JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 64B, No. 1, January-March 1960

The Minimum of a Certain Linear Form [1]

Karl Goldberg

(March 23, 1959)

The positive minimum of the integral linear form $L(x_1, \ldots, x_n)=a_1x_1+ \ldots +a_nx_n$ is found subject to the conditions $a_i>0$ and $L(x_1, \ldots, x_n)\geq 2a_ix_i$ for $i=1,2, \ldots, n$.

Let $a_1 \leq a_2 \leq \ldots \leq a_n$ be $n\geq 3$ positive integers. We seek the positive minimum M of the linear form

$$L(x_1,x_2, \ldots ,x_n)=a_1x_1+a_2x_2+ \ldots +a_nx_n$$

over all non-negative integers $x_1, x_2, \ldots, x_n$ such that

$$L(x_1,x_2, \ldots, x_n)\geq 2a_ix_i \tag{1}$$

for all $i=1, 2, \ldots, n$.

Let $[a_1,a_2]$ denote the least common multiple of a_1 and a_2.

For each $i=3, 4, \ldots, n$, define r_i in the following way: If either a_1 or a_2 divides a_i, or if $a_i=a_j$ for some $j\neq i$, set $r_i=0$. Otherwise, let r_i be the minimum of the least non-negative residues modulo a_1 of

$$a_2-a_i,\ 2a_2-a_i,\ \ldots,\ [(a_i-1)/a_2]a_2-a_i.$$

We shall prove

THEOREM: *M is the minimum of* $2[a_1,a_2]$, $2a_3+r_3$, $2a_4+r_4, \ldots, 2a_n+r_n$.

As a consequence we have the inequality

$$2a_3+a_1-1\geq M\geq 2a_2.$$

Also, if $L(x_1,x_2, \ldots, x_n)=M$, then at most three of the x_k are positive. At least two must be positive. If exactly two are positive, then either $x_1=[a_1,a_2]/a_1$ and $x_2=[a_1,a_2]/a_2$, or $x_1=a_i/a_1$ and $x_i=1$, or $x_2=a_i/a_2$ and $x_i=1$, or $x_i=x_j=1$ for some $j>i\geq 3$. If three of the x_k are positive, then both x_1 and x_2 are positive; the other positive x_i equals 1 and we have $x_1=-[(a_2x_2-a_i)/a_1]$ for that i. Under any conditions M is achieved only with $x_i\leq 1$ for all $i\geq 3$. We shall prove all this.

M. Newman [2] refers to our theorem in the case $n=3$. We shall treat this case first.

We have $a_1\leq a_2\leq a_3$, and we want to find the positive minimum M of the linear form

$$L(x_1,x_2,x_3)=a_1x_1+a_2x_2+a_3x_3$$

over all non-negative integers x_1, x_2, x_3 satisfying

$$L(x_1,x_2,x_3)\geq 2a_ix_i \qquad i=1,2,3. \tag{2}$$

Let $x_1'=-[(a_2-a_3)/a_1]$. Because $a_2\leq a_3$, x_1' is non-negative. It satisfies

$$a_1-1\geq a_2-a_3+a_1x_1'\geq 0. \tag{3}$$

Because $a_1\leq a_2$, this implies

$$a_3\geq a_3-(a_2-a_1)-1\geq a_1x_1'. \tag{4}$$

Now consider $L(x_1',1,1)=a_1x_1'+a_2+a_3$. From (3) we have

$$2a_3+a_1-1\geq L(x_1',1,1)\geq 2a_3. \tag{5}$$

We know that $2a_3\geq 2a_2$, so that $L(x_1',1,1)\geq 2a_3\geq 2a_2$. Finally, (4) yields $L(x_1',1,1)\geq 2a_3\geq 2a_1x_1'$.

This proves that $x_1=x_1'$, $x_2=x_3=1$ satisfies (2). It follows that the left-hand inequality in (5) holds for M:

$$2a_3+a_1-1\geq M. \tag{6}$$

From this point we assume that x_1, x_2, x_3 satisfy (2) and

$$L(x_1,x_2,x_3)=M.$$

Since $L(x_1,x_2,x_3)\geq 2a_3x_3$, we have from (6) and $a_3\geq a_1$ that $x_3=0$ or $x_3=1$.

If $x_3=0$, than (2) implies $a_1x_1=a_2x_2$. Under this condition the minimum value of $L(x_1,x_2,x_3)$ is $2[a_1,a_2]$, occurring for $x_1=[a_1,a_2]/a_1$ and $x_2=[a_1,a_2]/a_2$.

