Problem 6. «Studying Feistel schemes»

The classical Feistel scheme and its generalizations are widely used to construct iterated block ciphers. **Generalized Feistel schemes** (GFS) usually divide a message into m subblocks and applies the (classical) Feistel transformation for a fixed number of two subblocks, and then performs a cyclic shift of m subblocks.

Trudy wants to compare algebraic properties of different generalizations of the Feistel scheme based on shift registers over an arbitrary finite commutative ring with identity. For studying, she chooses a nonlinear feedback shift register (NLFSR), Type-II GFS and Target-Heavy (TH) GFS. She wants to decide whether or not these transformations belong to the **alternating group** (that is the group of all even permutations). Trudy needs your help!

Let us give necessary notions. By $A(X)$ we denote the alternating group on a set X. Let t be a positive integer, $t \geqslant 1$, $(R, +, \cdot)$ be a commutative ring with identity 1, $|R| = 2^t$. The characteristic $\mathrm{char}(R)$ of R is equal to 2^c for some $c \in \{1, ..., t\}$. In many block ciphers, we have

$$R \in \left\{\mathbb{Z}_2^t,\ \mathbb{Z}_{2^t},\ \mathbf{GF}(2^t)\right\},\ \mathrm{char}(\mathbb{Z}_{2^t}) = 2^t,\ \mathrm{char}\left(\mathbb{Z}_2^t\right) = \mathrm{char}\left(\mathbf{GF}(2^t)\right) = 2.$$

Q1 NLFSR. Let $\ell \geqslant 1$, $m = 2^\ell$, $h : R^{m-1} \to R$. Consider a mapping $g_{k,h}^{(\mathrm{NLSFR})} : R^m \to R^m$ defined by

$$g_{k,h}^{(\mathrm{NLSFR})} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_2, \alpha_3, ...,\ \alpha_{m-1}, \alpha_m, \alpha_1 + h(\alpha_2, ..., \alpha_m) + k)$$

for all $(\alpha_1, ..., \alpha_m) \in R^m$, $k \in R$. Describe all positive integers $t \geqslant 1$, $\ell, c \geqslant 1$ and a mapping $h : R^{m-1} \to R$ such that $g_{k,h}^{(\mathrm{NLSFR})} \in A(R^m)$ for any $k \in R$. Prove your answer!

Q2 Type-II GFS. Let $\ell \geqslant 2$, $m = 2^\ell$, $h = (h_1, ..., h_{m/2})$, where $h_i : R \to R$ for $1 \leqslant i \leqslant m/2$. Consider a mapping $g_{k,h}^{(\mathrm{GFS-II})} : R^m \to R^m$ defined by

$$g_{k,h}^{(\mathrm{GFS-II})} : (\alpha_1, ..., \alpha_m) \mapsto\ (\alpha_2 + h_1(\alpha_1) + k_1, \alpha_3, \alpha_4 + h_2(\alpha_3) + k_2, \alpha_5, ..., \alpha_{m-1}, \alpha_m + h_{m/2}(\alpha_{m-1}) + k_{m/2}, \alpha_1)$$

for all $(\alpha_1, ..., \alpha_m) \in R^m$, $k = (k_1, ..., k_{m/2}) \in R^{m/2}$. Describe all positive integers $t \geqslant 2$, $\ell, c \geqslant 1$ and mappings $h_1, ..., h_{m/2}$ such that $g_{k,h}^{(\mathrm{GFS-II})} \in A(R^m)$ for any $k \in R^{m/2}$. Prove your answer!

Q3 TH-GFS Let $\ell \geqslant 2$, $m = 2^\ell$, $h = (h_2, ..., h_m)$, where $h_i : R \to R$ for $2 \leqslant i \leqslant m$. Consider a mapping $g_{k,h}^{(\mathrm{TH})} : R^m \to R^m$ defined by

$$g_{k,h}^{(\mathrm{TH})} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_2 + h_2(\alpha_1) + k_2, \alpha_3 + h_3(\alpha_1) + k_3, ..., \alpha_{m-1} + h_{m-1}(\alpha_1) + k_{m-1}, \alpha_m + h_m(\alpha_1) + k_m, \alpha_1)$$

for all $k = (k_2, ..., k_m) \in R^{m-1}$. Describe all positive integers $t \geqslant 2$, $\ell, c \geqslant 1$ and mappings $h_2, ..., h_m$ such that $g_{k,h}^{(\mathrm{TH})} \in A(R^m)$ for any $k \in R^{m-1}$. Prove your answer!