ON A COMBINATORIAL PROBLEM IN NUMBER THEORY

Bernt Lindström

(received October 17, 1964)

1. Introduction and statement of results. Given an integer $k \geq 2$ and a finite set M of rational integers. Let v_i $(i = 1, 2, \ldots, n)$ be m-dimensional (column-)vectors with all components from M and such that the k^n sums

$$(1.1) \qquad \sum_{i=1}^{n} \varepsilon_i v_i \qquad (\varepsilon_i = 0, 1, 2, \ldots, k-1)$$

are all different. Then we shall say that $\{v_1, v_2, \ldots, v_n\}$ is a detecting set of vectors.

Let a be the maximum of absolute values of the elements in M. Then the components of the sums (1.1) lie between $-akn$ and akn. The number of m-dimensional vectors with all components in this interval is less than $(2akn)^m$. Hence

$$(1.2) \qquad k^{n-m} < (2an)^m .$$

For m fixed n is bounded above. Let $F_k(m)$ be the maximal number of m-dimensional vectors forming a detecting set. Similarly, m is bounded below for n fixed. Let $f_k(n)$ be the minimal m.

In the special case $k = 2$, $M = \{0, 1\}$ the problem of determining $f_2(n)$ is equivalent to the following weighing problem: what is the minimal number of weighings on an accurate scale to determine all false coins in a set of n coins,

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

if false coins weigh a and correct ones b $(a \neq b)$? The choice of coins for a weighing must not depend on results of previous weighings.

This weighing problem was first proposed by H. S. Shapiro in [8] for $n = 5$. N. J. Fine [6] proved that $f_2(5) = 4$. For large n, $f_2(n)$ is estimated in [2], [5], [7], [9]. If $M = \{0, 1\}$ or $\{-1, 1\}$, then

$$\lim_{n \to \infty} \frac{f_2(n) \log n}{n} = \log 4 .$$

This was proved in [7]. For $k > 2$ the problem to estimate $f_k(n)$ was first studied in [2] by D. G. Cantor.

The purpose of this note is to introduce a new method to construct detecting sets of vectors. The method is of more general scope than that used in [7]. A feature of the construction is the use of sets of integers d_i $(i = 1, 2, \ldots, h)$, $1 \leq d_i \leq x$, such that the sums

$$(1.3) \qquad \sum_{i=1}^{h} \varepsilon_i d_i \qquad (\varepsilon_i = 0, 1, 2, \ldots, k-1)$$

are all different (i.e. detecting sets of integers). A simple example is $d_i = k^{i-1}$. Let $h_k(x)$ be the maximum of h. $h_2(x)$ was studied by P. Erdős and L. Moser in [4]. It is easy to see that

$$(1.4) \qquad h_2(2^{n-1}) \geq n , \quad h_k(2^{n-1}) > \frac{n-1}{\log_2 k} .$$

Professor R. K. Guy, Delhi, has kindly sent me a detecting set of 23 integers $< 2^{21}$, i.e.

$$(1.5) \qquad h_2(2^{21}) \geq 23 .$$

The smallest number in Professor Guy's set is 1042698, and the largest 2094203.

By the aid of (1.4) we shall prove the following

THEOREM 1. If $M = \{0, 1\}$ then $F_2(m) \geq A(m)$ and $F_k(m) > \frac{A(m) - m}{\log_2 k}$, where $A(m)$ is the number of 1's in the binary representation of the first m positive integers.

I conjecture that $F_2(m) = A(m)$ for $m = 1, 2, \ldots, 15$ at least. It would follow that $f_2(A(m)) = m$ for $m = 1, 2, \ldots, 15$. On the other hand one can prove, by the aid of (1.5), that

$$F_2(m) > A(m) \text{ for } m \geq 2^{22}. \tag{1.6}$$

The following asymptotic formula was first proved by R. Bellman and H.N. Shapiro in [1] (for another proof see [3]),

$$A(m) \sim \frac{1}{2} m \log_2 m, \text{ as } m \to \infty. \tag{1.7}$$

By the aid of (1.7) and Theorem 1 we shall prove

THEOREM 2. For any finite set of integers M with $|M| \geq 2$ and any integer $k \geq 2$,

$$\lim_{n\to\infty} \frac{f_k(n) \log_k n}{n} = 2.$$

For the proof of Theorem 2 we shall also need the fact that

$$k^{n-m} \leq (ca)^m n^{m/2} \tag{1.8}$$

(c is an absolute constant $< 4e$),

if there is a detecting set of n m-dimensional vectors with

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

all components in M. In the special case $k = 2$, $m = 1$, $M = 1, 2, \ldots, x$, we get by (1.8)

$$(1.9) \qquad 2^{n-1}/\sqrt{n} \leq cx \quad \text{for} \quad n = h_2(x) .$$

The inequality (1.9) was proved by P. Erdős and L. Moser in [4]. (1.8) has been proved by L. Moser in the case $k = 2$, $a = 1$ (unpublished).

