# Moufang loops of order coprime to three that cyclically extend groups of dihedral type

Aleš Drápal

*Abstract.* This paper completely solves the isomorphism problem for Moufang loops $Q = GC$ where $G \trianglelefteq Q$ is a noncommutative group with cyclic subgroup of index two and $|Z(G)| \leq 2$, $C$ is cyclic, $G \cap C = 1$, and $Q$ is finite of order coprime to three.

*Keywords:* dihedral group; Moufang loop; cyclic extension; semidirect product

*Classification:* 20N05

## 1. Introduction

Gagola [4] proved that for Moufang loops of order coprime to three it is possible to define a semidirect product by a single formula if the factor over the normal subloop is a cyclic group. This might turn out to be, after further generalizations, a decisive tool in enhancing our knowledge of constructions of Moufang loops. The formula can be presented as

$$(x, b^i) \cdot (y, b^j) = (f^{2i+j}(f^{-2i-j}(x) \cdot f^{i-j}(y)), b^{i+j}), \tag{1.1}$$

where $f$ is a semiautomorphism of a Moufang loop $S$. Denote the arising loop by $S \rtimes_f^3 C$ where $C = \langle b \rangle$. If $f$ and $C = \langle b \rangle$ are given then (1.1) may not define an operation upon $S \times C$. However, if the operation is well defined then (1.1) yields a loop, and $(1, 1)$ is its neutral element.

If $Q = SC$, $S \cap C = 1$, $S \trianglelefteq Q$, and $C$ is finite, cyclic, and of order coprime to three then $Q \cong S \rtimes_f^3 C$ for some $f$. However, the formula (1.1) does not give a Moufang loop for every semiautomorphism $f$. The necessary conditions for the loop to be Moufang have been described in [3]. These conditions simplify considerably when $S = G$ is assumed to be a group.

The purpose of this paper is to classify completely the isomorphism classes in a situation when $G$ is a finite noncommutative group with a normal cyclic subgroup of index two such that $|Z(G)| \in \{1, 2\}$. The case $G \cong Q_8$ is treated separately in Section 7. Assume $G \not\cong Q_8$. Then there exist $x, y \in G$ such that $G = \langle x, y \rangle$, $\langle y \rangle \trianglelefteq G$, $|G : \langle y \rangle| = 2$, and every semiautomorphism $f$ can be expressed as $f = f_s\alpha$, where $\alpha \in \operatorname{Aut} G$, $s \in \mathbb{Z}_n^*$, $n = |y|$, $f_s(y^i) = y^i$ and $f_s(xy^i) = xy^{is}$, for all $i \in \mathbb{Z}$.

DOI 10.14712/1213-7243.2015.187

However, not all semiautomorphisms $f$ yield a Moufang loop. By [3] one of the necessary conditions is that $s^2 \equiv 1 \bmod n$. In Section 2 further basic and structural properties of a Moufang loop $Q = G \rtimes_f^3 C$ are recapitulated and refined. Amongst others it is shown that both $s$ and $n = |y|$ are invariants of $G$.

The automorphisms $\alpha$ can be recorded as $\alpha_{t,r}$ where $y \mapsto y^r$ and $x \mapsto xy^t$. Further sections deal with the questions which properties of $r$ and $t$ provide isomorphism invariants, and how far the isomorphism type of $Q$ determines the isomorphism type of $G$.

The classification scheme that is unravelled is quite complex. To deal with it effectively there are introduced various notational conventions that appear in many statements throughout the paper. To make the paper accessible, the last section contains a guide to the classification that does not assume prior knowledge of these conventions.

Three levels of arguments are employed to solve the isomorphism problem. The first level which stretches over Sections 3 and 4 is concerned with the choice of a complement $C$ with $G$ fixed so that the parameters obtained are as simple as possible. This means that the given $b$ is replaced by $b^i y^j$ for some $i$ and $j$. The classification obtained appears in Theorems 5.1 and 5.2. The rest of the Section 5 corresponds to the second level of arguments. At this level $b$ may be also replaced by $bx$. This turns out to be technically quite complex since in $Q$ there may be no complement to $G$ that is generated by some $b^i xy^j$. The third level of arguments is concerned with the question whether the isomorphism type of $G$ is determined by the isomorphism type of $Q$ uniquely. That is true in most situations but not in all — which is a source of considerable difficulties. Nevertheless, the case when the order of $|C|$ is divisible by 4 allows for a classification that might be considered as relatively transparent (Theorems 6.1 and 6.2). On the other hand, the case of $|C|/2$ odd provides many isomorphisms for which it seems difficult to find a common principle. The eligible situations are described in Tables 1 and 2. The bigger part of Section 6 consists of *ad hoc* arguments that explain when an isomorphism occurs. The obtained results are formulated in Theorems 6.20 and 6.21. However, technical nature of arguments caused that these theorems are formulated in a way that uses not only the Tables 1 and 2 but also a number of definitions that have been made throughout the preceding text.

Sections 2–6 assume that $G$ is not equal to the group of quaternions. The case $G \cong Q_8$ is solved in Section 7.

If $Q$ is nonassociative and $C$ is finite then $C$ has to be of even order. This fact can be proved in many ways. For example, it follows from the characterization of the nucleus in Proposition 2.2. The case of $Q$ associative (i.e. the case of $Q$ a group) is considered throughout the classification efforts too but with the restriction that $C$, if finite, is assumed to be of an even order like in the nonassociative case. (Groups $Q$ such that $C$ is of an odd order are relatively easy to classify but they are regarded as being out of scope of this paper.) Furthermore, the associative case presents a certain ambiguity that pertains to the case $Q \cong (D_{2m} \rtimes \mathbb{Z}_h) \times \mathbb{Z}_4 \times \mathbb{Z}_2$ (cf. (2.7) and ensuing comments).

The only general tool that is available for isomorphism problems seems to be the following variant of Gagola's [4] theorem:

**Proposition 1.1.** *Let $Q$ be a loop, $C = \langle b \rangle$ a finite cyclic group, and $f$ a permutation of $Q$, $f(1) = 1$, such that the loop $Q \rtimes_f^3 C$ is well defined. For every $\alpha \in \operatorname{Aut} Q$ and $k \in \mathbb{Z}$, $\gcd(k, |C|) = 1$, the loop $Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$ is also well defined, and there exists an isomorphism $\Psi_{\alpha,k} \colon Q \rtimes_f^3 C \cong Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$, $(u, b^i) \mapsto (\alpha(u), b^{i\bar{k}})$, $k\bar{k} \equiv 1 \bmod |C|$. If $\Psi \colon Q \rtimes_f^3 C \cong Q \rtimes_g^3 C$ is such that $\Psi(Q \times 1) = Q \times 1$ and $\Psi(1 \times C) = 1 \times C$ then $\Psi = \Psi_{\alpha,k}$ for some $\alpha \in \operatorname{Aut} Q$ and $k \in \mathbb{Z}$, $\gcd(k, |C|) = 1$. In such a case $Q \rtimes_g^3 C = Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$.*

Proof: In $Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$ the product of $\Psi_{\alpha,k}(u, b^i) = (\alpha(u), b^{i\bar{k}})$ with $\Psi_{\alpha,k}(v, b^j) = (\alpha(v), b^{j\bar{k}})$ is equal if the loop is well defined, to

$$\Big( (\alpha f^{2i+j} \alpha^{-1}) \left( (\alpha f^{-2i-j} \alpha^{-1})(\alpha(u)) \cdot (\alpha f^{i-j} \alpha^{-1})(\alpha(v)) \right), b^{\bar{k}(i+j)} \Big)$$
$$= \Big( \alpha(f^{2i+j}(f^{-2i-j}(u) \cdot f^{i-j}(v))), b^{\bar{k}(i+j)} \Big) = \Psi_{\alpha,k}\left( (u, b^i) \cdot (v, b^j) \right).$$

On the other hand, if this equality holds for all $i, j \in \mathbb{Z}$ then the loop is well defined. Now, $Q \rtimes_f^3 C$ is well defined if and only if the result of (1.1) does not change whenever $i$ and $j$ are replaced by $i'$ and $j'$ such that $b^i = b^{i'}$ and $b^j = b^{j'}$. We assume that $Q \rtimes_f^3 C$ is well defined. Hence $Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$ is well defined as well, and $\Psi_{\alpha,k} \colon Q \rtimes_f^3 C \cong Q \rtimes^3_{\alpha f^k \alpha^{-1}} C$.

By the assumptions on $\Psi$ there exist $\alpha \in \operatorname{Aut} Q$ and $k, \bar{k} \in \mathbb{Z}^*_{|C|}$ such that $k\bar{k} \equiv 1 \bmod |C|$, $\Psi((u, 1)) = (\alpha(u), 1)$ and $\Psi((1, b)) = (1, b^{\bar{k}})$. This implies that $\Psi((u, b^i)) = (\alpha(u), b^{i\bar{k}}) = \Psi_{\alpha,k}(u, b^i)$, for all $u \in Q$ and $i \in \mathbb{Z}$. □

Section 6 of [3] investigates the situation when $G$ is a group and $G \rtimes_f^3 C$ a Moufang loop. The following facts are taken from Proposition 6.9 and Theorem 6.11.

**Proposition 1.2.** *Let $G$ be a group, $C$ a cyclic group and $f$ a semiautomorphism of $G$ such that $G \rtimes_f^3 C$ is a well defined Moufang loop. Define another group operation upon $G$ by $u * v = f^{-1}(f(u)f(v))$ for all $u, v \in G$. Then there exists an action $\mu$ of $G$ upon $G$ such that $\mu_v(uv) = u * v = \mu_u^{-1}(uv)$ and $\mu_u f = f \mu_{f^2(u)}$, for all $u, v \in G$.*

## 2. Structural subloops and some invariants

Let $Q = G \rtimes_f^3 C$ be a loop such that $f = f_s \alpha_{t,r}$, $C = \langle b \rangle$, and $G = \langle x, y;\ y^n = 1,\ x^2 = y^{n/\lambda},\ xyx^{-1} = y^{-1+n/\kappa} \rangle$ is a noncommutative group, $\lambda, \kappa \in \{1, 2\}$ and $G \not\cong Q_8$. The integer $n$ may be odd. However, it must be even if $\lambda = 2$ or $\kappa = 2$. Furthermore, if $\kappa = 2$, then $4 \mid n$.

There is $|Z(G)| \in \{1, 2, 4\}$, where $|Z(G)| = 4$ if and only if $\kappa = 2$, $4|n$, $n > 4$ and $8 \nmid n$. When the case $|Z(G)| = 4$ is omitted then the remaining groups $G$ may be described abstractly as finite noncommutative groups with $|Z(G)|$ dividing 2 that possess a cyclic subgroup of index two, the group of quaternions excepted.

Let $\alpha_{t,r}$ be the automorphism of $G$ such that $\alpha_{t,r}(x) = xy^t$, $t \in \kappa\mathbb{Z}_n$, and $\alpha_{t,r}(y) = y^r$, $r \in \mathbb{Z}_n^*$. Since we assume that $G$ is not isomorphic to the group of quaternions, there can be proved easily that each automorphism of $G$ can be expressed in this form. Note that

$$\alpha_{t,r}(x^\varepsilon y^i) = x^\varepsilon y^{\varepsilon t + ri} \text{ for all } \varepsilon \in \{0,1\} \text{ and } i \in \mathbb{Z}_n. \tag{2.1}$$

By $f_s$, $s \in \mathbb{Z}_n^*$, there will be denoted the semiautomorphism of $G$ that fixes $\langle y \rangle$ pointwise, and sends $xy^i$ to $xy^{si}$, $i \in \mathbb{Z}_n$. By [3, Theorem 8.5] the loop $Q = G \rtimes_f^3 C$ (if well defined) is Moufang if and only if

$$s^2 \equiv 1, \quad (s-1)(r^3+1) \equiv 0 \quad \text{and} \quad (s-1)t(r^2-r+1) \equiv 0 \bmod n. \tag{2.2}$$

Note that $s \equiv 1 \bmod n$ if and only if $Q$ is a group. If $C$ is infinite, then $G \rtimes_f^3 C$ is a well defined loop for any semiautomorphism $f$. If $C$ is finite, then it is well defined if and only if $|f|$ divides $3|C|$, by [3, Proposition 3.8]. In our case this is equivalent to

$$r^{6h} \equiv 1 \bmod n \text{ and } t(1+r+\cdots+r^{6h-1}) \equiv 0 \bmod n, \text{ where } |C| = 2h \tag{2.3}$$

since

$$(f_s\alpha_{t,r})^{6j} = \alpha_{t(1+r+\cdots+r^{6j-1}),r^j} \text{ for every } j \geq 0. \tag{2.4}$$

The latter fact follows from (2.2) and from the easily verifiable equalities

$$(f_s\alpha_{t,r})^2 = \alpha_{(s+r)t,r^2} \text{ and } (\alpha_{t,r})^i = \alpha_{t(1+r+\cdots+r^{i-1}),r^i}, \ i \geq 0. \tag{2.5}$$

Indeed, $ts(1+r^2+r^4) \equiv t(1+r^2+r^4) \bmod n$ by (2.2) as $r^4+r^2+1 = (r^2-r+1)(r^2+r+1)$. Thus if $j \equiv (r+s)(1+r^2+r^4) \bmod n$ then, by (2.5), $\alpha_{t(1+\cdots+r^5),r^6} = \alpha_{tj,r^6} = ((f_s\alpha_{t,r})^2)^3 = (f_s\alpha_{t,r})^6$.

