Problem 2: Separating Functions

Team: Belarus

Abstract

In this paper the initial problem was considered and completely solved. The main method for it is using the formula, obtained in Theorem 2.3. Some estimations of F were obtained (see Proposition 2.4). We also introduced the algorythm for calculation the value of $F(a_1, \ldots, a_n)$ for arbitrary n (see page 4). Some steps towards simplification of calculation $F(a_1, a_2, a_3)$ were made (Theorem 1.5)

Definition: a positive integer is called *representable by a set X{ $a_1,a_2,a_3,\ldots\ldots,a_n$ }* if and only if it can be represented as a linear combination of nonnegative integers from the set *X*.

Proposition 2.1: for all *sets* $\{a_i\}$, where $gcd(a_1,a_2,a_3,\ldots\ldots,a_n)=1$ there exists a positive number $F(a_1,a_2,a_3,\ldots\ldots,a_n)$ such that for any integer $a \geq F(a_1,a_2,a_3,\ldots\ldots,a_n)$ we have $a \in S$

Proof: Since $\gcd(a_1,a_2,\ldots,a_n)=1$, $x_1a_1+x_2a_2+\ldots+x_na_n=1$ for some integers x_i

Denote by D and $-C$ the sum of positive and negative terms in this decomposition respectively. Remark that by definition $D - C = 1$.

Any nonnegative integer K can be represented as $ba_1 + t$, with $b \geq 0$ and $0 \leq t < a_1$. Thus, $(a_1\text{-}1)C + K = ba_1 + (a_1\text{-}1\text{-}t)C + tD$, and any integer not less than $(a_1 -1)C$ is representable by $\{a_1,a_2,\ldots\ldots,a_n\}$.

Proposition 2.2: $F(a_1,a_2)=(a_1\text{-}1)(a_2\text{-}1)$

Proof: Show that $(a_1 -1)(a_2 - 1) -1 = a_1a_2 - a_1 - a_2$ is not representable by $\{a_1, a_2\}$.

Really, suppose that $a_1a_2 - a_1 - a_2 = ka_1 + la_2$ for some $k,l \geq 0$, so $0 \leq l < a_1 - 1$ (otherwise $a_1a_2 - a_1 - a_2 < ka_1 + la_2$, contradiction)

$a_1a_2 - (k+1)a_1 - (l+1)a_2 = 0 \qquad (l+1)a_2 \equiv 0 \bmod a_1$

But $(a_1,a_2)=1$, so $l+1 \equiv 0 \bmod a_1$, and $0 < l+1 < a_1$, contradiction.

Thus $a_1a_2 - a_1 - a_2$ is not representable by $\{a_1, a_2\}$.

Assume $m= a_1a_2 - a_1 - a_2$

Show that $m+i$ is representable by $\{a_1, a_2\}$ for all integers $i \geq 1$. As $(a_1,a_2)=1$ there always exist two integers r_1 and r_2 $(0 \leq r_1 < a_2)$ such that $a_1r_1+a_2r_2=1$ (note that if r_1 and r_2 satisfy this equality, then $r_1\text{-}ta_2$ and r_2+ta_1 also satisfy it (for all $t \in Z$) so we can make r_1 satisfy the required inequalities) (multiply by i: $a_1(i*r_1)+a_2(i*r_2)=i$) then

$m+i= (a_2 -1 + i*r_1)*a_1 +(i*r_2-1)*a_2$

We may represent $m+i= v_1a_1+v_2a_2$ with $(0 \leq v_2 < a_1)$. (note that we can find required v_2 similarly as above)

Since $-i=m - v_1a_1-v_2a_2= (-v_1 -1)a_1 +(a_1 -1 -v_2)a_2$ is not representable (because it's negative), and as $a_1 -1 -v_2 \geq 0$ then $-v_1 -1 < 0$ (otherwise $-i \geq 0$) implying that $v_1 > -1$ and thus $v_1 \geq 0$. So $m+i$ is representable, since $v_1, v_2 \geq 0$.

Theorem 2.3: if $\gcd(a_1,a_2,a_3,,\ldots,a_{n-1})=d$ then

$F(a_1,a_2,a_3,\ldots\ldots,a_n)=d*F(a_1/d,a_2/d,\ldots, a_{n-1}/d,a_n) + F(d,a_n)$

Proof:

We need to show that $d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n) - 1$ is not representable as a linear combination of $a_1,a_2,a_3,\ldots\ldots,a_n$.

