Problem 4. «Orthomorphisms»

A young cryptographer Bob wants to build a new block cipher based on the Lai-Massey scheme. The Lai-Massey scheme depends on a finite group G with the neutral element e and an orthomorphism of G. Bob decides to use a nonabelian group and chooses a dihedral group D_{2^m}, $m \geqslant 4$, generated by a, u with presentation

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u.$$

Let θ be a permutation of a finite group G. Then θ is called an **orthomorphism of** G if the mapping $\pi : \alpha \mapsto \alpha^{-1}\theta(\alpha)$ is a permutation of G.

Bob needs to construct an orthomorphism of D_{2^m}. He considers the set DM_m consisting of all mappings $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$ on D_{2^m} given by

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i + c_1} & \text{if } i \in \{0, \ldots, 2^{m-2}-1\}, \\ a^{r_2 i + c_2}u & \text{if } i \in \{2^{m-2}, \ldots, 2^{m-1}-1\}, \end{cases}$$

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i + b_1}u, & \text{if } i \in \{0, \ldots, 2^{m-2}-1\}, \\ a^{q_2 i + b_2}, & \text{if } i \in \{2^{m-2}, \ldots, 2^{m-1}-1\}, \end{cases}$$

and depending on $b_i, c_i, r_i, q_i \in \{0, \ldots, 2^{m-1}-1\}$ for $i \in \{1, 2\}$, where the operations addition and multiplication are over the residue ring $\mathbb{Z}_{2^{m-1}}$.

Q1 Let $m = 4$. Help Bob to describe all orthomorphisms of DM_m and find their number.

Q2 For each $m \geqslant 4$, help Bob to describe all orthomorphisms of DM_m, i. e. give necessary and sufficient conditions on b_i, c_i, r_i, q_i for $i \in \{1, 2\}$ such that $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$ is an orthomorphism of D_{2^m}.