If $Q$ is well defined (i.e. $C$ is infinite or (2.3) holds), then the operation of $Q$ can be described [3, Equation (8.6)] by

$$ub^i \cdot vb^j = \begin{cases} uf^{3i}(v) \cdot b^{i+j} & \text{if } j \text{ is even,} \\ f_s\left(f_s(u)f_sf^{3i}(v)\right)\right) \cdot b^{i+j} & \text{if } j \text{ is odd.} \end{cases} \tag{2.6}$$

This formula is to be interpreted in such a way that the elements of the semidirect product are written as $ub^i$ rather than $(u, b^i)$.

If $\kappa = 2$, the $n = |G|$ is divisible by 4, and $x$ and $xy$ have different orders. Hence it is always possible to choose $x$ in such a way that $\lambda = 1$ if $\kappa = 2$.

We shall assume that $|G| = n = 2^k m$, where $m$ is odd. Thus $k = v_2(n)$.

While $G$ is assumed to be noncommutative, there are cases when the 2-Sylow subgroups of $G$ are commutative:

**Lemma 2.1.** *A 2-Sylow subgroup of $G$ is commutative if and only if either $k \le 1$, or $k = \kappa = 2$. In the latter case $Z(G) = \{y^{im};\ 0 \le i \le 3\}$. For all other groups $G$ either $Z(G) = 1$ and $k = 0$, or $Z(G) = \{1, y^{n/2}\}$ and $k \ge 1$.*

If $Q$ is a loop, then the *associator subloop* is defined as the least normal subloop $A$ such that $Q/A$ is a group. The *nucleus* of $Q$ consists of all elements $a$ such that $x \cdot yz = xy \cdot z$ whenever $a \in \{x, y, z\}$.

From here on we shall assume that $Q = G \rtimes_f^3 C$ is a well defined Moufang loop. The structure of the nucleus $N = N(Q)$ and of the associator subloop $A = A(Q)$ is described in [3, Corollary 8.7] and [3, Proposition 8.12]:

**Proposition 2.2.** *If $s \not\equiv 1 \bmod n$, then $N = \{y^i b^{2j};\ i(s-1) \equiv 0 \bmod n\}$ and $A = \langle y^{s-1} \rangle$. The inclusion $A \le N$ holds if and only if $2(s-1) \equiv 0 \bmod n$. The loop $Q$ is a group if and only if $s \equiv 1 \bmod n$.*

The next statement works with condition $s \equiv 1 \bmod 2^k$. Note that this condition is always satisfied when $k \le 1$.

**Proposition 2.3.** *If $s \equiv 1 \bmod 2^k$ and $s \not\equiv 1 \bmod n$, then $Q/AN = \langle xAN, bAN \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $y^m \in N$. If $s \not\equiv 1 \bmod 2^k$, then $Q/AN = \langle xAN, yAN, bAN \rangle$ is of order 8. In such a case $Q/AN \cong \mathbb{Z}_2^3$ when $t$ is even, and $Q \cong D_8$ if $t$ is odd.*

Proof: By Proposition 2.2, $AN \le \langle y \rangle \langle b^2 \rangle$. Therefore none of $x$, $b$ and $bx$ belongs to $AN$. Furthermore, $y^2 = y^{1-s} y^{1+s} \in AN$ and $b^2 \in N$. Hence the question is when $y \in AN$. If $k = 0$, then $\langle y^2 \rangle = \langle y \rangle$. Assume $k \ge 1$. Then $s$ is odd, and $y \in AN$ if and only if $y^m \in AN$. If $s \equiv 1 \bmod 2^k$, then $m(s-1) \equiv 0 \bmod n$, and so $y^m \in N$. Assume that $s \not\equiv 1 \bmod 2^k$. Then $k \ge 2$. If $k = 2$, then $s \equiv 3 \bmod 4$. If $k \ge 3$, then either $s \equiv 2^{k-1} + 1 \bmod 2^k$, or $s \equiv -1 \bmod 2^{k-1}$. In all these cases $A \le \langle y^2 \rangle$, by Proposition 2.2. Since $G \cap N \le \langle y^2 \rangle$, there is never $y \in AN$ if $s \not\equiv 1 \bmod 2^k$. The rest is easy. □

**Lemma 2.4.** *Assume $k \ge 1$. Then $A \le \langle y^2 \rangle$. Furthermore, $Q/\langle y^2 \rangle$ is abelian if and only if $t$ is even.*

Proof: We have $y^{s-1} \in \langle y^2 \rangle$ since $s - 1$ has to be even. It is clear that $[x, y], [y, b] \in \langle y^2 \rangle$, while $[x, b] \in \langle y^2 \rangle$ if and only if $t$ is even. □

The following statement is an immediate consequence of the fact that $b^2 \in N$. In [3] it appears as Lemma 8.8.

**Lemma 2.5.** *It is true that $\langle y, b^2 \rangle \trianglelefteq Q$, that $Q/\langle y, b^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and that all three intermediate subloops $\langle x, y, b^2 \rangle = \langle G, b^2 \rangle$, $\langle y, b \rangle$ and $\langle xb, y, b^2 \rangle$ are groups.*

**Corollary 2.6.** *$Q' \le \langle y \rangle$. If $k \ge 1$ and $t$ is even, then $Q' \le \langle y^2 \rangle$.*

Proof: Loops $Q/G$ and $Q/\langle y, b^2 \rangle$ are abelian groups, by the construction of $Q$ and by Lemma 2.5. Clearly $G \cap \langle y, b^2 \rangle = \langle y \rangle$. If $t$ is even and $k \ge 1$, then $y \notin Q'$ by Lemma 2.4. □

If $\lambda = 1$ (i.e. $x^2 = 1$), then $G$ contains a subgroup $G_m = \langle x, y^{2^k} \rangle$ of order $2m$. If 2-Sylow subgroups of $G$ are commutative (cf. Lemma 2.1), then $G_m$ is noncommutative. If $v_2(t) \geq k$, then $G_m \trianglelefteq Q$, and $Q_m = G_m \rtimes_g^3 C$ is a (normal) subloop of $Q$ (where $g$ is the restriction of $f$ to $G_m$).

**Lemma 2.7.** *If $k \geq 1$, then $y^{n/2} \in Z(Q)$. If $k = 1$, $\lambda = 1$ and $t$ is even, then $Q \cong Q_m \times \langle y^m \rangle$. If $k = 2 = \kappa$, then $y^m \in Z(Q)$ if and only if $s \equiv r \equiv 1 \bmod 4$. If $k = 2 = \kappa$, $4 \mid t$ and $s \equiv r \equiv 1 \bmod 4$, then $Q \cong Q_m \times \langle y^m \rangle$.*

Proof: If $k \geq 1$, then $y^{n/2}$ has to be central since, clearly, $\{1, y^{n/2}\} \trianglelefteq Q$. That makes obvious the case of $k = 1$, $\lambda = 1$ and $t$ even. Suppose that $k = 2 = \kappa$. Then $y^m \in N$ if and only if $s \equiv 1 \bmod 4$, by Proposition 2.2, and $y^m$ commutes with $b$ if and only if $r \equiv 1 \bmod 4$, by (2.6). Thus $y^m \in Z(Q)$ if and only if $s \equiv r \equiv 1 \bmod 4$. The rest is easy. □

**Proposition 2.8.** *The derived subloop $Q'$ is equal to $\langle y \rangle$ if and only if $n$ or $t$ are odd. If $k = 2 = \kappa$, $4 \mid t$ and $s \equiv r \equiv 1 \bmod 4$, then $Q' = \langle y^4 \rangle$. In all other cases $Q' = \langle y^2 \rangle$.*

Proof: We have $y^{-1}y^x = y^{-2+n/\kappa}$. Thus $y^2 \in Q'$ unless $k = 2 = \kappa$. Hence $Q' = \langle y \rangle$ if $k = 0$, by Corollary 2.6. Assume that $k = 2 = \kappa$. Then $t$ is even, $(G_m)' = \langle y^4 \rangle$, and $y^{n/2} = [y^m, b]$ if $r \equiv 3 \bmod 4$. If $4 \nmid t$, then $\langle [x, b], y^4 \rangle = \langle y^2 \rangle$. Thus $Q' = \langle y^2 \rangle$ if $r \equiv 3 \bmod 4$ or if $v_2(t) = 1$, while $Q' = \langle y^4 \rangle$ if $s \equiv r \equiv 1 \bmod 4$ and $4 \mid t$, by Lemma 2.7.

The only remaining case with $k = 2 = \kappa$ is that of $s \equiv 3 \bmod 4$, $r \equiv 1 \bmod 4$ and $v_2(t) \geq 2$. Then $[xy, b^{-1}] \in \langle y^2 \rangle \setminus \langle y^4 \rangle$, and so $Q' = \langle y^2 \rangle$, by Corollary 2.6.

Suppose now that $k \geq 1$ and that $\kappa = 1$ if $k = 2$. We have already established that, then $y^2 \in Q'$. By considering $x^{-1}bxb^{-1}$ we see that $y \in Q'$ if $t$ is odd. Suppose that $t$ is even. Then $Q' = \langle y^2 \rangle$ by Corollary 2.6. □

Put $\mathbb{Z}_0 = \mathbb{Z}$. Every finitely generated abelian group is isomorphic to a group $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_\ell}$, where $d_i \geq 2$ or $d_i = 0$, and $d_{i+1}$ divides $d_i$, $1 \leq i < \ell$. The sequence $(d_1, \ldots, d_\ell)$ is determined by the abelian group uniquely. Let us call $\ell$ the *rank* of the group. The groups $\mathbb{Z}_{d_i}$ are the *factors*.

**Proposition 2.9.** *Suppose that $s \not\equiv 1 \bmod n$. The rank of $Q/Q'$ is equal to 2 if and only if $Q' = \langle y \rangle$. In all other cases the rank of $Q/Q'$ is equal to 3. If this is true, then $k = 2 = \kappa$, $4 \mid t$ and $s \equiv r \equiv 1 \bmod 2^k$ take place if and only if (a) there exist two factors of $Q/Q'$ of order different from 2, or (b) there exist two factors of $Q/Q'$ that are of order 2, one factor of finite order $j$, $v_2(j) = 2$, and $Q'Z(Q)/Q'$ contains an element of order 4.*

Proof: The group $Q/Q'$ is generated by $xQ'$, $yQ'$ and $bQ'$. The order of $xQ'$ is 2, and the order of $bQ'$ is infinite or even. In any case $|b| = |bQ'|$. The order of $yQ'$ is 1, 2 or 4, and $Q' \leq \langle y \rangle$, by Proposition 2.8. Hence the rank of $Q/Q'$ is two if and only if $y \in Q'$, and is equal to three in all other cases.

Suppose that $y \notin Q'$. Our goal is to distinguish the case when $|yQ'| = 4$ from the case when $y^2 \in Q'$. In the latter case there always exist two factors of order two, and hence that is what we may assume. Let $j$ be the order of the third factor. If $v_2(j) \neq 2$, then $|yQ'| \neq 4$, and $y^2 \in Q'$. Assume that $v_2(j) = 2$. Then

$|yQ'| = 4$ if and only if $|b|$ is finite and $|b|/2$ is odd. If this is true, then $n = 4m$ and $Z(Q) \geq \langle y^m \rangle$, by Lemma 2.7, and thus $y^m Q' \in Q'Z(Q)/Q'$ is an element of order 4.

On the other hand, if $y^2 \in Q'$, then the assumptions on the structure of factors imply that $|b| = j$ (where $v_2(j) = 2$). Every element of $Q'Z(Q)$ can be expressed as $y^i b^\ell$ since $Q'Z(Q) \leq Q'N \subseteq \{y^i b^{2\ell};\ i, \ell \in \mathbb{Z}\}$. Since $(y^i b^{2\ell})^2 \in \langle y^2 \rangle$, none of elements of $Q'Z(Q)/Q'$ can be of order 4. □

The purpose of this paper is to solve the isomorphism problem. It may happen that $Q = \tilde{G} \rtimes^3_{\tilde{f}} \tilde{C}$ where $\tilde{G}$ is again a noncommutative group with a cyclic subgroup of index two, $\tilde{G} \not\cong Q_8$. This will be called an *alternative expression of* $Q$. We are asking about the relationship of $G$, $C$ and $f$ to $\tilde{G}$, $\tilde{C}$ and $\tilde{f}$. A property or structure will be called *invariant* if it is the same for all alternative expressions.