There is a class of detecting sets of vectors, which could be characterized as residue-class representing. A set in this class is obtained as follows. Let $v_1, v_2, \ldots, v_m$ be m-dimensional independent vectors with all components from M. They generate a sublattice Λ in the lattice $\mathcal{K}$ of all m-dimensional vectors with integral components. Assume that $v_{m+1}, \ldots, v_n$ have all components in M, and that the sums

$$\sum_{i=m+1}^{n} \varepsilon_i v_i \quad (\varepsilon_i = 0, 1, \ldots, k-1)$$

are incongruent modulo Λ. Then $\{v_1, v_2, \ldots, v_n\}$ is a detecting set. For example, it is easy to see that the detecting sets in [7] and [9] are of the residue-class representing type.

By a lemma in geometric number theory, the number of residue-classes in $\mathcal{K}$ modulo Λ is $|\det(v_1, v_2, \ldots, v_m)|$. It follows that

$$(1.10) \qquad k^{n-m} \leq |\det(v_1, v_2, \ldots, v_m)|$$

and, by an application of Hadamard's inequality,

$$(1.11) \qquad k^{n-m} \leq a^m m^{m/2} .$$

If $k = 2$ and $M = \{0, 1\}$ one can prove the existence of detecting sets of the residue-class representing type for every integer $m \geq 3$ and with $n = A(m)$ for which equality holds in

(1.10). Below will be given a table with references to previous detecting sets of this type.

One possible method to find detecting sets with $n \geq A(m)$ is to choose $v_1, v_2, \ldots, v_m$ such that $\det(v_1, v_2, \ldots, v_m)$ is as large as possible and then try to find $v_{m+1}, \ldots, v_n$. This method will be illustrated by an example in section 3.

Table of the function A(m) with references to detecting sets.

m	3	4	5	6	7	8	9	10	11	12	13	14	15
A(m)	4	5	7	9	12	13	15	17	20	22	25	28	32
Ref.	9	6	9		7		9						7

2. Proof of Theorem 1. Any positive integer s can be uniquely written in the form

$$(2.1) \qquad s = 2^{n_1} + 2^{n_2} + \ldots + 2^{n_\nu},$$

where $n_1 < n_2 < \ldots < n_\nu$ are non-negative integers. We put

$$S = \{n_1, n_2, \ldots, n_\nu\}$$

and write $s = (S)_2$. We then put $0 = (\emptyset)_2$, where $\emptyset$ is the empty set. Let $\alpha(s) = \nu$ for $s > 0$ and $\alpha(0) = 0$. For any two non-negative integers $s = (S)_2$ and $t = (T)_2$ we define $s \cap t = (S \cap T)_2$ and write $s \subset t$ if $S \subset T$. Now we prove the

LEMMA. Let $b_0, b_1, \ldots, b_n$ be a sequence of numbers and r an integer ≥ 0 such that $b_{s \cap r} = b_s$ for $s = 0, 1, 2, \ldots, n$. Then

$$\sum_{s \subset t} (-1)^{\alpha(s)} b_s = 0 \text{ if } t \not\subset r, \quad 1 \leq t \leq n.$$

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

Proof of the lemma. Since $t \not\subset r$ there are integers u and v, $u = 2^v$, such that $u \subset t$ but $u \not\subset r$. If $s \subset t - u$ then $(s+u) \cap r = s \cap r$ and so $b_{s+u} = b_s$ by the condition $b_{s\cap r} = b_s$. Since $\alpha(s+u) = \alpha(s) + 1$ we get

$$\sum_{s \subset t} (-1)^{\alpha(s)} b_s = \sum_{s \subset t-u} (-1)^{\alpha(s)} (b_s - b_{s+u}) = 0 ,$$

and the lemma is proved.