From now on $x_3=1$. From $M=a_1x_1+a_2x_2+a_3$ and (2), we have $M\geq 2a_3$. From (6) we have

$$2a_3+a_1-1\geq 2a_3+a_1x_1+(a_2x_2-a_3),$$

from which it follows that $x_1>0$ implies $a_3-1\geq a_2x_2$. If $x_1=0$, then (2) implies $a_2x_2=a_3x_3$, so that $M=2[a_2,a_3]$.

[1] The preparation of this paper was supported in part by the Office of Naval Research.

[2] M. Newman, Construction and application of a class of modular functions, II, Proc. London Math. Soc. **9**, 373 (1959).

But $2[a_2,a_3]>2a_3+a_1-1$ unless a_2 divides a_3. Thus $x_1=0$ is possible only if a_2 divides a_3, in which case $x_2=a_3/a_2$ and $M=2a_3$. Similarly $x_2=0$ is possible only if a_1 divides a_3, in which case $x_1=a_3/a_1$ and $M=2a_3$. Since a_3 divisible by either a_1 or a_2 leads to $M=2a_3$ which is the best possible result with $x_3=1$, we may now assume that neither a_1 nor a_2 divides a_3 and that $x_1x_2>0$.

With $x_1>0$ we must have $a_3-1\geq a_2x_2$. Fix x_2. We shall find that permissible value of x_1 which minimizes $L(x_1,x_2,x_3)=a_1x_1+a_2x_2+a_3$. Clearly this is the least positive value of x_1 satisfying (2). We have

$$L(x_1,x_2,x_3)=a_1x_1+1+(a_3-1-a_2x_2)+2a_2x_2>2a_2x_2$$

for any value of x_1. The other inequalities require

$$\frac{a_3+a_2x_2}{a_1}\geq x_1\geq\frac{a_3-a_2x_2}{a_1}.$$

Since $2a_2x_2\geq 2a_2>a_1$, there are values of x_1 satisfying these inequalities. The least such x_1 is the least integer greater than or equal to $(a_3-a_2x_2)/a_1$. This last quantity is positive, so this value of x_1 is positive. It can be written

$$x_1''=-\left[\frac{a_2x_2-a_3}{a_1}\right].$$

Let $r_3(x_2)$ be the least non-negative residue modulo a_1 of $a_2x_2-a_3$. Then $r_3(x_2)=a_2x_2-a_3+a_1x_1''$. It follows that

$$L(x_1'',x_2,1)=2a_3+r_3(x_2).$$

We want the least of these values for x_2 lying between 1 and $[(a_3-1)/a_2]$. Under our assumptions on the divisibility of a_3, this is just $2a_3+r_3$ with r_3 as defined in the theorem. This proves the theorem for $n=3$.

Now assume $n>3$. We have $a_1\leq a_2\leq\ \ldots\ \leq a_n$, and we want to find the positive minimum M of the linear form $L(x_1,x_2,\ \ldots,\ x_n)$ over all non-negative integers $x_1,x_2,\ \ldots,\ x_n$ satisfying (1).

If x_1,x_2,x_3 satisfy (2), then $x_1,x_2,x_3,\ 0,\ \ldots,\ 0$ satisfy (1). Therefore our new M satisfies (6). Let

$$L(x_1,x_2,\ \ldots,\ x_n)=M.$$

Then

$$2a_3+a_1-1\geq a_1x_1+a_2x_2+a_3x_3+\ \ldots\ +a_nx_n$$
$$\geq a_1(x_1+x_2)+a_3(x_3+\ \ldots\ +x_n).$$

It follows that

$$x_3+x_4+\ \ldots\ +x_n\leq 2$$

and that $x_3+x_4+\ \ldots\ +x_n=2$ requires $x_1+x_2=0$. On the other hand,

$$3a_i>2a_3+a_1-1\geq L(x_1,x_2,\ \ldots,\ x_n)\geq 2a_ix_i,\quad i=3,4,\ \ldots,\ n,$$

implies

$$x_i\leq 1,\qquad i=3,4,\ \ldots,\ n.$$

Assume $x_3+x_4+\ \ldots\ +x_n=2$. Then $x_i=x_j=1$ for some $i,j\geq 3$ and all other $x_k=0$. Then (1) implies $a_i=a_j$ and $M=2a_i$. Again this is the best possible result with $x_i=1$.

If $x_3+x_4+\ \ldots\ +x_n=0$, then (1) implies $a_1x_1=a_2x_2$. As before, this implies $M=2[a_1,a_2]$.

If $x_3+x_4+\ \ldots\ +x_n=1$, then $x_i=1$ for some $i\geq 3$ and all other $x_k=0$ for $k\geq 3$. The problem then reverts to the case $n=3$ with a_i replacing a_3. Our previous arguments complete the proof of the theorem, and the statements in the subsequent paragraph.

WASHINGTON, D.C. (Paper 64B1-20)