Problem 5. «Curl27»

Bob is developing the 3OTA infrastructure and has designed a new hash function Curl27 for it. A distinguishing feature of the infrastructure is the ternary logic: trits from the set $\mathsf{T} = \{0, 1, -1\}$ are used instead of bits, ternary strings and words are used instead of binary ones. The Curl27 hash function is defined below. Its implementation in Java can be found here.

Find a collision for Curl27, that is, different ternary strings X and X' such that $\mathsf{Curl27}(X) = \mathsf{Curl27}(X')$. Submit colliding strings as two lines of trits separated by commas. An example of a (wrong!) solution is:

```
-1,1,0,1,1,0
-1,-1,1,0,1,1,-1,0
```

Description of Curl27. The Curl27 function maps a ternary string X of arbitrary length to a hash value from T^{243}. When hashing, an auxiliary sponge function Curl27-f: $\mathsf{T}^{729} \to \mathsf{T}^{729}$ is used. The hashing algorithm:

1. Pad X with zeros to make its length a multiple of 243. Divide the resulting string into blocks $X_1, X_2, \ldots, X_d \in \mathsf{T}^{243}$.
2. Prepare the state $W = W_0W_1W_2 \in \mathsf{T}^{729}$ consisting of words $W_i \in \mathsf{T}^{243}$. Initialize the state by filling W_0 and W_2 with zeros and W_1 with the encoded initial (before padding) length of X. The length is encoded by a ternary word according to the little-endian conventions: less significant trits go first. For example, the length $25 = 1 - 3^1 + 3^3$ is presented by the word $\underbrace{1\bar{1}01000\ldots0}_{243}$.

   Here $\bar{1}$ stands for -1.
3. For $i = 1, 2, \ldots, d$, do: $W_0 \leftarrow X_i$, $W \leftarrow \mathsf{Curl27\text{-}f}(W)$.
4. Return W_0.

Description of Curl27-f. In Curl27-f the S-box

$$S\colon \mathsf{T}^3 \to \mathsf{T}^3, \quad (a, b, c) \mapsto (F(a, b, c), F(b, c, a), F(c, a, b))$$

is used. Here

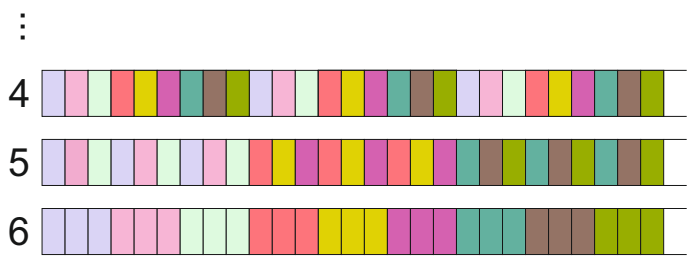
$$\begin{aligned} F(a, b, c) = {} & a^2b^2c + a^2bc^2 - ab^2c^2 + a^2b^2 - a^2bc + a^2c^2 + ab^2c \\ & - a^2c + ab^2 - ac^2 + b^2c + bc^2 - a^2 - b^2 + bc - c^2 - c + 1, \end{aligned}$$

where the calculations are carried out modulo 3 while the residue 2 is represented by the trit -1.

To transform the state W, 27 rounds are performed. A round consists of 6 steps. At each step triplets of trits of W are grouped in a certain way. Then each triplet (a, b, c) is replaced with $S(a, b, c)$.

Turn to the next page.

Groupings are organized as follows (see figure). At the first step, the state is divided into 3 words of 243 trits. Trits of these words in the same positions are grouped. In the second step, the state is divided into 9 words of 81 trits. Trits of the 1st, 2nd and 3rd words in the same positions are grouped, then trits of the 4th, 5th and 6th words, and so on. After that, the state is divided into words of length 27, then length 9, then length 3 while maintaining the logic of groupings. In the last sixth step, consecutive triplets of trits are grouped.



Groupings (3 last steps, grouped trits are painted the same color

Bonus problem (extra scores, a special prize!).

Find a collision when the state is initialized in a different way: now W_0, W_2 are not filled with zeros, the word $\underbrace{01\bar{1}01\bar{1}\ldots01\bar{1}}_{243}$ is written in each of them instead.