We shall define a class of matrices D_m with m rows $(m = 1, 2, \dots)$, such that if v_i $(i = 1, 2, \dots, n)$ are the columns in D_m then $\{v_1, v_2, \dots, v_n\}$ is a detecting set, $(M = \{0, 1\})$.

For any r in $1 \le r \le m$ let $d_1^{(r)}, d_2^{(r)}, \dots, d_h^{(r)}$ be a detecting set of integers with $1 \le d_j^{(r)} \le 2^{\alpha(r)-1}$, $j = 1, 2, \dots, h$, and $h = h^{(r)} \le h_k(2^{\alpha(r)-1})$. Since $\alpha(i)$ is an odd integer for $2^{\alpha(r)-1}$ integers i, $i \subset r$, we can determine $d_{ij}^{(r)} = 0$ or 1 for $i \subset r$ such that

$$(2.2) \qquad \sum_{i \subset r} (-1)^{\alpha(i)+1} d_{ij}^{(r)} = d_j^{(r)} , \quad d_{0j}^{(r)} = 0$$

$$\text{for } j = 1, 2, \dots, h^{(r)} .$$

For $i \not\subset r$ we then define $d_{ij}^{(r)} = d_{i\cap r, j}^{(r)}$ and find by the Lemma

$$(2.3) \qquad \sum_{i \subset t} (-1)^{\alpha(i)+1} d_{ij}^{(r)} = 0 \text{ for } r < t \le n .$$

Define a matrix $D_m^{(r)} = (d_{ij}^{(r)})$, $i = 1, 2, \dots, m$; $j = 1, 2, \dots, h^{(r)}$, and put $D_m = (D_m^{(1)}, D_m^{(2)}, \dots, D_m^{(m)})$. We shall prove that the

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

column vectors in D_m are a detecting set.

Let x_t and y_t $(t = 1, 2, \ldots, m)$ be column vectors of dimension $h^{(t)}$, with all components from the set $\{0, 1, 2, \ldots, k-1\}$. Suppose that

$$(2.4) \qquad \sum_{t=1}^{m} D_m^{(t)} x_t = \sum_{t=1}^{m} D_m^{(t)} y_t .$$

We shall prove $x_t = y_t$ for $t = 1, 2, \ldots, m$. If this is not true let r be the largest t for which $x_t \neq y_t$. If $r < m$ we subtract the terms with $t > r$ from both members of (2.4). This is allowed since $x_t = y_t$ for $t > r$. Then we multiply the i^{th} components in both members by $(-1)^{\alpha(i)+1}$ and add for all i with $i \subset r$. By (2.2) and (2.3), with t and r interchanged, we get

$$(2.5) \quad (d_1^{(r)}, d_2^{(r)}, \ldots, d_h^{(r)}) x_r = (d_1^{(r)}, d_2^{(r)}, \ldots, d_h^{(r)}) y_r .$$

The $d_j^{(r)}$ $(j = 1, 2, \ldots, h^{(r)})$ form a detecting set, hence $x_r = y_r$. But this contradicts the assumption, and we have proved that the column vectors in D_m form a detecting set.

If we choose $h^{(r)} = h_k(2^{\alpha(r)-1})$, we find by (1.4) for the number n of columns in D_m

$$n = \sum_{i=1}^{m} h_k(2^{\alpha(i)-1}) > \sum_{i=1}^{m} \frac{\alpha(i) - 1}{\log_2 k} = \frac{A(m) - m}{\log_2 k} .$$

The second inequality in Theorem 1 is proved. The first is proved similarly.

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

If we take $d_j^{(r)} = k^{j-1}$ we get a detecting set of the residue-class representing type. For in this case (2.5) implies $x_r = y_r$ even if the h^{th} components are allowed to take any integer value. It follows that the sums (1.1) of column vectors in D_m take different values even if m of the ε_i are allowed to take any integer value. This implies that the column vectors form a detecting set of the residue-class representing type.

Consider the case $k = 2$. The number of columns in D_m is $A(m)$. Those columns in D_m which generate Λ form a matrix $B_m = (b_{ij})$, where b_{ij} is given by the formula

$$(2.6) \qquad b_{ij} = \frac{1}{2}((-1)^{\alpha(i \cap j)+1} + 1), \quad i, j = 1, 2, \ldots, m .$$

We can prove that

$$(2.7) \qquad |\det B_m| = 2^{A(m)-m} .$$

Hence equality holds in (1.10).