Any information about $G$ that can be derived from the structure of $Q$ is necessarily invariant. Propositions 2.8 and 2.9 thus immediately give the following consequence:

**Corollary 2.10.** *If $s \not\equiv 1 \bmod n$, then orders of $G$ and $C$ are invariant.*

Let us assume that $Q$ is a group. Then there exist cases when Corollary 2.10 fails. However, they can be easily described, as will be demonstrated now. The initial arguments of Proposition 2.9 remain true. Thus we may assume that $Q$ has a form with parameters $\kappa = 2 = k$, $4|t$ and $s \equiv r \equiv 1 \bmod 4$, by Proposition 2.8. Thus $Q \cong Q_m \times \langle y^m \rangle$ and $|y^m| = 4$, by Lemma 2.7. Furthermore, $Q_m \cong D_{2m} \rtimes \mathbb{Z}_{2h}$ since $s = 1$. The arguments of Proposition 2.9 can fail only at the very end of the proof, where it is assumed that $Q' = \langle y^2 \rangle$ and $|b| = 4\ell$, $\ell$ odd. The existence of an element of order 4 in $Q'Z(Q)/Q'$ implies that $y^i b^\ell \in Z(Q)$ for some $i \in \mathbb{Z}$, and that gives $b^\ell \in Z(Q)$. From $Q \cong Q_m \times \mathbb{Z}_4$ it follows that $v_2(|Q|) \geq 4$, and so in the present setting (i.e. the setting with $Q' = \langle y^2 \rangle$) the group $\langle y \rangle$ contains a central involution that is not in $\langle b^\ell \rangle$. Thus $Q_m$ contains a nontrivial central involution. In the present setting $|G : Q'| = 4$ while in the former setting $|G : Q'| = 8$. Hence $|b| = 4h$, and $h = \ell$ is odd. The existence of central involution within $Q_m$ implies that $Q_m \cong (D_{2m} \rtimes \mathbb{Z}_h) \times \mathbb{Z}_2$. Therefore

$$Q \cong (D_{2m} \rtimes \mathbb{Z}_h) \times \mathbb{Z}_4 \times \mathbb{Z}_2 \text{ where } m \text{ and } h \text{ are odd.} \tag{2.7}$$

This is the only case when Corollary 2.10 fails for $Q$ associative. Throughout the paper we accept the fact that it may appear in the classification at two different places. However, in the overview of Section 8 the situation of (2.7) is classified by giving preference to the interpretation with $k = 1$.

If $Q$ is infinite, then $G$ consists of all elements of finite order. Hence $G$ is invariant if $Q$ is infinite. If $Q$ is finite, then even the isomorphism type of $G$ need not be invariant. Our next aim is to prove that the value of $s$ is invariant. We shall need [3, Lemma 8.11]:

**Lemma 2.11.** *Let $u, v \in Q$ be such such that $\{u, v\}$ is not a subset of any of the groups $\langle y, b \rangle$, $\langle x, y, b^2 \rangle$ and $\langle xb, y, b^2 \rangle$. Then $L_{u,v}(y^i b^{2j}) = y^{si} b^{2j}$ for all $i, j \in \mathbb{Z}$.*

The centralizer $C_Q(A) = \{u \in Q;\ uy^{s-1} = y^{s-1}u\}$ contains $A$, and hence it is a normal subloop of $Q$.

**Lemma 2.12.** *If $2(s-1) \equiv 0 \bmod n$, then $C_Q(A) = Q$. If $2(s-1) \not\equiv 0 \bmod n$, then $C_Q(A) = \langle y, b^2\rangle$.*

Proof: If $2(s-1) \equiv 0 \bmod n$, then $A = 1$ or $A = \{1, y^{n/2}\} \le Z(Q)$. Then $C_Q(A) = Q$. Suppose that $2(s-1) \not\equiv 0 \bmod n$. By (2.6), (2.4) and (2.2), $b^2y^{s-1} = y^{r^6(s-1)}b^2 = y^{r^3(1-s)}b^2 = y^{s-1}b^2$. Therefore $\langle y, b^2\rangle \le C_Q(A)$. By Lemma 2.5 to prove the converse we need to show that none of $x$, $b$ and $xb$ commutes with $y^{s-1}$. Note that $xy^{s-1}x^{-1} = y^{1-s}$ in all cases since $s-1$ is even when $\kappa = 2$. However, $y^{s-1} \neq y^{1-s}$, unless $2(s-1) \equiv 0 \bmod n$. Similarly, $by^{s-1} = y^{r^3(s-1)}b = y^{1-s}b \neq y^{s-1}b$ and $xb \cdot y^{s-1} = xy^{1-s} \cdot b \neq xy^{s-1} \cdot b = y^{s-1} \cdot xb$ if $2(s-1) \not\equiv 0 \bmod n$. □

**Lemma 2.13.** *The value of $s$ modulo $m$ is always invariant. The value of $s$ modulo $n$ is invariant in all cases with the possible exception of situations when $C$ is finite, $k \ge 3$ and $s \equiv -1 \bmod 2^{k-1}$.*

Proof: We can assume that $2(s-1) \not\equiv 0 \bmod n$, by Lemma 2.12. The left inner mappings of $Q$ induce only one nontrivial automorphism of $C_Q(A)$, by Lemmas 2.11 and 2.12. This automorphism is thus invariant. It sends $y^ib^{2j}$ to $y^{si}b^{2j}$. This gives $s$ immediately when $\langle y\rangle$ is invariant — which is always the case when $Q$ is infinite. In general, $\langle y^{2^k}\rangle$ is known to be invariant, by Proposition 2.8, and that gives the value of $s$ modulo $m$. The case when $s \equiv 1 \bmod 2^k$ can be recognized by Proposition 2.3. For $k = 2$ there is either $s \equiv 1 \bmod 4$ or $s \equiv 3 \bmod 4$, and so $k \ge 3$ can be assumed. From $A = \langle y^{s-1}\rangle$ we see that 4 divides $|A|$ if and only if $s \equiv -1 \bmod 2^{k-1}$. Since $s \equiv \pm 1 \bmod 2^{k-1}$ is always true, there is nothing more to prove. □

To treat the exceptional cases of Lemma 2.13 we shall need the following statement:

**Lemma 2.14.** *Let $\tilde G \rtimes^3_f \tilde C$ be an alternative expression of $Q$, where $|G : Q'| \le 2$. Let $\tilde y \in \tilde G$ be of order $n$. If $k = 0$ or $t$ is odd or $Q$ is infinite, then $\langle \tilde y\rangle = \langle y\rangle$. Suppose that $C$ is finite, that $2(s-1) \not\equiv 0 \bmod n$ and that $zyz = y^{\bar r}$, where $z$ is the (only) involution of $C$. If $\tilde y \notin \langle y\rangle$ and $k \ge 2$, then $\tilde y \in \langle y^2, z\rangle$, $\bar r \equiv 1 \bmod 4$, $|C|/2$ is even, and $\bar r \equiv 1 \mod 2^k$ if $s \equiv -1 \bmod 2^{k-1}$.*

Proof: If $k = 0$ or $t$ is odd or $Q$ is infinite, then $\langle y\rangle$ is invariant, by Proposition 2.8 and by the fact that $G$ is invariant when $Q$ is infinite. In these cases we must have $\tilde y \in \langle y\rangle$. Suppose that $\tilde y \notin \langle y\rangle$, $k \ge 2$, $2(s-1) \not\equiv 0 \bmod n$ and $|C| = 2h$. By Lemma 2.12, $\tilde y = y^ib^{2j}$ for some $i, j \in \mathbb{Z}$. Now, $i$ is odd since $\tilde y \notin Q'N$, and $b^{2j} = z$ since $\tilde y^2 \in \langle y^2\rangle$. Therefore $\langle \tilde y\rangle = \langle yz, y^2\rangle$ and $h$ is even. Clearly $zyz = y^{\bar r}$ for some $\bar r \in \mathbb{Z}$ such that $\bar r^2 \equiv 1 \bmod n$. Since $h$ is even, $\bar r = r^{3h}$ is an even power of $r$. Thus $\bar r \equiv 1 \bmod 4$. Finally, suppose that $s \equiv -1 \bmod 2^{k-1}$ and $k \ge 3$. Then $r \equiv -1 \bmod 2^{k-1}$ by (2.2), and so $r^2 \equiv \bar r \equiv 1 \bmod 2^k$. □

**Proposition 2.15.** *The value of $s$ modulo $n$ is invariant.*

Proof: Let $\tilde{G} \rtimes_{\tilde{f}}^{3} \tilde{C}$ be an alternative expression of $Q$. If $\tilde{y} \in \langle y \rangle$, then $\tilde{s} \equiv s \bmod n$ by Lemma 2.11. Assume that $\tilde{y} \notin \langle y \rangle$. By Lemmas 2.13 and 2.14 we may also assume that $Q$ is finite, $k \geq 3$, $t$ is even, $2(s-1) \not\equiv 0 \bmod n$ and $s \equiv -1 \bmod 2^{k-1}$. By Proposition 2.8, $|G : Q'| = 2$. By Lemma 2.14, $y^m$ and $z$ commute since $\bar{r} \equiv 1 \bmod 2^k$. Hence $(y^{im}z)^s = y^{ims}z$ for every odd $i \in \mathbb{Z}$. By Lemma 2.14 there exists an odd $i$ such that $\tilde{y}^m = y^{im}z$. Therefore any nontrivial action of a left inner mapping upon $C_Q(A)$ sends $\tilde{y}^m$ to $\tilde{y}^{ms}$, and thus $s \equiv \tilde{s} \bmod 2^k$. By Lemma 2.13, $s \equiv \tilde{s} \bmod m$, and we are done. □

The case of $C$ infinite seems to be relatively easy to handle. However, at this point there do not seem to be many reasons why to classify infinite Moufang loops. From here on it will be assumed that $C$ is finite of order $2h$.

## 3. Invariants for fixed components

In this section, we shall analyze situations when $G = \tilde{G}$ and $C = \tilde{C}$. By Proposition 1.1 this is equivalent to studying $G \rtimes_{\tilde{f}}^{3} C$ where $\tilde{f} = \alpha f^j \alpha^{-1}$, $j \in \mathbb{Z}_{2h}^*$ and $\alpha = \alpha_{q,p} \in \operatorname{Aut} G$.

The following statement can be verified by a direct computation,

**Lemma 3.1.** *If $\alpha = \alpha_{q,p} \in \operatorname{Aut} G$ and $\tau \in \mathbb{Z}_n$ is such that $p\tau \equiv t + q(r-s) \bmod n$, then $(f_s\alpha_{t,r})^\alpha = f_s\alpha_{\tau,r}$.*

**Corollary 3.2.** *Sets $\{f^\alpha;\ \alpha \in \operatorname{Aut} G\}$ and $\{f_s\alpha_{\tau,r};\ \tau \in t\mathbb{Z}_n^* + \kappa(r-s)\mathbb{Z}_n\}$ are equal.*

This makes clear why the ensuing auxiliary result will be useful.

**Lemma 3.3.** *Let $n > 1$ be an integer. If $\alpha, \beta \in \{1, \dots, n\}$, then $\alpha\mathbb{Z}_n^* + \beta\mathbb{Z}_n = \tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n$, where $\sigma = \gcd(\beta, n)$ and $\tau = \gcd(\alpha, \sigma)$.*

*If $\tau'|\sigma'$, $\sigma'|n$ and $1 \leq \tau' \leq \sigma' \leq n$, then $\tau'\mathbb{Z}_n^* + \sigma'\mathbb{Z}_n = \tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n$ if and only if $\tau = \tau'$ and, for every prime $p$, $p|\sigma$ if and only if $p|\sigma'$.*

Proof: If $m|n$, then, in some cases within this proof, we shall treat $\mathbb{Z}_m$ as the subset $\{0, 1, \dots, m-1\}$ of $\mathbb{Z}_n$. The proof consists of several steps.

(3.1) There exist $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$ such that $x\alpha + y\beta \equiv \gcd(\alpha, \beta) \bmod n$.

It suffices to find $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$ with $x\alpha + y\beta \in \gcd(\alpha, \beta)\mathbb{Z}_n^*$. By CRT (the Chinese Remainder Theorem) this needs to be proved only when $n$ is a power of a prime $p$. In such a case set $x = 1$ and $y = 0$ if $v_p(\alpha) \leq v_p(\beta)$, and $x = 1 = y$ if $v_p(\alpha) > v_p(\beta)$.

$$\alpha\mathbb{Z}_n^* + \beta\mathbb{Z}_n = \tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n. \tag{3.2}$$

Choose $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$ in such a way that $\tau = \alpha x + \sigma y$, and note that $\beta\mathbb{Z}_n = \sigma\mathbb{Z}_n$. Clearly $\tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n \subseteq \alpha\mathbb{Z}_n^* + \beta\mathbb{Z}_n$. The converse inclusion follows from $\alpha \in \tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n$.

(3.3) If $n = md$ and $\gamma \in \mathbb{Z}_m^*$, then $\gamma + xm \in \mathbb{Z}_n^*$ for some $x \in \{0, 1, \dots, d-1\}$.

