7. An experiment

ITYM 2012, Team Croatia

June 30, 2012

Abstract

The central question of this task was to study the operator α. We easily found examples for the first three cases and also proved that from existence of one solution follows existence of an infinite number of solutions. In the first part we studied the existence of superbalanced sets. In the second part we came up with a different task, similar to the first one. So we took the initial 2-base and turned it into a n-base set (where n is an odd number). We weren't able to proove the existance of l-balanced set for each l.

1 Balanced n- tuples

Let l be a positive integer. Find the number of balanced $n-$tuples $X = (a_1, a_2, ..., a_n)$ in the set$(F_2)^n$ such that the n-tuples $\alpha(X), ..., \alpha^l(X)$are balanced as well. Start with $l = 1, 2, 3$.

We have found some balanced $4l$-tuples such that $\alpha(X), ..., \alpha^l(X)$ are balanced as well, and we know that if exists on tuple like that, there is an infinite number of them.

4 0011

8 00010111

12 000011010111

16 0000011010111011

20 00000011010110111011

So we have reasons to believe that for every natural number$l$, it is possible to construct balanced $4l$-tuple, such that $\alpha(X), ..., \alpha^l(X)$ are balanced as well, and that means that there is an infinite number of them.

Proof: Suppose we take a sequence $X = (a_1, a_2, ..., a_n)$ such that $\alpha(X), ..., \alpha^l(X)$ is balanced as well. Let us perform the following operation on the sequence X:

- begin with X;
- in the n-th step, concatenate X to the sequence obtained in the previous step.

We observe that the property of the initial sequence remains unchanged throughout the proccess. In this way, we can obtain an infinite number of sequences with the same property.

2 Superbalanced n- tuples

Do there exist superbalanced $n-$tuples? How many?

Definition **Cycle** X is a sequence that will eventually (after preforming several α-operations) repeat itself and be balanced all the way during the process.

And if such a sequence exists, then it will be a superbalanced sequence.

Let us assume that there is a superbalanced n-tuple. The number of diferent $n-$tuples is 2^n, so that means that there exists a cycle.

We name one n-tuple of that cycle X, and we know that it is also superbalanced.

Lenght of the cycle is B ($\alpha^B(X) = X$).

Let X be $(a_1, a_2, ..., a_n)$.

Proposition The sequence $\alpha^{2^k}(X)$ is equal to $(a_1 \oplus a_{[1+2^k]}, ..., a_n \oplus a_{[n+2^k]})$, where $[i]$ is the residue i modulo n (if n|i, then $[i] = n$). Conversely, if $\alpha^m(X)$ is of the form $(a_1 \oplus a_{1+2^k}, ..., a_n \oplus a_{n+2^k})$, then $m = 2^k$, for some $k \in \mathbb{N}$.

Proof by induction on k :

- first, we check for $k = 0$:

$$\alpha(X) = (a_1 \oplus a_2, ..., a_n \oplus a_1),$$

- let us assume that for a non-negative integer k, $\alpha^{2^k}(X)$ is equal to$(a_1 \oplus a_{[1+2^k]}, ..., a_n \oplus a_{[n+2^k]})$.
- we now use the above assumption. Define $b_m = a_m \oplus a_{[m+2^k]}$. Now rewrite the above sequence as $Y = (b_1, b_2, ..., b_n)$, and we have the following:

$$\begin{aligned}
\alpha^{2^k}(Y) &= (b_1 \oplus b_{[1+2^k]}, ..., b_n \oplus b_{[n+2^k]}) \\
&= \alpha^{2^{k+1}}(X) \\
&= (a_1 \oplus a_{[1+2^k]} \oplus a_{[1+2^k]} \oplus a_{[1+2^{k+1}]}, ..., a_n \oplus a_{[n+2^k]} \oplus a_{[n+2^k]} \oplus a_{[n+2^{k+1}]}) \\
&= (a_1 \oplus a_{[1+2^{k+1}]}, ..., a_n \oplus a_{[n+2^{k+1}]}).
\end{aligned}$$

Therefore, n can't be 2^k due to the fact that after 2^k changes we get a sequence of 0's.

After B changes we have $(a_1, a_2, ..., a_n)$. After one more change ($B + 1$ althogether) we have $(a_1 \oplus a_2, a_2 \oplus a_3, ..., a_n \oplus a_1)$. And after one more change (althogether B+2) we have $(a_1 \oplus a_3, ..., a_n \oplus a_2)$.

We see that $B+1 = 2^k$, and $B+2 = 2^m \Rightarrow 2^k \cdot (2^{m-k}-1) = 1$, so we conclude that $k = 0$, $m = 1$ and $B = 0$.

Therefore the cycle doesn't exist, and there are no superbalanced $n-$tuples.

3 $n-$tuples of residues mod p

We considered an $n-$tuple X=$(a_1, a_2, ..., a_n)$, where $a_1, a_2, ..., a_n$ are elements of the set of residues modululo p, for odd p. For X to be balanced, neccessary conditions are:

(i) length n of X must be $k \cdot p$

(ii) X must contain equal number of all residues.

Proposition If X is of the form $(0, 1, ..., p-1)$ or $(0, 1, ...p-1, 0, 1, .., p-1, 0, 1, ..., p-1)$, then X is superbalanced.

Sketch of proof It is easy to prove using induction that after 2^k changes, two numbers in X that are next to each other differ by residue 2^k modulo p.

In other words $a_{[i+1]} = a_{[i]} \oplus 2^k$ ($[i]$ is residue i modulo n where n is the lenght of X. Also, if $n|$i then $[i] = n$).

Because $gcd(2^k, p) = 1$, all residues will appear equal number of times.