In order to prove (2.7), we note that

$$(2.8) \qquad \sum_{i \subset m} (-1)^{\alpha(i)} b_{ij} = \begin{cases} 0 & \text{for } j < m , \\ -2^{\alpha(m)-1} & \text{for } j = m , \end{cases}$$

by (2.6) and our Lemma. Multiply the last row in B_m by $(-1)^{\alpha(m)}$ and add to this the i^{th} multiplied by $(-1)^{\alpha(i)}$, if $i \subset m$. We get

$$(-1)^{\alpha(m)}(\det B_m) = -2^{\alpha(m)-1}(\det B_{m-1}) ,$$

and then (2.7) easily follows.

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

3. Two examples.

Example 1. We shall illustrate the method in section 2 by proving that the columns in the matrix D_6 below form a detecting set, $(k = 2)$.

$$
\begin{array}{cc}
 & \begin{array}{cccccccccccc} r: & 1 & 2 & 1+2 & & 4 & 1+4 & & 2+4 & & i: & (-1)^{\alpha(i)+1} \end{array} \\
D_6 = & \left(\begin{array}{ccccccccc}
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}\right)
\begin{array}{cc}
1 & +1 \\
2 & +1 \\
1+2 & -1 \\
4 & +1 \\
1+4 & -1 \\
2+4 & -1
\end{array}
\end{array}
$$

The columns in D_6 are denoted $v_1, v_2, \ldots, v_9$. We shall prove that the sums $\sum_{i=1}^{9} \varepsilon_i v_i$, $\varepsilon_i = 0$ or 1, are all different.

Let $x_1, x_2, \ldots, x_9$ and $y_1, y_2, \ldots, y_9$ be 0 or 1.

Suppose that

$$\sum_{i=1}^{9} x_i v_i = \sum_{i=1}^{9} y_i v_i .$$

Take the "sum" of rows with $i \subset 2+4$: row 2 + row 4 - row(2+4). We get

$$x_8 + 2x_9 = y_8 + 2y_9$$

and conclude that $x_8 = y_8$ and $x_9 = y_9$. Next take the "sum" of rows with $i \subset 1+4$: row 1 + row 4 - row (1+4). We get $x_6 + 2x_7 = y_6 + 2y_7$ and conclude that $x_6 = y_6$ and $x_7 = y_7$.

Now we prove $x_5 = y_5$. The 4th row is

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

$x_5 + x_7 + x_9 = y_5 + y_7 + y_9$. We have already proved $x_7 = y_7$ and $x_9 = y_9$. It follows $x_5 = y_5$. Etc.

Example 2. $k = 2$, $m = 6$, $M = \{0, 1\}$. The maximum value of determinants of order 6 with all entries 0 or 1 is 9. The following matrix with determinant = 9 can be found[1)]

$$D = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

We triangulate D by the operations: (i) add a multiple of one column to another column, (ii) two columns change places, (iii) the elements in a column are multiplied by -1. Then we get the following matrix:

$$D' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & -2 & -6 & -5 & -5 & 9 \end{pmatrix}.$$

The columns in D and D' generate the same sublattice Λ in $\mathcal{K}$. Observe that the sums $\varepsilon_1 + 2\varepsilon_2 + 5\varepsilon_3$, $\varepsilon_i = 0$ or 1, are incongruent modulo 9. Then the following column vectors are incongruent modulo Λ :

---

1) cf. J. Williamson, Determinants whose elements are 0 and 1, Amer. Math. Monthly 53 (1946), 427-434.

$$\begin{pmatrix}0\\0\\0\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\\0\end{pmatrix}.$$

These vectors and those in D form a detecting set of the residue-class representing type.

4. Proof of Theorem 2. First assume that $M = \{0, 1\}$. Put $f_k(n) = m$. Then $n > F_k(m-1) > (A(m-1) - m + 1)/\log_2 k$ by Theorem 1. The function $\log x/x$ is decreasing for $x > e$. Then we find for n sufficiently large

$$(4.1) \qquad \frac{f_k(n)\log_k n}{n} < \frac{m\log_2 A(m-1)}{A(m-1)-m+1} .$$

Let $n \to \infty$. Then, by (1.2), $m \to \infty$. It follows by (4.1) and (1.7)

$$(4.2) \qquad \limsup_{n\to\infty} \frac{f_k(n)\log_k n}{n} \le 2 .$$

In order to prove (4.2) for an arbitrary M, we observe that if $\{v_1, v_2, \ldots, v_n\}$, $v_i = (a_{i1}, a_{i2}, \ldots, a_{im})$, is detecting, then also $\{v'_1, v'_2, \ldots, v'_n\}$, $v'_i = (ca_{i1}+b, ca_{i2}+b, \ldots, ca_{im}+b, b)$, $c \neq 0$, is detecting. Let $a, b \in M$, $a \neq b$. Put $c = a-b$. If the vectors v_i have all components in $\{0, 1\}$, then the vectors v'_i have all components from M. The immediate conclusion is that $f_k(n)$ cannot increase by more than 1 (the vectors v'_i are $(m+1)$-dimensional) at the transition from $\{0, 1\}$ to M. Thus (4.2) holds in the general case.

