from the evidence of the senses. Many conclude from these facts that all in all it is the most methodical and the best coordinated subject. But this is an error. Take an algebra book, whether a textbook or some original work, and you will see nothing but a confused accumulation of propositions, whose individual logical structures contrast bizarrely with the disorder of the work as a whole. It seems that the ideas have already cost the author too much for him to take the trouble to tie them together and that the conception of the ideas that underlie his work has so exhausted him that his mind has lost the strength to give birth to an organizing idea.

If you do find an organization, a connection, a coordination, these are artificial and false. There are groundless subdivisions, arbitrary unifications, and entirely conventional arrangements. This defect, worse than the lack of any organization at all, is especially common in textbooks. Most of these are put together by men who have no clear understanding of the science that they teach.

All this will greatly astonish the man in the street, who generally takes the word *mathematics* to be a synonym for logical organization.

However, one will be still more astonished if one reflects that here as elsewhere science is the work of the human mind, which is destined rather to study than to know, to seek the truth rather than to