Find the least $m'|n$ such that $m|m'$, $n = m'd'$ and $\gcd(m', d') = 1$. Then $d'|d$, $\mathbb{Z}_m^* \subseteq \mathbb{Z}_{m'}^*$, and $\gamma + xm' \in \mathbb{Z}_n^*$ for some $x \in \{0, 1, \dots, d'-1\}$ by the CRT (note that $m' = md/d'$).

$$\tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n = \tau\left(\mathbb{Z}_{n/\tau}^* + (\sigma/\tau)\mathbb{Z}_{n/\tau}\right). \tag{3.4}$$

Put $m = n/\tau$. Then $\tau\mathbb{Z}_n = \tau\mathbb{Z}_m$ and $\sigma\mathbb{Z}_n = \sigma\mathbb{Z}_m$. Using (3.3) we see that $\tau\mathbb{Z}_n^* = \tau\mathbb{Z}_m^*$.

To characterize $\tau\mathbb{Z}_n^* + \sigma\mathbb{Z}_n$ it thus suffices, by (3.4), to characterize $\mathbb{Z}_m^* + d\mathbb{Z}_m$ for every $d|m$. What is needed is to show that such a set is determined only by prime divisors of $d$. If $i \in \mathbb{Z}_m^* + d\mathbb{Z}_m$, then $\gcd(i, d) = 1$. On the other hand, if $i \in \{1, \dots, n\}$ satisfies $\gcd(i, d) = 1$, then $i = jd + \gamma$ for some $j \geq 0$ and $\gamma \in \mathbb{Z}_d^*$. In such a case $i \in \mathbb{Z}_m^* + d\mathbb{Z}_m$, by (3.3). □

For every $a \in \mathbb{Z}_n^*$ denote by $\operatorname{ord}_n(a)$ the order of $a$ in the group $\mathbb{Z}_n^*$.

**Lemma 3.4.** *If* $\operatorname{ord}_n(r)$ *is coprime to* 3, *then* $(s-1)(r+1) \equiv 3t(s-1) \equiv 0 \bmod n$. *If* $|f|$ *is coprime to* 3, *then* $\operatorname{ord}_n(r)$ *is coprime to* 3, $t(s-1) \equiv 0 \bmod n$ *and* $(f_s\alpha_{t,r})^j = (f_s)^j\alpha_{t(1+\cdots+r^{j-1}),r^j}$ *for every* $j \geq 0$.

Proof: By (2.2), $(s-1)r^{6j} \equiv s-1 \bmod n$ and $(s-1)r^{6j+3} \equiv 1-s \bmod n$, for every $j \in \mathbb{Z}$. Thus $2(s-1) \equiv 0 \bmod n$ if $\operatorname{ord}_n(r)$ is odd. Let $\operatorname{ord}_n(r)$ be coprime to 3. Then $r = r^{3i}$ for some $i \in \mathbb{Z}$. If $i$ is even, then $\operatorname{ord}_n(r)$ is odd. Hence $(s-1)r \equiv 1-s \bmod n$ in every case. Therefore $(s-1)t(r^2-r+1) \equiv 3(s-1)t \bmod n$, and so $3(s-1)t \equiv 0 \bmod n$, by (2.2).

Let $|f|$ be coprime to 3. Then there exist a semiautomorphism $g$ and an odd integer $i$ such that $g^3 = f$ and $f^i = g$. The semiautomorphism $g$ is equal to $f_s\alpha_{\tau,\rho}$ for some $\rho \in \mathbb{Z}_n^*$ and $\tau \in \mathbb{Z}_n$ such that $\rho^3 \equiv r \bmod n$ and $r^i \equiv \rho \bmod n$, by (2.5). Hence $\operatorname{ord}_n(r) = \operatorname{ord}_n(\rho)$ is coprime to three. By the previous part of the proof $(s-1)(r+1) \equiv 0 \bmod n$. Hence $(s-1)(\rho+1) \equiv 0 \bmod n$ as well. Since $\tau \in t\mathbb{Z}_n$, there is also $3\tau(s-1) \equiv 0 \bmod n$. For the rest it suffices to show that $(s-1)t \equiv 0 \bmod n$ since that implies, by (2.5), that $f^2 = \alpha_{t(1+r),r^2}$. We thus need to show that $(s-1)\tau(1+s\rho+\rho^2)$ vanishes modulo $n$. Indeed, $(s-1)\tau(1-\rho+\rho^2) \equiv \tau(s-1)(1+1+1) \equiv 0 \bmod n$. □

**Lemma 3.5.** *Suppose that* $\gcd(|f|, 3) = 1$. *Then* $f$ *is determined by* (2.6) *uniquely, and* $|f|$ *divides* $|C| = 2h$.

Proof: This can be observed directly in many ways, e.g. by $bub^{-1} = f^3(u)$ and $u = b^{2h}ub^{-2h} = f^{6h}(u)$, for every $u \in G$. □

**Lemma 3.6.** *Let* $j \geq 1$ *be such that* $\gcd(j, |f|) = 1$, *Then* $(r^j - s)\mathbb{Z}_n = (r-s)\mathbb{Z}_n$ *and*

$$\{\alpha f^j \alpha^{-1};\ \alpha \in \operatorname{Aut} G\} = \{f_s\alpha_{\tau,r^j};\ \tau \in t\mathbb{Z}_n^* + \kappa(r-s)\mathbb{Z}_n\}.$$

Proof: By Lemma 3.4, $f^j = f_s\alpha_{\tau,r^j}$ for some $\tau \in t\mathbb{Z}_n$. Let $\bar{\jmath} \in \mathbb{Z}$ be such that $(f^j)^{\bar{\jmath}} = f$. Then $r^{j\bar{\jmath}} \equiv 1 \bmod n$. If $s \not\equiv 1 \bmod n$, then $|f|$ is even, and both $j$ and $\bar{\jmath}$ are odd. Therefore $r^j - s \in (r-s)\mathbb{Z}_n$, as

$$r^j - s \equiv r^j - s^j = (r-s)(r^{j-1} + r^{j-2} + \cdots + rs^{j-2} + s^{j-1}) \bmod n.$$

Similarly, $r - s = (r^j)^{\bar{\jmath}} - s \in (r^j - s)\mathbb{Z}_n$. Thus $(r^j - s)\mathbb{Z}_n = (r-s)\mathbb{Z}_n$. By Corollary 3.2 and Lemma 3.3 it remains to show that $\gcd(t, \kappa(r-s), n) = \gcd(\tau, \kappa(r-s), n)$. Because of symmetry it suffices to prove that $\gcd(\tau, \kappa(r-s), n)$ is a multiple of $\gcd(t, \kappa(r-s), n)$. That is clear since $\tau \in t\mathbb{Z}_n$. □

It is clear from (2.6) that if elements $x$, $y$ and $b$ are fixed, then they determine uniquely the structure of $f^3$. Hence $r$ and $t$ are uniquely determined by $x$, $y$ and $b$ if $|f|$ is coprime to three. The next statement gives their values in those alternative expressions of $Q$ in which $\tilde G = G$ and $\tilde C = C$.

**Proposition 3.7.** *Suppose that* $\gcd(3, |f|) = 1$. *Consider the set of all* $(\tilde t, \tilde r) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ *for which there exist* $\tilde x, \tilde y \in G$ *and* $\tilde b \in C$ *such that* $G = \langle \tilde x, \tilde y\rangle$, $C = \langle \tilde b\rangle$, $|x| = |\tilde x|$, $\langle y\rangle = \langle \tilde y\rangle$, *and* $Q = G \rtimes^3_{\tilde f} C$, *where* $\tilde f = \tilde f_s\tilde\alpha_{\tilde t,\tilde r}$ *is of order coprime to three. (The operation and the mappings involving* $\tilde f$ *are defined with respect to* $\tilde x$, $\tilde y$ *and* $\tilde b$*.) Then* $(\tilde t, \tilde r)$ *belongs to such a set if and only if there exists* $j \in \mathbb{Z}$ *such that*

$$\tilde r = r^j,\ \gcd(j, 2h) = 1,\ \text{ and } \tilde t\mathbb{Z}_n^* + \kappa(r-s)\mathbb{Z}_n = t\mathbb{Z}_n^* + \kappa(r-s)\mathbb{Z}_n. \tag{3.5}$$

Proof: Suppose first that $\tilde r$ and $\tilde t$ satisfy (3.5). Then $\gcd(j, |f|) = 1$ since $|f|$ divides $2h$, by Lemma 3.5. Hence $f_s\alpha_{\tilde t,\tilde r}$ is equal to $\alpha f^j \alpha^{-1}$ for some $\alpha \in \operatorname{Aut} G$, by Lemma 3.6. Proposition 1.1 states that $Q$ can be expressed as $G \rtimes^3_{\tilde f} C$ where $\tilde f = f_s\alpha_{\tilde t,\tilde r}$. Note that $|\tilde f| = |f|$.

For the reverse argument consider an alternative expression with $\gcd(|\tilde f|, 3) = 1$. Proposition 1.1 implies the existence of an alternative expression that uses $\alpha f^j \alpha^{-1}$ for some $\alpha \in \operatorname{Aut} G$ and $j$ coprime to $2h$. By Lemma 3.5, $\tilde f = \alpha f^j \alpha^{-1}$ since $|f| = |f^j|$. Hence Lemma 3.6 can be used again. □

## 4. Conjugation and complements

For $u, v \in G$ set $u * v = f_s(f_s(u)f_s(v))$. Then $u * v$ can be also expressed as $f^{-1}(f(u)f(v))$ since there exists $\beta \in \operatorname{Aut} G$ such that $f = \beta f_s$, say by Lemma 3.1. By Proposition 1.2 there exists an action $\mu$ of $G$ upon $G$ that fulfills $\mu_v(uv) = u*v$ for all $u, v \in G$. The action of $G$ upon $G$ by inner automorphisms will be denoted by $\varphi$. Direct computations yield:

**Lemma 4.1.** *Let $i \in \mathbb{Z}$. Put $\sigma = s + 1 + n/\kappa$. Then*

$$\varphi_{y^i} = \alpha_{-i(2+n/\kappa),1} \quad \text{and} \quad \varphi_{xy^i} = \alpha_{i(2+n/\kappa),-1+n/\kappa}; \tag{4.1}$$

$$\mu_{y^i} = \alpha_{i(s-1),1} \quad \text{and} \quad \mu_{xy^i} = \alpha_{i(1-s),s}; \tag{4.2}$$

$$\varphi_{y^i}\mu_{y^i}^{-1} = \alpha_{-i\sigma,1} \quad \text{and} \quad \varphi_{xy^i}\mu_{xy^i}^{-1} = \alpha_{i\sigma,-s(1+n/\kappa)}; \tag{4.3}$$

$$f\varphi_{y^i}\mu_{y^i}^{-1} = f_s\alpha_{t-ir\sigma,r} \quad \text{and} \quad f\varphi_{xy^i}\mu_{xy^i}^{-1} = f_s\alpha_{t+ir\sigma,-sr(1+n/\kappa)}. \tag{4.4}$$

**Lemma 4.2.** *If $u \in G$, then $\mu_{f^3(u)} = \mu_u^{-1}$ and $\mu_u f^3 = f^3\mu_u$.*

Proof: Suppose first that $u = y^i$. Then $f^3(u) = y^{ir^3}$ and $\mu_{f^3(u)} = \alpha_{ir^3(s-1),1} = \alpha_{i(1-s),1}$, by (2.2). Thus $\mu_{f^3(u)} = \mu_u^{-1}$ if $u \in \langle y \rangle$.

Suppose that $u = xy^i$. Then $f^3(u) = xy^{sj}$ where $j \equiv t(1+sr+r^2)+ir^3 \bmod n$. Since $\mu_{f^3(u)} = \alpha_{(s-1)j,s}$ and since $\mu_u^2 = (\alpha_{i(1-s),s})^2 = \mathrm{id}_G$, it suffices to show that $(s-1)j \equiv (1-s)i \bmod n$. That is true because (2.2) implies that $(s-1)t(1+sr+r^2) \equiv (s-1)t(1-r+r^2) \equiv 0 \bmod n$ and that $(s-1)ir^3 \equiv (1-s)i \bmod n$.

By Proposition 1.2, $\mu_u f = f\mu_{f^2(u)}$. Therefore $\mu_u f^3$ is equal to $f^3\mu_{f^6(u)}$. The previous part of the proof implies that $\mu_{f^6(u)} = \mu_u$. □

**Lemma 4.3.** *If $u, v \in G$ and $i$ is an odd integer, then*

$$b^i u \cdot v \cdot u^{-1}b^{-i} = f^{3i}\varphi_u\mu_u^{-1}(v).$$

Proof: The semiautomorphism $f^{3i}$ can be written as $\beta f_s$ for some $\beta \in \operatorname{Aut} G$. Thus $f^{3i}(u)f^{3i}(v) = f^{3i}(u * v) = f^{3i}(\mu_v(uv)) = f^{3i}(\mu_u^{-1}(uv)) = f^{3i}(u\mu_u^{-1}(v))$. From these equalities, and from Lemma 4.2 it follows that

$$\begin{aligned} f^{3i}(u\mu_u^{-1}(v)) * f^{3i}(u^{-1}) &= \mu_{f^{3i}(u^{-1})}(f^{3i}(u\mu_u^{-1}(v))f^{3i}(u^{-1})) \\ &= \mu_u(f^{3i}(\mu_u^{-1}(u\mu_u^{-1}(v)u^{-1}))) = f^{3i}\varphi_u\mu_u^{-1}(v). \end{aligned}$$

Therefore $b^i u \cdot v \cdot u^{-1}b^{-i} = (f^{3i}(u)b^i \cdot v)(u^{-1}b^{-i}) = (f^{3i}(u)f^{3i}(v) \cdot b^i)(u^{-1}b^{-i})$ is equal to $f^{3i}(u\mu_u^{-1}(v)) * f^{3i}(u^{-1}) = f^{3i}\varphi_u\mu_u^{-1}(v)$. □

From here on we shall assume that there exists an element $a \in C$ such that $a^3 = b$. This is equivalent to $3 \nmid h$ since $C = \langle b \rangle$. The element $a$ is determined uniquely.

