Problem 4. «An infinite set of collisions»

Bob is very interested in blockchain technology, so he decided to create his own system. He started with the construction of a hash function. His first idea for a hash function was the function H with a hash value of length 16.

It works as follows.

- Let $u_1, u_2, \ldots, u_n \in \mathbb{F}_2$ be a data representation, n is arbitrary.
- Bob calculates $z^0, \ldots, z^n \in \mathbb{F}_2^{32}$, $z^0 = (0, \ldots, 0)$, and z^{i+1} is obtained from z^i in the following way:

$$z' = \begin{cases} (z_1^i, z_2^i, \ldots, z_{16}^i, z_1^i \oplus z_{17}^i, z_2^i \oplus z_{18}^i \ldots, z_{16}^i \oplus z_{32}^i) & \text{if } u_i = 1, \\ (z_1^i \oplus z_{17}^i, z_2^i \oplus z_{18}^i, \ldots, z_{16}^i \oplus z_{32}^i, z_{17}^i, z_{18}^i, \ldots, z_{32}^i) & \text{if } u_i = 0, \end{cases}$$

$$z'' = \begin{cases} z' & \text{if } u_i \neq z'_{32}, \\ (z'_1 \oplus 1, z'_2 \oplus 1, \ldots, z'_{32} \oplus 1) & \text{if } u_i = z'_{32}, \end{cases}$$

$$z^{i+1} = (z''_2, z''_3, \ldots, z''_{32}, u_i).$$

- Finally, $H(u_1, \ldots, u_n) = (z_1^n \oplus z_{17}^n, z_2^n \oplus z_{18}^n, \ldots, z_{16}^n \oplus z_{32}^n)$.

But then Bob found out that his hash function is weak for using in cryptographic applications. Prove that Bob was right by constructing an infinite set $C \subset \bigcup_{n=1}^{\infty} \mathbb{F}_2^n$ such that all elements of C have the same hash value H.

An example. Let us calculate $H(0, 1, 0)$:

$$\begin{aligned} z^1 &= (\underbrace{1, 1, \ldots, 1}_{31}, 0), \\ z^2 &= (\underbrace{0, \ldots, 0}_{15}, \underbrace{1, \ldots, 1}_{15}, 0, 1), \\ z^3 &= (\underbrace{1, \ldots, 1}_{13}, 0, 0, \underbrace{1, \ldots, 1}_{14}, 0, 1, 0), \\ H(0, 1, 0) &= (\underbrace{0, \ldots, 0}_{14}, 1, 1). \end{aligned}$$