Assume the contrary. Suppose it's representable, i.e. $d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n)-1 = l_1*a_1+l_2*a_2+\ldots+l_{n-1}a_{n-1}+(d*l_n+k)a_n$.

Since $F(d,a_n)=d*a_n-d-a_n+1$ by Proposition 2.2, we obtain

$d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n) - 1= l_1*a_1 + l_2*a_2 +\ldots+ l_{n-1}a_{n-1} + (d*l_n + k)a_n= k*a_n + (l_1*a_1+l_2*a_2+\ldots+d*l_n*a_n)=$

$= d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + d*a_n-d-a_n$ (for some non-negative k, l_i, $1 \leq i \leq n$, $0 \leq k \leq d\text{-}1$)

$d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + d*a_n-d-a_n \equiv -a_n \bmod d$

$k*a_n + (l_1*a_1+l_2*a_2+\ldots+d*l_n*a_n) \equiv k*a_n \bmod d$, as $gcd(a_1,a_2,a_3,,\ldots,a_{n-1})=d$

As $0 \leq k \leq d\text{-}1$ *and as* $ka_n \equiv -a_n \bmod d$

$((k+1)a_n \equiv 0 \bmod d)$ *and as* $gcd(d,a_n)=1 \rightarrow \qquad k=d\text{-}1 \rightarrow$ substitude k:

So we need to represent $(l_1*a_1+l_2*a_2+\ldots+d*l_n*a_n) + d*a_n - a_n = d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + d*a_n-d-a_n$:

$d*(\ F(a_1/d, a_2/d, \ldots, a_{n-1}/d, a_n) - 1\ ) = d*(\ l_1*a_1/d + l_2*a_2/d + \ldots + l_n*a_n)$, that contradicts the definition of F . So $d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n) - 1$ is not representable by $\{a_1,a_2,a_3,\ldots\ldots,a_n\}$.

Show that numbers greater than $d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n) - 1$ are representable by $\{a_1,a_2,a_3,\ldots\ldots,a_n\}$.

Let $x = d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n) + k$, $k \geq 0$

Suppose $x \equiv y \bmod d$, consider p such that $pa_n \equiv y \bmod d$(we can do it because $gcd(a_n,d)=1$).

$0*a_n$, $1*a_n$,…, $(d-1)a_n$ give all residues modulo d, otherwise if $s*a_n \equiv t*a_n \bmod d$ *(for some integers s and t such that* $0 \leq s \leq d-1$ *and* $0 \leq t \leq d-1$ *and* $s \neq t$*)* $(s - t) \equiv 0 \bmod d$*, contradiction.*

Then:

$x = t*d + p*a_n$, $0 \leq p \leq d-1$, for some t

Show that $t \geq F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n)$:

$t*d + a_n*(d-1) \geq x = t*d + p*a_n = d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + d*a_n - d - a_n + k + 1 =$

$= d * F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) - d + a_n*(d-1) + (k+1) >$

$> d *(F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) - 1) + a_n*(d-1)$.

One can notice that $t > F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) - 1$, it means $t*d$ is representable as a linear combination of $a_1,a_2,a_3,\ldots\ldots,a_{n-1},d*a_n$.

Therefore every $x \geq d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d,a_n) + F(d,a_n)$ is representable by $\{a_1,a_2,a_3,\ldots\ldots,a_n\}$.

There are a lot of generalizations connected with this formula and solving particular tasks, of course:

3 a) Corollary: if 2 of 3 integers are even $(d=2*k)$, then

$F(2k*a_1,2k*a_2,a_3) = 2k * F(a_1,a_2,a_3) + F(2k,a_3) =$

$= 2k * F(a_1,a_2,a_3) + (a_3-1)*(2k-1)$ is also even.

b) Corollary 3.b: $d = gcd(a_1,a_2) \rightarrow F(a_1,a_2,a_3) = d* F(a_1/d,a_2/d,a_3) + F(d,a_3)$

Note that if $a_3 \geq F(a_1/d,a_2/d)$ *(it means* a_3 *is representable by* $\{ a_1/d,a_2/d \}$*)* , then $F(a_1/d,a_2/d,a_3) = F(a_1/d,a_2/d) \rightarrow$

Proved.