We can now assume that $f = T_a \restriction G$ since $f^3(u) = bub^{-1} = a^3ua^{-3}$ for every $u \in G$. Since $a$ is of order coprime to three, $T_a$ is also of order coprime to three. Hence $f = T_a \restriction G$ is the only possible choice of $f$ such that $\gcd(3, |f|) = 1$, by Lemma 3.5. In the rest of this paper we shall thus assume that

$$f(u) = aua^{-1} \ \text{ for every } \ u \in G.$$

If $j \in \mathbb{Z}$ is such that $3j \equiv 1 \bmod 2h$, then $b^j = a$ and $f^{3j} = f$. Hence Lemma 4.3 can be expressed as

$$a^i u \cdot v \cdot u^{-1}a^{-i} = f^i\varphi_u\mu_u^{-1}(v) \ \text{ for all } \ u, v \in G \ \text{ and all odd } \ i \in \mathbb{Z}. \tag{4.5}$$

**Lemma 4.4.** *Put $M = \{i \in \mathbb{Z}_n;\ i(s-1) \equiv 0 \bmod n\}$. If $n$ is even and $s \equiv \pm 1 \bmod 2^k$, then $M = ((s+1)/2)\mathbb{Z}_n$. Otherwise $M = (s+1)\mathbb{Z}_n$.*

Proof: Set $d^- = \gcd(n, s-1)$ and $d^+ = \gcd(n, s+1)$. Clearly $\gcd(d^-, d^+) \in \{1, 2\}$ and so $d^-d^+ \in \{n, 2n\}$ (note that $d^-d^+ \equiv s^2 - 1 \equiv 0 \bmod n$). If $d^-d^+ = n$ (which happens, e.g., when $n$ is odd), then $M = d^+\mathbb{Z}_n = (s+1)\mathbb{Z}_n$, otherwise $M = (\frac{s+1}{2})\mathbb{Z}_n$. Let $n$ be even. If $2^k$ divides $s-1$ or $s+1$, then $2^{k+1}$ divides $d^-d^+$, and so $d^-d^+ = 2n$. In the remaining cases there must be $k \geq 3$, and one of $s-1$ and $s+1$ is $\equiv 2^{k-1} \bmod 2^k$. In such cases $d^-d^+ = n$. □

**Lemma 4.5.** *Assume $k \geq 2$. Put $M = \{i \in \mathbb{Z}_n;\ i(s-1) \equiv 0 \bmod n\}$ and $\sigma = s + 1 + n/2$. If $k = 2$ and $s \equiv 1 \bmod 4$, then $M = (\sigma/4)\mathbb{Z}_n$. If $k \geq 3$ and $s \equiv 1 \bmod 2^k$ or $s \equiv -1 + 2^{k-1} \bmod 2^k$, then $M = (\sigma/2)\mathbb{Z}_n$. Otherwise $M = \sigma\mathbb{Z}_n$.*

Proof: We shall proceed like in the proof of Lemma 4.4, setting $d^- = \gcd(s-1, n)$ and $d^+ = \gcd(\sigma, n)$. Since $(s-1)\sigma \equiv 0 \bmod n$, the set $M$ can be expressed as $(d^+/\delta)\mathbb{Z}_n = (\sigma/\delta)\mathbb{Z}_n$, where $\delta = d^-d^+/n$. Now, $\delta = 4$ if $k = 2$ and $s \equiv 1 \bmod 4$, while $\delta = 2$ if $k \geq 3$, and $s \equiv 1$ or $s \equiv -1 + 2^{k-1} \bmod 2^k$. In the remaining cases $\delta = 1$. □

**Lemma 4.6.** *Put $\sigma = s + 1 + n/\kappa$. If $j \geq 1$ is odd, then*

$$\{f^j \varphi_u \mu_u^{-1};\ u \in \langle y \rangle\} = \{f_s \alpha_{\tau, r^j};\ \tau \in t + \sigma\mathbb{Z}_n\}, \text{ and}$$
$$\{f^j \varphi_u \mu_u^{-1};\ u \in x\langle y \rangle\} = \{f_s \alpha_{\tau, -sr^j(1+n/\kappa)};\ \tau \in t + \sigma\mathbb{Z}_n\}.$$

Proof: We shall first prove the equality in a modified form in which $\tau$ runs through $t(1 + \cdots + r^{j-1}) + \sigma\mathbb{Z}_n$. For $j = 1$ this directly follows from (4.4). If $\ell \geq 1$, then $f^{2\ell} = \alpha_{t(1+\cdots+r^{2\ell-1}), r^{2\ell}}$, by Lemma 3.4, and $f^{2\ell} f_s = f_s f^{2\ell}$ (because $ts \equiv t \bmod n$, again by Lemma 3.4). Therefore

$$f^{2\ell} f_s \alpha_{t+\gamma\sigma, r} = f_s \alpha_{t(1+\cdots+r^{2\ell}) + \sigma\gamma r^{2\ell}, r^{2\ell+1}}$$

for every $\gamma \in \mathbb{Z}_n$. By (4.4) that yields the case $j = 2\ell + 1$ for every $u \in \langle y \rangle$. For $u \in x\langle y \rangle$ the situation is only slightly different.

For the rest it suffices to show that $\delta = t(1 + \cdots + r^{j-1}) - t \in \sigma\mathbb{Z}_n$. Put $M = \{i \in \mathbb{Z}_n;\ i(s-1) \equiv 0 \bmod n\}$. By Lemma 3.4, $t \in M$, and thus also $\delta \in M$. If $n$ is even, then $\sigma$ is even, $r + \cdots + r^{j-1}$ is even, and so $\delta/2 \in M$. This solves cases $M = \sigma\mathbb{Z}_n$ and $M = (\sigma/2)\mathbb{Z}_n$. By Lemmas 4.4 and 4.5 the only remaining case is that of $k = \kappa = 2$ and $s \equiv 1 \bmod 4$. In this case $M = (\sigma/4)\mathbb{Z}_n$ and $v_2(\sigma) = 2$. Hence it suffices to verify $v_2(\delta) \geq 2$. This is true because $t$ is even (there is $\kappa = 2$). □

**Proposition 4.7.** *Let $j \in \mathbb{Z}$ be such that $\gcd(j, 2h) = 1$. Put $T = t\mathbb{Z}_n^* + (s + 1 + n/\kappa)\mathbb{Z}_n + \kappa(r - s)\mathbb{Z}_n$. If $G = \langle \tilde{x}, \tilde{y} \rangle$, $|\tilde{x}| = |x|$, $\langle \tilde{y} \rangle = \langle y \rangle$, then for every $u \in G$ the mapping $T_{a^j u} \restriction G$ can be expressed as $\tilde{f}_s \tilde{\alpha}_{\tau, \tilde{r}}$, where $\tau \in T$ and $\tilde{r}$ is equal to $r^j$ if $u \in \langle y \rangle$, and to $-sr^j(1 + n/\kappa)$ if $u \in x\langle y \rangle$. On the other hand, for any choice of $\tau \in T$ and $\tilde{r} \in \{r^j, -sr^j(1 + n/\kappa)\}$ there exist $u$, $\tilde{x}$ and $\tilde{y}$ such that $T_{a^j u}$ yields $\tilde{f}_s \tilde{\alpha}_{\tau, \tilde{r}}$.*

Proof: The change of generators $(x, y) \mapsto (\tilde{x}, \tilde{y})$ corresponds to an automorphism of $\tilde{G}$. By Proposition 1.1 and Corollary 3.2 every such change means that $f = f_s\alpha_{t,r}$ is equal to $\tilde{f} = \tilde{f}_s\tilde{\alpha}_{\tau,r}$, where $\tau \in t\mathbb{Z}_n^* + \kappa(r-s)\mathbb{Z}_n$, and for every such $\tau$ there exist $\tilde{x}$ and $\tilde{y}$ that produce such a $\tilde{f}$. By (4.5) the mapping $T_{a^ju} \restriction G$ is equal to $\tilde{f}^j\tilde{\varphi}_u\tilde{\mu}_u^{-1}$. The rest follows from Lemma 4.6. □

If $\tilde{C} = \langle \tilde{a} \rangle$, then $\tilde{a} = a^j u$ for some $u \in G$ and $j \in \mathbb{Z}$, $\gcd(j, 2h) = 1$. Hence the set $T$ does not depend upon the choice of a complement (and its generator). It depends only upon the choice of $G \trianglelefteq Q$ and upon the specification of $|x| \in \{2, 4\}$ (which is needed only when $\kappa = 2$). We shall denote $T$ by $T_G$, assuming that $|x| = 2$ (i.e. $\lambda = 1$) when $\kappa = 2$. Thus $T_G = t\mathbb{Z}_n^* + (s+1+n/\kappa)\mathbb{Z}_n + \kappa(r-s)\mathbb{Z}_n$. Our aim now is to simplify this description.

**Lemma 4.8.** *Put $\sigma = s + 1 + n/\kappa$ and $\Sigma = \sigma\mathbb{Z}_n$. Then $t + \Sigma = t\mathbb{Z}_n^* + \Sigma$. Furthermore, $t \notin \Sigma$ if and only if (a) $t$ is odd and $k \geq 1$, or (b) $v_2(t) = k-1 \geq 1$ and $s \equiv -1+n/\kappa \bmod 2^k$. Furthermore, $t+\Sigma = m+\Sigma$ in case (a), and $t+\Sigma = n/2+\Sigma$ in case (b).*

*The set $\Sigma$ does not contain $\kappa(r-s)$ if and only if*

$$k \geq 2,\ \kappa = 1,\ s \equiv -1 \bmod 2^k \ \textit{and}\ r \equiv 2^{k-1} - 1 \bmod 2^k.$$

*In the latter case $T_G = ((s+1)/2)\mathbb{Z}_n$.*

Proof: Put $M = \{i \in \mathbb{Z}_n;\ i(s-1) \equiv 0 \bmod n\}$. Clearly $s + 1 \in M$. By Lemma 3.4, $t \in M$ and $r + 1 \in M$. Hence $r - s \in M$ as well, and so $T_G \subseteq M$. Every of the sets $t + \Sigma \subseteq t\mathbb{Z}_n^* + \Sigma \subseteq T_G$ (cf. Proposition 4.7) is a union of cosets modulo $\Sigma$. Hence if $M \subseteq \Sigma = M$, then $t \in \Sigma$ and all these three sets coincide and are equal to $M$. In the rest of the proof it therefore suffices to investigate the cases when $M \neq \Sigma$.

Suppose first that $\kappa = 1$ and $\Sigma \neq M$. By Lemma 4.4 we need to investigate the case when $k \geq 1$, $s \equiv \pm 1 \bmod 2^k$ and $(s+1)/2 \in M \backslash \Sigma$. Clearly, $t+\Sigma = t\mathbb{Z}_n^*+\Sigma = \Sigma$ if and only if $v_2(t) \geq \ell$, where $\ell = \min(v_2(s+1), k)$, while $t+\Sigma = t\mathbb{Z}_n^*+\Sigma = M\backslash\Sigma$ if and only if $v_2(t) < \ell$ (then $v_2(t) = \ell - 1$). Similarly, $r - s \notin \Sigma$ if and only if $v_2(r-s) < \ell$.

If $t$ is odd, then $v_2(t) < \ell$. By Lemma 3.4 in such a case $s \equiv 1 \bmod 2^k$ (since $t(s-1) \equiv 0 \bmod 2^k$). Now, $s \equiv 1 \bmod 2^k$ implies that $m \in M \setminus \Sigma$, and hence $t + \Sigma = m + \Sigma$. We have $\ell = 1$, and so $r - s \in \Sigma$.

If $t$ is even, then $v_2(t) < \ell$ can happen only if $\ell \geq 2$. Therefore $k \geq 2$, $s \equiv -1 \bmod 2^k$ and $\ell = k$. Hence $\Sigma \neq M$ if and only if $v_2(t) = k - 1$, and then $n/2 \in M \setminus \Sigma$.

If $v_2(r - s) < \ell$, then we again obtain that $k \geq 2$, $s \equiv -1 \bmod 2^k$ and $\ell = k$. By Lemma 3.4, $(r + 1)(s - 1) \equiv 0 \bmod n$. Hence $v_2(r - s) < \ell$ if and only if $r \equiv -1 + 2^{k-1} \bmod 2^k$. In such a case $(s-r)\mathbb{Z}_n + \Sigma = M$. Since $T_G \subseteq M$, there is $t \in M$, and so $T_G = M = ((s+1)/2)\mathbb{Z}_n$.