Next we want to prove

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

(4.3) $$\liminf_{n\to\infty} \frac{f_k(n)\log_k n}{n} \geq 2 .$$

The inequality (1.8) implies

$$\frac{f_k(n)\log_k n}{n} \geq \frac{2}{1 + O(1/\log n)} .$$

Now we shall prove (1.8) by the method of L. Moser.

Let $\{v_1, v_2, \ldots, v_n\}$ be a detecting set with $v_i = (a_{i1}, a_{i2}, \ldots, a_{im})$ and all components from the set M. Let a denote the maximum of absolute values of the elements in M.

Put

$$\sum_{i=1}^{n} a_{ij}\varepsilon_i = x_j \quad \text{for } j = 1, 2, \ldots, m .$$

The k^n vectors

$$(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{n} \varepsilon_i v_i , \quad (\varepsilon_i = 0, 1, 2, \ldots, k-1) ,$$

are all distinct. Now we define the mean value operator E by

$$E = k^{-n} \sum_{\varepsilon_1=0}^{k-1} \sum_{\varepsilon_2=0}^{k-1} \cdots \sum_{\varepsilon_n=0}^{k-1} , \text{ and put } \operatorname{Var} x = E(x - Ex)^2 .$$

By simple calculations one can prove

$$E\,\varepsilon_i = \frac{1}{2}(k-1) \text{ and } \operatorname{Var}\varepsilon_i = (k^2-1)/12 .$$

If we observe that

https://doi.org/10.4153/CMB-1965-034-2 Published online by Cambridge University Press

$$\operatorname{Var} x_j = \sum_{i=1}^{n} a_{ij}^2 \operatorname{Var} \varepsilon_i < k^2 a^2 n/12 ,$$

we find

$$\sum_{j=1}^{m} E(2x_j - 2Ex_j)^2 < (1/3)k^2a^2mn .$$

Hence, there are at least $\frac{1}{2}k^n$ vectors $(x_1, x_2, \ldots, x_m)$ for which

$$\sum_{j=1}^{m} (2x_j - 2Ex_j)^2 < (2/3)k^2a^2mn .$$

Since x_j and $2Ex_j$ are integers, we conclude that the inequality

$$\sum_{j=1}^{m} y_j^2 < (2/3)k^2a^2mn = R^2$$

has at least $\frac{1}{2}k^n$ integer solutions. We can find an upper bound for the number of solutions, if we calculate the volume of an m-dimensional sphere with radius R: $(C_1R^2/m)^{m/2} = (C_2ka)^m n^{m/2}$ for suitable constants C_1 and C_2. (1.8) follows immediately.

REFERENCES

1. R. Bellman and H.N. Shapiro, On a problem in additive number theory, Ann. Math. (2) 49 (1948), 333-340.

2. D.G. Cantor, Determining a set from the cardinalities of its intersections with other sets, Canad. J. Math. 16 (1964), 94-97.

3. G. F. Clements and B. Lindström, A sequence of (± 1)-determinants with large values, Proc. Amer. Math. Soc. June 1965.

4. P. Erdös, Problems and results in additive number theory, Colloque sur la théorie des nombres, Bruxelles (1955), 127-137.

5. P. Erdös and A. Rényi, On two problems of information theory, Publ. Hung. Acad. Sci. 8 (1963), 241-254.

6. N. J. Fine, Solution El 399, Amer. Math. Monthly 67 (1960), 697.

7. B. Lindström, On a combinatory detection problem, Publ. Hung. Acad. Sci. 9 (1964), 195-207.

8. H. S. Shapiro, Problem El 399, Amer. Math. Monthly 67 (1960) 82.

9. S. Söderberg and H. S. Shapiro, A combinatory detection problem, Amer. Math. Monthly 70 (1963), 1066-1070.

University of Stockholm