4) and 5) As $gcd(a_1,a_2,a_3,a_{n-1})=d \rightarrow$

by Theorem 2.3.

Corollary:→ if $n-1$ of n integers are even , then $F(a_1,a_2,a_3,\ldots\ldots,a_n)$ is also even.

Corollary: → if $n-1$ of n integers are multiple of d , then $F(a_1,a_2,a_3,\ldots\ldots,a_n) \equiv 1 - a_n \bmod d$

$F(a_1,a_2,a_3,\ldots\ldots,a_n) + a_n - 1$ is multiple of d

Corollary: if 2 of 3 integers are multiple of d, $gcd(a_1,a_2)=d$, then $F(a_1,a_2,a_3) + a_3 - 1$ is multiple of d.

Corollary: And if $a_n \geq F(a_1/d,a_2/d,\ldots,a_{n-1}/d)$ then

$F(a_1,a_2,a_3,\ldots\ldots,a_n) = d*F(a_1/d,a_2/d,\ldots,a_{n-1}/d) + F(d,a_n)$

Example of usage of formula:
$F(15,28,63)=7*F(15,4,9)+F(7,15)=7*(3*F(5,4,3)+F(3,4))+F(7,15)=189$

Proposition 2.4. if $gcd(a_1,a_2,\ldots,a_i)=d$ and $(i < n)$, then
$F(a_1,a_2,\ldots,a_n) \le d* F(a_1/d,a_2/d,\ldots,a_i/d) + F(d,a_{i+1},\ldots,a_n)$

Proof: All numbers multiple of d are representable starting from $d*F(a_1/d,a_2/d,\ldots,a_i/d)$ (they are representable by $\{ a_1,a_2,\ldots,a_i \}$), and all residues modulo d we can find starting from $F(d,a_{i+1},\ldots,a_n)$ (next part of proof is similar to proof of Theorem 2.3.),

Show that numbers greater than $d*F(a_1/d,a_2/d,\ldots,a_i/d) + F(d,a_{i+1},\ldots,a_n) - 1$ are representable by $\{a_1,a_2,a_3,\ldots\ldots,a_n\}$.

Let $x = d*F(a_1/d,a_2/d,\ldots,a_i/d) + F(d,a_{i+1},\ldots,a_n)+ s , \quad s \ge 0$

Denote $F(a_1/d,a_2/d,\ldots,a_i/d)$ by k;

Denote $F(d,a_{i+1},\ldots,a_n)+ s$ by t ;

So $x = kd + t$, as $t \ge F(d,a_{i+1},\ldots,a_n)$ so $t = ld + l_{i+1}a_{i+1} + \ldots + l_na_n$ for some non-negative integers $l , l_t \quad (i+1) \le t \le n$.

So $x = (k + l)d + l_{i+1}a_{i+1} + \ldots + l_na_n$ for some non-negative integers $l , l_t \quad (i+1) \le t \le n$.

$(k+l)d$ is representable by $\{ a_1,a_2,\ldots,a_i \}$, because $(k+l)d \ge kd$ and

$l_{i+1}a_{i+1} + \ldots + l_na_n$. So any $x \ge d*F(a_1/d,a_2/d,\ldots,a_i/d) + F(d,a_{i+1},\ldots,a_n)$ is representable by $\{a_1,a_2,a_3,\ldots\ldots,a_n\}$.

Therefore $F(a_1,a_2,\ldots,a_n) \le d* F(a_1/d,a_2/d,\ldots,a_i/d) + F(d,a_{i+1},\ldots,a_n)$.

The principle of finding $F(a_1,a_2,\ldots,a_n)$ in general case is such:

1. Determine the smallest number in the set $\{ a_1,a_2,\ldots,a_n \}$ (call it c)
2. Determine T such that $T \ge F(a_1,a_2,\ldots,a_n)$.

For example, if some $a_1,a_2,\ldots,a_n$ have *2* relatively prime numbers a_i and a_j, then $T=a_i*a_j -a_j -a_i +1=F(a_i,a_j) \ge F(a_1,a_2,\ldots,a_n)$ if there are none, then we can act the same way as in Proposition 2.1 ($T= (a_1 - 1)C$)) or use well-known facts about T(see below).