Suppose now that $\kappa = 2$, and assume first that $k \geq 3$. By Lemma 4.5 we need to investigate situations when $s \equiv 1$ or $s \equiv -1 + 2^{k-1} \bmod 2^k$, $|M : \Sigma| = 2$ and

$(s+1)/2+n/4 \in M \setminus \Sigma$. Put $\ell = \min(v_2(\sigma), k)$. Like in the case $\kappa = 1$ we need to decide when $v_2(t) < \ell$ and $v_2(2(r-s)) < \ell$. If $s \equiv 1 \bmod 2^k$, then $\ell = 1$ while both $t$ and $r-s$ are even. Hence we can assume that $s \equiv -1+2^{k-1} \bmod 2^k$. Then $\ell = k$ and $r \equiv -1 \bmod 2^{k-1}$, by $(r+1)(s-1) \equiv 0 \bmod n$. Therefore $v_2(2(r-s)) \geq k$, while $\Sigma \neq M$ if and only if $v_2(t) = k-1$. In the latter case $t+\Sigma = n/2+\Sigma = M \setminus \Sigma$.

Finally assume that $k = \kappa = 2$. By Lemma 4.5, $s \equiv 1 \bmod 4$ and $|M : \Sigma| = 4$. Then $\Sigma = 4M \leq 4\mathbb{Z}_n$, $m \in M$ and $2m = n/2 \in 2M$. Since $t$ is even there is $t+M \subseteq 2M$. Hence $\Sigma \neq M$ if and only if $t \in 2M \setminus 4M$, i.e. if and only if $v_2(t) = 1$. Finally, note that $2(r-s) \in 4M = \Sigma$ since $r-s \in 2M$. □

**Proposition 4.9.** *Put $\sigma = s+1+n/\kappa$. The set $T_G$ is different from $\sigma\mathbb{Z}_n$ in exactly these cases:*

1. *if $t$ is odd and $k \geq 1$, then $T_G = m+(s+1)\mathbb{Z}_n$. In such a case $s \equiv 1 \bmod 2^k$;*
2. *if $k \geq 2$, $\kappa = 1$, $s \equiv -1 \bmod 2^k$ and $r \equiv -1+2^{k-1} \bmod 2^k$, then $T_G = ((s+1)/2)\mathbb{Z}_n$; and*
3. *$T_G = n/2+\sigma\mathbb{Z}_n$ if $k \geq 2$, $s \equiv -1+n/\kappa \bmod 2^k$, $v_2(t) = k-1$, and either $\kappa = 2$, or $\kappa = 1$ and $r \equiv -1 \bmod 2^k$.*

Proof: Put $\Sigma = \sigma\mathbb{Z}_n$. By Lemma 4.8, $t+\Sigma \neq T_G$ exactly when case (2) takes place. The rest follows from Lemma 4.8 as well (note that $r \equiv -1 \bmod 2^{k-1}$ if $s \equiv -1 \bmod 2^{k-1}$ and $k \geq 2$, by Lemma 3.4). □

Define now $t'$ as the least integer in $t+\sigma\mathbb{Z}_n$. By Lemma 4.8, $t' = 0$ unless $t$ is odd and $k \geq 1$ (then $t' = m$) or if $v_2(t) = k-1 \geq 1$ and $s \equiv -1+n/\kappa \bmod 2^k$ (then $t' = n/2$). Note that $t' = \min T_G$, with the exception of case (2) in Proposition 4.9.

Since $t' \in t+\sigma\mathbb{Z}_n \subseteq T_G$, equations (4.4) and (4.5) immediately yield:

**Corollary 4.10.** *There exists $a' \in a\langle y\rangle = \langle y\rangle a$ such that $T_{a'} \restriction G = f_s\alpha_{t',r}$.*

Our next aim is to investigate when $a'$ can be chosen in such a way that $\langle a'\rangle$ is a complement to $G$. The following well known fact will be useful.

**Lemma 4.11.** *Let $j \geq 2$ be even and let $\rho \in \mathbb{Z}$ be odd. Then*

$$v_2(1+\rho+\cdots+\rho^{j-1}) = v_2(j)+v_2(\rho+1)-1.$$

Proof: We claim that $v_2(1+\cdots+\rho^{j-1}) = v_2(j)$ for all $\rho \equiv 1 \bmod 4$. If that is known, then $v_2(1+\cdots+\rho^{j-1})+1 = v_2(\rho+1)+v_2(j)$ for every $\rho \equiv 3 \bmod 4$ since

$$(1+\cdots+\rho^{j-1})(1-\rho) = 1-\rho^j = 1-(-\rho)^j = (1+\rho)(1+\cdots+(-\rho)^{j-1}).$$

(Note that $-\rho \equiv 1 \bmod 4$ if $\rho \equiv 3 \bmod 4$.)

Suppose that $\rho \equiv 1 \bmod 4$ and let $j = \sum j_i 2^i$, $j_i \in \{0,1\}$. Then $1+\cdots+\rho^{j-1} = \sum j_i \rho^{s_i}(1+\cdots+\rho^{2^i-1})$, where $s_i = \sum_{\ell<i} j_\ell 2^\ell$. Hence it suffices to show that $v_2(1+\cdots+\rho^{2^i-1}) = i$. We shall proceed by induction on $i$. The case $i=1$ is trivial. The induction step follows from $1+i+v_2(\rho-1) = v_2(\rho^{2^i}+1)+$

$v_2(1+\cdots+\rho^{2^i-1})+v_2(\rho-1) = v_2(\rho^{2^i}+1)+v_2(\rho^{2^i}-1) = v_2(\rho^{2^{i+1}}-1) = v_2(1+\cdots+\rho^{2^{i+1}-1})+v_2(\rho-1)$. □

By direct computation,

$$(y^i a)^{2h} = y^{i(1+r+\cdots+r^{2h-1})} \text{ for every } i \in \mathbb{Z}. \tag{4.6}$$

Since $f^{2h}(u) = a^{2h}ua^{-2h} = u$ for every $u \in G$, Lemma 3.4 yields that

$$t(1+r+\cdots+r^{2h-1}) \equiv 0 \bmod n \text{ and } r^{2h} \equiv 1 \bmod n. \tag{4.7}$$

By applying Lemma 4.11 to (4.7) we obtain that

$$v_2(t)+v_2(h)+v_2(r+1) \geq k. \tag{4.8}$$

**Proposition 4.12.** *Let $a' \in a\langle y\rangle$ be such that $T_{a'} \restriction G = f_s\alpha_{t',r}$. If $k \leq 1$ or if $t$ is odd or if $r \equiv -1 \bmod 2^k$ then $(a')^{2h} = 1$. If $k \geq 2$, then $(a')^{2h} \in \{1, y^{n/2}\}$.*

Proof: Put $\sigma = s+1+n/\kappa$ and note that $t' = t - ir\sigma$ for some $i \in \mathbb{Z}_n$, by (4.4) and (4.5). Since $\sigma(s-1) \equiv 0 \bmod n$, there is $t'(s-1) \equiv 0 \bmod n$, by Lemma 3.4. Therefore $(f_s\alpha_{t',r})^2 = \alpha_{t'(s+r),r^2} = \alpha_{t'(1+r),r^2}$, and $(f_s\alpha_{t'r})^{2h} = \alpha_{t'\rho,1}$, where $\rho = 1+r+\cdots+r^{2h-1}$. We shall now show that $t'\rho \equiv 0 \bmod n$. If $t' \in \{0, n/2\}$, then this is clear. If $t' = m$ and $k \geq 1$, then $t$ is odd, and $\rho \equiv 0 \bmod 2^k$ by (4.7). Therefore $(f_s\alpha_{t',r})^{2h} = \mathrm{id}_G$. This mapping is also equal to $T_z \restriction G$ where $z = (a')^{2h}$. Since $z \in G$, the triviality of the mapping implies that $z \in Z(G)$. Hence $z = 1$ if $k = 0$. Assume $k \geq 1$. By Lemma 2.1, $z = y^j$ for some $j \in \mathbb{Z}$. Clearly, $z = 1$ if $v_2(j) \geq k$.

Let $i \in \mathbb{Z}$ be such that $a' = y^i a$. Thus $j \equiv i\rho \bmod n$, by (4.6). There is $v_2(\rho) \geq 1$, if $k \geq 1$. If $t$ is odd, then $v_2(\rho) \geq k$ by (4.7). If $r \equiv -1 \bmod 2^k$, then $\rho \equiv 0 \bmod 2^k$. Hence it remains to show that $z \in \{1, y^{n/2}\}$ whenever $k \geq 2$. By Lemma 2.1 this is clear with the exception of the case when $|Z(G)| = 4$. However, in that case it suffices to have $v_2(j) \geq 1$. And that follows from the fact that $\rho$ is even. □

**Lemma 4.13.** *Let $a' \in a\langle y\rangle$ be such that $(a')^{2h} = y^{n/2}$ and $T_{a'} \restriction G = f_s\alpha_{t',r}$. Put $\sigma = s+1+n/\kappa$. If $i \in \mathbb{Z}$, then $T_{a'y^i} = f_s\alpha_{t'-ir\sigma,r}$ and*

$$(a'y^i)^{2h} = 1 \quad \Leftrightarrow \quad i(1+r+\cdots+r^{2h-1}) \equiv n/2 \bmod n.$$

Proof: Suppose that $a' = ay^j$. We have $T_{a'y^i} \restriction G = f\alpha_{-(i+j)\sigma,1} = f\alpha_{-j\sigma,1}\alpha_{-i\sigma,1} = f_s\alpha_{t',r}\alpha_{-i\sigma,1} = f_s\alpha_{t'-ir\sigma,r}$, by (4.3) and (4.5). The other claim follows from $(a'y^i)^{2h} = (a')^{2h}y^{i\rho}$ where $\rho = 1+r+\cdots+r^{2h-1}$. □

**Corollary 4.14.** *If $t' \neq 0$ or if $s \equiv -1+n/\kappa \bmod 2^k$, $k \geq 2$, then there exists $a' \in a\langle y\rangle$ such that $T_{a'} \restriction G = f_s\alpha_{t',r}$ and $(a')^{2h} = 1$.*

Proof: If $t' = m$, then the existence of $a'$ follows from Proposition 4.12. The only other case with $t' \neq 0$ is that of $t' = n/2$, $k \geq 2$ and $s \equiv -1+n/\kappa \bmod 2^k$. We can thus assume that $s \equiv -1+n/\kappa \bmod 2^k$, $k \geq 2$. Put $\rho = 1+r+\cdots+r^{2h-1}$.

If $k = 2$, then $v_2(\rho) \geq k - 1$ since $r$ is odd. If $k \geq 3$, then $v_2(\rho) \geq k - 1$ by Lemma 4.11 since $v_2(r + 1) \geq k - 1$, by Lemma 3.4. By Corollary 4.10 there exists $a' \in a\langle y\rangle$ such that $T_{a'} \restriction G = f_s\alpha_{t',r}$. If $(a')^{2h} = 1$, then there is nothing to prove. By Proposition 4.12 we can thus assume that $(a')^{2h} = y^{n/2}$. By (4.6) we must have $v_2(\rho) = k - 1$. But then $(a'y^m)^{2h} = 1$ and $T_{a'y^m} \restriction G = f_s\alpha_{t',r}$, by Lemma 4.13, since $rm(s + 1 + n/\kappa) \equiv 0 \bmod n$. □

**Corollary 4.15.** *There always exist $\tilde{a} \in a\langle y\rangle$ and $j \in \{0, \dots, k\}$ such that $T_{\tilde{a}} \restriction G = f_s\alpha_{2^jm,r}$ and $\tilde{a}^{2h} = 1$.*

Proof: By Corollary 4.14 we can assume that $t' = 0$. By Proposition 4.12 there exists $a' \in a\langle y\rangle$ such that $(a')^{2h} \in \{1, y^{n/2}\}$ and $T_{a'} \restriction G = f_s\alpha_{0,r}$. Put $\tilde{a} = a'$ if $(a')^{2h} = 1$. For the rest of the proof assume that $(a')^{2h} = y^{n/2}$. There exists $i \in \mathbb{Z}$ such that $a = a'y^i$. Then $t = -ir\sigma$ and $i(1 + \cdots + r^{2h-1}) \equiv n/2 \bmod n$, by Lemma 4.13. If $\ell$ is odd, then Lemma 4.13 implies that $\langle a'y^{i\ell m}\rangle$ is a complement to $G$ as well, and that $T_{a'y^{i\ell m}} \restriction G = f_s\alpha_{-m\ell t,r}$. There exists $\ell \in \mathbb{Z}_n^*$ such that $-m\ell t$ is a divisor of $n$. Such a divisor is necessarily of the form $m2^j$, and hence $\tilde{a}$ may be chosen as $a'y^{i\ell m} = ay^{i(\ell m-1)}$, for a suitable $\ell \in \mathbb{Z}_n^*$. □