3. Construct all possible combinations of numbers $a_1,a_2,\ldots,a_n$ smaller than T.
4. For each q (q from 1 to c) to find the lowest b_q , such that $b_q \equiv q \bmod c$ among the constructed numbers.
5. $F(a_1,a_2,\ldots,a_n)= \max_{1 \le q \le a1-1} b_q - a_1+1$

Some Facts about T we found:

Erdos, Graham (1972):

$$F(a_1, a_2, \ldots, a_n) \le 2a_n\left[\frac{a-1}{n}\right] - a1+1$$

Vitek (1975):

$$2*F(a_1, a_2, \ldots, a_n) \le (a_2 - 1)(a_n - 2)$$

Selmer (1977):

$F(a1, a2, ..., an) \leq 2a_{n-1}\left[\frac{a\_n}{n}\right] - a_n + 1$

Beck, Diaz, Robins (2005):

$2*F(a_1, a_2, ..., a_n) \leq \sqrt{a_1 a_2 a_3 (a_1 + a_2 + a_3)} - a_1 - a_2 - a_3 + 2$

Rodseth (1978):

$F(a1, a2, ..., an) \geq \sqrt[n-1]{(n-1)!a1a2...an} - a_1 - a_2 - ... - a_n + 1$

Also we investigated the case n=3:

Say $A \notin (a,b,c)$ if A *is* not representable by $\{a,b,c\}$.

We simplified finding $F(a,b,c)$ $(a<b<c)$, so we just need represent c as in Lemma 1.1. and act by Theorem 1.5.

Make a, b, c pairwise coprime by Theorem 2.3. and Corollary 3.b.

Lemma 1.1 Given a relatively prime pair (a, b) and c not multiple of a and not multiple of b, c is of exactly one of the following forms: $c = ax + by$ *or* $c = ab - ax - by$, with $x, y > 0$.

Proof: Let u be a solution of the congruence $au \equiv c \bmod b$ so that $0 < u < b$. Then $c = au + bv$ for some $v \in Z$, and $v \neq 0$ *(otherwise c is multiple of a)*. If v is positive, then c has the form $ax + by$ with $x = u$ and $y = v$.

If v is negative, then $v = -y$ for $y > 0$, and so

$c = au + bv = ab - a(b - u) - by = ab - a(b - u) - by$

So $x = b - u$, and c is of the form $ab - ax - by$.

c is not simultaneously representable in both forms. If it were,

$ab - ax - by = ax_1 + by_1$, where $x, x_1, y, y_1 > 0$. So $ab = a(x + x_1) + b(y + y_1)$. Therefore $(y + y_1)$ is multiple of a, which is not possible, as $(y + y_1) < a$.(otherwise $ab < a(x + x_1) + b(y + y_1)$)

Corollary 1.2 Let a and b be relatively prime and c be a positive integer. Then $c \notin (a,b)$ if and only if $c = ab - ax - by$ for some integers $x, y > 0$.

Proof:

If $c \notin (a,b)$, c is not divisible by a or b, so $c = ab - ax - by$ for some integers $x, y > 0$ by Lemma 1.1. If $c = ab - ax - by$ for some integers $x, y > 0$, c is not multiple of a or b and $c \neq ax_1 + by_1$ by Lemma 1.1. So $c \notin (a,b)$.

Proposition 1.3 Let a and b be relatively prime and c be a positive integer. Then $F(a, b, c) = F(a, b)$ if and only if $c = ax + by$ for some $x, y \geq 0$.

Proof:

First note that $F(a, b, c) \leq F(a, b)$. Now assume $c = ax+by$ for some $x, y \geq 0$.

$F(a, b) - 1 = ua + vb + wc$ for some integers $u, v, w \geq 0$. But then

$F(a, b) - 1 = ua + vb + wc = ua + vb + w(ax + by) = (u + wx)a + (v + wy)b$, a contradiction.

So $F(a, b, c) = F(a, b)$. For the converse, suppose c not a linear combination of a and b. Then by Lemma 1.1, $c = ab - ax - by$ for some $x, y > 0$. Furthermore *by proposition 2.2* $F(a, b) - 1 = ab - a - b = ab - ax - by + ax - a + by - b = c + a(x - 1) + b(y - 1)$. *And* $x - 1, y - 1 \geq 0$, *so* $F(a, b, c) \leq F(a, b) - 1 < F(a, b)$. Thus $F(a, b, c) < F(a, b)$.