**Lemma 4.16.** *Suppose that $v_2(h) + v_2(r + 1) \geq k \geq 2$. Then $\langle ay^{im}\rangle$ is a complement to $G$ for every $i \in \mathbb{Z}$. Furthermore, if $a' \in a\langle y\rangle$ is such that $T_{a'} \restriction G = f_s\alpha_{t',r}$, then $\langle a'\rangle$ is a complement to $G$.*

Proof: Put $\rho = 1 + r + \cdots + r^{2h-1}$. Assume that $v_2(h) + v_2(r + 1) \geq k$. Then $v_2(\rho) \geq k$, by Lemma 4.11, and $(y^{im}a)^{2h} = y^{im\rho} = 1$, by (4.6). If $a' \in a\langle y\rangle$ is such that $T_{a'} \restriction G = f_s\alpha_{t',r}$, then $(a')^{2h} \in \{1, y^{n/2}\}$ by Proposition 4.12. However, by using Lemma 4.13 for $a = a'y^i$ we see that $v_2(\rho) \leq k - 1$ if $(a')^{2h} = y^{n/2}$. □

We are now ready to separate cases that always yield a complement $\langle a'\rangle$ from those where this need not happen. To this purpose we shall use the following condition:

$$(4.9) \qquad k \geq 2,\ t \text{ is even},\ v_2(s + 1 + n/\kappa) < k \text{ and } v_2(h) + v_2(r + 1) < k.$$

**Proposition 4.17.** *If (4.9) is not satisfied, then there exists $a' \in a\langle y\rangle$ such that $(a')^{2h} = 1$ and $T_{a'} \restriction G = f_s\alpha_{t',r}$. If (4.9) is satisfied, then $t' = 0$ and*

$$k > \delta = v_2(s + 1 + n/\kappa) + k - 1 - v_2(h) - v_2(r + 1) \geq 1.$$

Proof: If $k \leq 1$ or if $t$ is odd, use Proposition 4.12. Put $\sigma = s + 1 + n/\kappa$. If $v_2(\sigma) \geq k$, use Corollary 4.14. If $v_2(h) + v_2(r + 1) \geq k$, use Lemma 4.16. This covers all situations in which (4.9) is not satisfied. By the definition of $t'$ this also covers all situations with $t' \neq 0$.

Suppose now that (4.9) holds. Then $k - 1 - v_2(h) - v_2(r + 1) \geq 0$, and hence $\delta \geq 1$. If $k = 2$, then $k - 1 - v_2(h) - v_2(r + 1) = 0$ and $v_2(\sigma) = 1$. Hence $k > \delta$ if $k = 2$. Assume $k \geq 3$. Then $k > \delta$ is clear if $v_2(\sigma) = 1$. Assume that $v_2(\sigma) = k - 1$. Then $v_2(r + 1) = k - 1$ by Lemma 3.4 (since (4.9) forbids $v_2(r + 1) = k$), and so $k > \delta$ again. □

**Proposition 4.18.** *Let (4.9) be true. Denote by $\mathcal{M}$ the set of all $(\tau,\rho)$ for which there exists $\tilde{a}\in\langle a,y\rangle$ such that $\langle\tilde{a}\rangle$ is a complement to $G$ and $T_{\tilde{a}}\restriction G=f_s\alpha_{\tau,\rho}$. Then either*

(1) *$v_2(t)>\delta$. Then $v_2(\tau)>\delta$ for every $(\tau,\rho)\in\mathcal{M}$, and there exists $a'\in a\langle y\rangle$ such that $(a')^{2h}=1$ and $T_{a'}\restriction G=f_s\alpha_{0,r}$; or*

(2) *$v_2(t)=\delta$. Then $v_2(\tau)=\delta$ for every $(\tau,\rho)\in\mathcal{M}$, and there exists $a'\in a\langle y\rangle$ such that $(a')^{2h}=1$ and $T_{a'}\restriction G=f_s\alpha_{2^\delta m,r}$.*

Proof: If $j$ is odd, then $r^j+1=(r+1)((-r)^{j-1}+\cdots+(-r)+1)$, and so $v_2(r^j+1)=v_2(r+1)$. Hence (4.9) remains valid when $r$ is replaced by $r^j$, $\gcd(j,2h)=1$. By Lemma 4.6 this means that we may investigate only the case when $\tilde{a}\in a\langle y\rangle$ (then $\rho=r$). Our claim depends upon the choice of $x,y\in G$ but not upon the choice of the complement $C$. Hence we can assume that $a=a'$ if there exists $a'\in a\langle y\rangle=\langle y\rangle a$ such that $(a')^{2h}=1$ and $T_{a'}\restriction G=f_s\alpha_{0,r}$. In such a case $\tilde{a}=y^ia$ yields a complement to $G$ if and only if $i(1+r+\cdots+r^{2h-1})\equiv 0 \bmod n$, by (4.6), and this gives $v_2(i)+v_2(r+1)+v_2(h)\geq k$ and $T_{\tilde{a}}\restriction G=f_s\alpha_{\tau,r}$ where $\tau\equiv -i\sigma r \bmod n$, $\sigma=s+1+n/\kappa$, by Lemma 4.11 and by (4.5) and (4.4). Therefore $v_2(\tau)\geq v_2(\sigma)+k-v_2(r+1)-v_2(h)=\delta+1$.

Suppose now that there exists no $\tilde{a}\in a\langle y\rangle$ such that $\langle a\rangle\cap G=1$ and $T_{\tilde{a}}\restriction G=f_s\alpha_{0,r}$. Then there exists, by Corollary 4.10 and Proposition 4.12, an element $a'\in a\langle y\rangle$ such that $T_{a'}\restriction G=f_s\alpha_{0,r}$ and $(a')^{2h}=y^{n/2}$. If $i\in\mathbb{Z}$ is such that $\langle a'y^i\rangle\cap G=1$ and $T_{a'y^i}=f_s\alpha_{\tau,r}$, then Lemma 4.13 implies that $\tau=-ir\sigma$ and that $v_2(i)+v_2(r+1)+v_2(h)=k-1$, by Lemma 4.11. Hence $v_2(\tau)=v_2(i)+v_2(\sigma)=\delta$. The rest follows from Corollary 4.15. □

Proposition 4.18 states that the cases when no $a'$ yields a complement are those cases when both (4.9) and $v_2(t)=\delta$ are true. We shall now investigate when this property remains true for all generators $\tilde{x}$ and $\tilde{y}$ of $G$.

**Proposition 4.19.** *Assume that $v_2(t)=\delta$ and that (4.9) is true. Denote by $\mathcal{M}$ the set of all $(\tau,\rho)$ for which there exist $\tilde{x},\tilde{y},\tilde{a}\in Q$ such that $G=\langle\tilde{x},\tilde{y}\rangle$, $\langle\tilde{y}\rangle=\langle y\rangle$, $\langle\tilde{a}\rangle$ is a complement to $G$, and $T_{\tilde{a}}\restriction G=\tilde{f}=\tilde{f}_s\tilde{\alpha}_{\tau,\rho}$. Denote by $\mathcal{M}_1\subseteq\mathcal{M}$ the set of those $(\tau,\rho)$ for which $|\tilde{x}|=|x|$.*

(1) *If $v_2(\kappa(r-s))\leq\delta$, then $(0,r)\in\mathcal{M}_1$.*

(2) *If $\kappa=2$ and $v_2(r-s)=\delta$, then $(0,r)\in\mathcal{M}$ and $v_2(\tau)=\delta$ for every $(\tau,\rho)\in\mathcal{M}_1$.*

(3) *If $v_2(r-s)>\delta$, then $v_2(\tau)=\delta$ for each $(\tau,\rho)\in\mathcal{M}$.*

Proof: By Proposition 4.18 the only aspect to consider is the value of $v_2(\tilde{t})$ when $\tilde{f}$ is expressed with respect to $\tilde{x}$ and $\tilde{y}$. If $|\tilde{x}|=|x|$, then the transformation can be obtained by means of an automorphism. By Corollary 3.2 we thus have to investigate $v_2(\tau)$ where $\tau$ runs through $t\mathbb{Z}_n^*+\kappa(r-s)\mathbb{Z}_n$. It is clear (cf. Lemma 3.3) that $v_2(\tau)=\delta$ for every such $\tau$ if and only if $v_2(\kappa(r-s))>\delta$. This settles the case $\kappa=1$ and the case $v_2(r-s)<\delta$.

Suppose now that $\kappa=2$ and $v_2(r-s)\geq\delta$. By the previous part of the proof and by Proposition 4.18 it suffices to express $f$ with respect to $\tilde{x}=xy$ and

$\tilde{y} = y$. By Lemma 3.4, $a(xy)a^{-1} = xy^{st+rs} = xy^{t+1+r-s} = xy \cdot y^{t+r-s}$ and so $v_2(t+r-s) > \delta$ if and only if $v_2(r-s) = \delta$. Since $t+r-s = \tilde{t}$, we are done, by Proposition 4.18. □

**Proposition 4.20.** *Assume that $v_2(t) = \delta$ and (4.9) are true, and that $r \equiv 3 \bmod 4$. Then $k \geq 3$, $v_2(2h) = v_2(\mathrm{ord}_n(r)) = k - v_2(r+1)$ and $\delta = v_2(\sigma)$, $\sigma = s + 1 + n/\kappa$.*

(1) *If $s \equiv 1 \bmod 2^{k-1}$, then $\delta = 1 = v_2(r-s) = v_2(r-1)$.*
(2) *If $s \equiv -1 \bmod 2^{k-1}$, then $h$ is odd, $\delta = k-1$, $r \equiv 2^{k-1} - 1 \bmod 2^k$ and $\min\{k, v_2(r-s)\} = k + 1 - \kappa$.*

Proof: By (4.9), $v_2(r+1) < k$. Hence $k \geq 3$. The multiplicative order of $r$ modulo $2^k$ is equal to $2^{k-v_2(r+1)}$. Hence $v_2(\mathrm{ord}_n(r)) \geq k - v_2(r+1)$. Furthermore, $v_2(2h) \geq v_2(\mathrm{ord}_n(r))$ since $r^{2h} \equiv 1 \bmod n$. By Lemmas 4.11 and 4.13, $v_2(r+1) + v_2(h) \leq k-1$. Thus $k - v_2(r+1) \geq v_2(2h) \geq v_2(\mathrm{ord}_n(r)) \geq k - v_2(r+1)$, and the definition of $\delta$ in Proposition 4.17 implies that $\delta = v_2(\sigma)$.

Thus $\delta = 1$ if $s \equiv 1 \bmod 2^{k-1}$. In such a case $s \equiv 1 \bmod 4$, and so $v_2(r-s) = v_2(r-1) = 1$.

Assume that $s \equiv -1 \bmod 2^{k-1}$. Then $r \equiv -1 + 2^{k-1} \bmod 2^k$ by Lemma 3.4 and (4.9). Furthermore, $\sigma \equiv 2^{k-1} \bmod 2^k$, also by (4.9), and so $\delta = v_2(\sigma) = k-1$. Since $k - v_2(r+1) = 1$, we must have $v_2(h) = 0$, by the previous part of the proof. If $\kappa = 1$, then $\sigma = s+1$ and $v_2(r-s) \geq k$. If $\kappa = 2$, then $v_2(r-s) = k-1$. □

**Proposition 4.21.** *Assume that $v_2(t) = \delta$ and (4.9) are true, and that $r \equiv 1 \bmod 4$. Then $s \equiv 1 \bmod 2^{k-1}$, $\delta = k - v_2(2h)$ and $v_2(r-1) \geq k - v_2(\mathrm{ord}_n(r)) \geq \delta$.*

(1) *If $k = 2$, then $\delta = 1$ and $h$ is odd. Furthermore, if $\kappa = 1$, then $s \equiv 1 \bmod 4$ and $v_2(r-s) > 1$, while if $\kappa = 2$, then $s \equiv 3 \bmod 4$ and $v_2(r-s) = 1$.*
(2) *If $k \geq 3$ and $h$ is even, then $v_2(r-s) \geq \delta$ and $v_2(h) \geq k - v_2(r-1)$. Furthermore, $v_2(r-s) = \delta$ if and only if $v_2(2h) = k - v_2(r-1)$.*
(3) *If $k \geq 3$ and $h$ is odd, then $v_2(r-s) \geq \delta = k-1$, $r \equiv 1 \bmod 2^{k-1}$, and $v_2(r-s) = \delta$ if and only if $r - s \equiv 2^{k-1} \bmod 2^k$.*

Proof: By Lemma 3.4, $s \equiv 1 \bmod 2^{k-1}$. We see that $v_2(2h) \geq v_2(\mathrm{ord}_n(r)) \geq k - v_2(r - 1 + 2^k)$. By the definition, $\delta = 1 + k - 1 + v_2(h) - v_2(r+1) = k - v_2(2h)$. Hence $v_2(r-1) \geq k - v_2(\mathrm{ord}_n(r)) \geq k - v_2(2h) \geq \delta$.