Proposition 1.4 Let a and b be relatively prime and c be a positive integer. Then $F(a,b,c)=F(a, b) - ax - by$ for some $x, y \geq 0$.

Proof: $F(a,b,c)$ is not representable as a linear combination of a and b, so $F(a,b) - 1 = ab-a-b \geq F(a, b, c) - 1 = ab - ax - by$ for some $x, y > 0$, and so $F(a, b, c) = ab - ax - by + 1 = F(a, b) + a + b - ax - by = F(a, b) - (x - 1)a - (y - 1)b$.

Theorem 1.5 Let a and b be relatively prime and c be any positive integer. Then

1. $c \in (a,b)$ *(including the case when c is multiple of a or b)* if and only if $F(a, b, c) = F(a, b)$

2. $c \notin (a,b)$ if and only if $c = ab - ax - by$ for some $x, y > 0$.

(a) if $ax < by$ and $0 < y \leq [a/2]$, then $F(a, b, c) = F(a, b) - ax$ можно избавиться от 2 условия?

(b) if $ax > by$ and $0 < x \leq [b/2]$, then $F(a, b, c) = F(a, b) - by$. Аналогично (a)

Proof: follows from Lemma 1.1:

1. if c is not multiple of a or b then the proof follows from Proposition 1.3, else if c is multiple of a or b, then w.l.o.g. c is multiple of a ($c=ka$),then $F(a,b,ka)=F(a,b)$, and vice-versa.

2. (a) if $ax < by$ and $0 < y \leq [a/2]$, then $F(a, b, c) = F(a, b) - ax$

Suppose $F(a, b, c) < F(a, b)-ax$. Then $F(a, b)-ax-1 = ra+sb+t(ab-ax-by)$ for some $r, s, t \geq 0$ where $c = ab-ax-by$. Note that $t > 0$, otherwise $F(a, b)-1 = (r+x)a+sb$, a contradiction.

Suppose t is even. Then $F(a, b) - 1 = (r + x + \frac{t}{2}(b - 2x))a + (s + \frac{t}{2}(a - 2y))b$. But $y \leq \frac{a}{2}$ and so $x \leq \frac{b}{2}$ since $ax < by$. Thus $F(a, b) - 1 \in (a,b)$, a contradiction.

Now suppose t is odd. Then

$$F(a, b) - 1 = (r + x + \frac{t-1}{2}(b - 2x))a + (s + \frac{t-1}{2}(a - 2y))b + \frac{1}{2}(b - 2x)a + \frac{1}{2}(a - 2y)b =$$

$$= (r + x + \frac{t-1}{2}(b - 2x))a + (s + \frac{t-1}{2}(a - 2y))b + c$$

Define f and g as follows:

$$f = r + x + \frac{t-1}{2}(b - 2x)$$

$$g = s + \frac{t-1}{2}(a - 2y)$$

So $c = ab - a - b - fa - gb = ab - (f + 1)a - (g + 1)b$

Therefore $f + 1 = x$ since $c = ab - ax - by$ uniquely. So

$$f + 1 - x = r + \frac{t-1}{2}(b - 2x) + 1 = 0,$$

a contradiction since $t > 0$ and $b \geq 2x$. Thus $F(a, b, c) \geq F(a, b) - ax$.

Suppose now that $F(a, b, c) > F(a, b) - ax$. By Proposition 1.4 $F(a, b, c) = F(a, b) - ra - sb$ for some $r, s \geq 0$. So $F(a, b) - ra - sb > F(a, b) - ax$, and so $ra + sb < ax$. Thus $r < x$ and since $ax < by$, $s < y$.
As $F(a, b) - ra - sb - 1$ is not representable with a,b,c, you can see
$F(a, b) - ra - sb - 1 = ab - a - b - ra - sb = ab - ax - by + ax + by - a - b - ra - sb =$
$= c + (x - r - 1)a + (y - s - 1)b.$
But $x - r - 1 \geq 0$, and $y - s - 1 \geq 0$, so $c + (x - r - 1)a + (y - s - 1)b \in (a,b,c)$, a contradiction. Thus $F(a, b, c) \leq F(a, b) - ax$, and so $F(a, b, c) = F(a, b) - ax$.

(b) is analogous (a).