Case (1) is straightforward. Assume that $k \geq 3$. Note that $\delta \leq k-2$ if $h$ is even, while $\delta = k-1$ if $h$ is odd. If $r \not\equiv 1 \bmod 2^{k-1}$, then $k-2 \geq v_2(r-1) = v_2(r-s) \geq \delta$, $v_2(h) \geq 1$, $k - \delta = v_2(2h) \geq 2$, and $v_2(r-s) = \delta$ if and only if $v_2(r-1) = k - v_2(2h)$. Suppose that $r \equiv 1 \bmod 2^{k-1}$. If $h$ is even, then $v_2(r-s) \geq k-1 > \delta$. Suppose that $h$ is odd. Then $v_2(r-s) \geq k-1 = \delta$, and $v_2(r-s) = \delta$ if and only if $r - s \equiv 2^{k-1} \bmod 2^k$. □

## 5. Classification with respect to a given normal subgroup

Let $Q_i = G \rtimes_{f_i}^{3} C_i$ be (Moufang) loops, $C_i = \langle b_i \rangle$, $i \in \{1, 2\}$. Call $Q_1$ and $Q_2$ *$G$-isomorphic* if there exists $\Psi\colon Q_1 \cong Q_2$ such that $\Psi(G) = G$.

Let $G$ be like above, i.e. $G = \langle x, y;\, y^n = 1,\, x^2 = y^{n/\lambda},\, xyx^{-1} = y^{-1+n/\kappa}\rangle$, $G$ is noncommutative, $\lambda, \kappa \in \{1, 2\}$ and $G \not\cong Q_8$, $\lambda = 1$ if $n$ is odd, $\kappa = 1$ if $4 \nmid n$.

Call $Q_1$ and $Q_2$ *strongly $G$-isomorphic* if there exists $\Psi\colon Q_1 \cong Q_2$ such that $\Psi(G) = G$ and $\Psi(\langle y\rangle C_1) = \langle y\rangle C_2$.

Implicit assumptions of this section are the same as before, i.e. $Q = G \rtimes_f^3 C$, $C = \langle b\rangle$, $|C| = 2h$, $3 \nmid h$, $b = a^3$, $f = f_s\alpha_{t,r}$, $s^2 - 1 \equiv t(s-1) \equiv (r+1)(s-1) \equiv 0 \bmod n$, $n = 2^k m$, $m$ odd. Recall that $\mathrm{ord}_{2^k}(r)$ divides $\mathrm{ord}_n(r)$, and that divides $2h$. Furthermore,

$$v_2(\mathrm{ord}_{2^k}(r)) = k - v_2(r - (-1)^{(r-1)/2}) \text{ if } v_2(r \pm 1) < k.$$

Say that *$Q$ is given in a canonical form* if one of the following conditions is satisfied.

(A1) $t = 0$, $k \le 1$ and $\lambda \le k + 1$.
(A2) $t = 0$, $k \ge 2$, $\kappa + \lambda \le 3$, $v_2(r - s) \ge k - 1$, and if $\kappa = 2$ and $r - s \equiv n/2 \bmod 2^k$, then $s \not\equiv -1 + n/2 \bmod 2^k$ and $h$ is even.
(A3) $t = 0$, $k \ge 3$, $\kappa + \lambda \le 3$, $v_2(r - s) \le k - 2$, and if $\kappa = 2$ and $v_2(r + 1) < k$, then $v_2(2h) > k - v_2(r - (-1)^{(r-1)/2})$.
(B2) $t = 0$, $k \ge 2$, $\kappa = 2$, $\lambda \in \{1, 2\}$, $h$ is odd, $r - s \equiv n/2 \bmod 2^k$ and $v_2(r + 1) < k$.
(B3) $t = 0$, $k \ge 3$, $\kappa = 2$, $\lambda \in \{1, 2\}$, $v_2(2h) = k - v_2(r - (-1)^{(r-1)/2})$, $v_2(r + 1) < k$ and $v_2(r - s) \le k - 2$.
(B4) $t = 0$, $k \ge 2$, $\kappa = 2$, $\lambda \in \{1, 2\}$, $s \equiv -1 + n/2 \bmod 2^k$ and $r \equiv -1 \bmod 2^k$.
(C2) $t = n/2$, $k \ge 2$, $\kappa + \lambda \le 3$, $h$ is odd, $v_2(r - s) \ge k$, $v_2(r + 1) < k$ and $s \not\equiv -1 + n/\kappa \bmod 2^k$.
(C3) $t = 2^{k - v_2(2h)}m$, $k \ge 3$, $\kappa + \lambda \le 3$, $h$ is even, $k - v_2(r - 1) < v_2(2h) < k$ and $r \equiv 1 \bmod 4$.
(D2) $t = n/2$, $k \ge 2$, $\kappa + \lambda \le 3$ and $r \equiv s \equiv -1 + n/\kappa \bmod 2^k$.
(E1) $t = m$, $k \ge 1$, $\kappa = 1$, $\lambda \in \{1, 2\}$, $s \equiv 1 \bmod 2^k$ and $v_2(h) + v_2(r + 1) \ge k$.

Recall that if $k = 2$ and $m = 1$, then $\kappa = \lambda = 1$ (since $G \not\cong Q_8$ and $G$ is noncommutative).

**Theorem 5.1.** *If $k = 0$, then $Q$ is strongly $G$-isomorphic to a loop of type (A1). If $k = 1$, then $Q$ is strongly $G$-isomorphic to a loop of type (A1) if and only if $t$ is even, and to a loop of type (E1) if and only if $t$ is odd. In these cases the type, the value $\lambda$, and the set $\{r^j;\, j \in \mathbb{Z}$ and $\gcd(j, 2h) = 1\} \subseteq \mathbb{Z}_n^*$ fully determine the class of all loops that are strongly $G$-isomorphic to $Q$.*

Proof: By Proposition 4.7, the parity of $t$ and the set $\{r^j;\, j \in \mathbb{Z}$ and $\gcd(j, 2h) = 1\}$ are invariant with respect to strong $G$-isomorphisms. By Proposition 4.12, $t$ may be chosen as $t'$, where $t' = 0$ if $t$ is even, and $t' = m$ if $t$ is odd. □

**Theorem 5.2.** *Assume $k \ge 2$. Then $Q = G \rtimes_f^3 C$ is strongly $G$-isomorphic to a loop of one of the types (A2), …,(E1), and that type is uniquely determined. The class of all loops that are strongly $G$-isomorphic to $Q$ is fully determined by the type, by parameters $\kappa$ and $\lambda$, and by the set $\{r^j;\, j \in \mathbb{Z}$ and $\gcd(j, 2h) = 1\} \subseteq \mathbb{Z}_n^*$.*

Proof: First note that for every type the conditions that relate to $r$ depend only upon $\min\{k, v_2(r-1)\}$ and $\min\{k, v_2(r+1)\}$. This value does not change when $r$ is replaced by $r^j$, $j$ odd. On the other hand $r$ can be replaced by every $r^j$, $\gcd(j, 2h) = 1$, and no other value can appear when there are considered loops strongly $G$-isomorphic to $Q$, by Proposition 4.7.

The main part of the proof is to show that exactly one of the types (A2), …, (E1) can apply. When this is settled the uniqueness of $\kappa$ and $\lambda$ has to be discussed. For $\kappa = 1$ the value of $\lambda$ is determined by the structure of $G$, and hence only those types have to be considered which allow for both values of $\lambda$ when $\kappa = 2$. The only such types are (B2), (B3) and (B4).

The parity of $t$ is invariant. Let $t$ be odd. Then (E1) is the only possible choice. By Corollary 4.10 and Proposition 4.12 we can assume that $t = m$. The further properties listed in (E1) follow from the structure of $G$ (which implies that $\kappa = 1$), from Proposition 4.9 (which gives $s \equiv 1 \bmod 2^k$) and from (4.9).

For the rest of the proof let $t$ be even. Put $\sigma = s + 1 + n/\kappa$.

Let there be $v_2(\sigma) \geq k$. Then $r \equiv -1 \bmod 2^{k-1}$, by Lemma 3.4, and we may assume that $t = t'$, by Corollary 4.14. If $t = n/2$ and $r - s \equiv 2^{k-1} \bmod 2^k$, then $a \cdot xy^m \cdot a^{-1} = xy^m \cdot y^{m(t+r-s)} = xy^m$, and so by switching from $x$ to $\tilde{x} = xy^m$ we can assume that $t = 0$ in this case as well (see below). The remaining cases with $t' = n/2$ are those for which $v_2(s-r) \geq k$. They are never $G$-isomorphic to a loop $\tilde{Q}$ with $\tilde{t} = 0$ since in these cases $0 \notin T_G$, by Proposition 4.9, and this does not change, by $T_a(xy^m) = xy^m y^{n/2}$, if $(\kappa, \lambda) = (2, 1)$ is switched to $(\kappa, \lambda) = (2, 2)$. Hence (D2) is the only possible choice.

Let us now have $v_2(\sigma) \geq k$ and $t = 0$. If $v_2(r-s) \geq k$ or $\kappa = 1$, use (A2) and note that no other type applies. If $r - s \equiv n/2 \bmod 2^k$ and $\kappa = 2$, then $v_2(r+1) \geq k$, and hence (B4) is the only applicable type.

To finish the case $v_2(\sigma) \geq k$ it needs to be verified that within type (B4) there do not exist two strongly $G$-isomorphic loops with different values of $\lambda$. If that were true, there would exist $\tilde{a} = a^j y^i$, $j$ odd, and $\tilde{x} = xy^\ell$, $\ell$ odd, such that $T_{\tilde{a}}(\tilde{x}) = \tilde{x}$. By direct computation, $a^j y^i \cdot xy^\ell \cdot y^{-i} a^{-j} = xy^\gamma$, where $\gamma \equiv -ir^j\sigma + s\ell r^j$. Since $v_2(\sigma) \geq k$, $r^j \equiv -1 \bmod 2^k$ and $s \equiv -1 + 2^{k-1} \bmod 2^k$ there is $\gamma \equiv (1 + 2^{k-1})\ell \bmod 2^k$, and hence there cannot be $\gamma \equiv \ell \bmod n$.

For the rest of the proof we thus may assume that $s \not\equiv -1 + n/\kappa \bmod 2^k$ and that $t' = 0$. Define $\delta$ as in Proposition 4.17, i.e. $\delta = v_2(\sigma) + k - 1 - v_2(h) - v_2(r+1)$. Under our assumptions the only types with $t \neq 0$ are (C2) and (C3). Our next aim is to verify that in these types $v_2(t) = \delta < v_2(r-s)$, and that (C2) and (C3) cover all situations when (4.9) holds and $v_2(t) = \delta < v_2(r-s)$. By our assumptions (4.9) holds if and only if $v_2(h) + v_2(r+1) < k$. If this is true, and if $v_2(t) = \delta < v_2(r-s)$, then we can assume that $t = 2^\delta m$, by Corollary 4.15 and Proposition 4.18, and we also know that this is the only possible value of $t$ if $m|t$ is assumed, by Proposition 4.19.

Assume first that $r \equiv 1 \bmod 4$. Then $s \equiv 1 \bmod 2^{k-1}$ by Lemma 3.4 and $v_2(h) + v_2(r+1) = v_2(2h)$. Hence (4.9) is equivalent to $v_2(2h) < k$, and that is assumed by both types (C2) and (C3). Furthermore, in both the types $\delta = v_2(t)$

since $\delta = 1 + k - 1 - v_2(h) - 1 = k - v_2(2h)$. Therefore both types satisfy the assumptions of Proposition 4.21, and what remains is to verify that the description of (C2) and (C3) corresponds to those cases of Proposition 4.21 in which $t = 2^\delta m$ and $v_2(r - s) > \delta$.

If $k = 2$, then Proposition 4.21 requires $s \equiv 1 \bmod 4$ and $\kappa = 1$ while (C2) has $s \equiv 1 \bmod 4$ and $s \not\equiv 3 + n/\kappa \bmod 4$ which is the same thing. Assume $k \geq 3$. If $h$ is odd, then the correspondence between (C2) and Proposition 4.21 is immediately clear. For $h$ even Proposition 4.21 states that $v_2(r - s) > \delta$ if and only if $v_2(r - 1) > \delta = k - v_2(2h)$ which is also a claim of (C3).

Let us now have $r \equiv 3 \bmod 4$. Then only applicable type is (C2), and by its assumptions $k \geq 3$ and $s \equiv -1 \bmod 2^{k-1}$. The assumptions of (C2) also yield that $r \equiv -1 + 2^{k-1} \bmod 2^k$. Hence there cannot be $\kappa = 2$ since that would imply $v_2(\sigma) \geq k$. Therefore $r \equiv s \equiv -1 + 2^{k-1} \bmod 2^k$, $k \geq 3$ and $\kappa = 1$ are the conditions that are expressed by (C2) if $r \equiv 3 \bmod 4$. Under these conditions (4.9) holds since $v_2(h) + v_2(r + 1) = k - 1 < k$, and $v_2(t) = \delta$ since $\delta = k-1+k-1-(k-1) = k-1$. By Proposition 4.20 type (C2), for $r \equiv 3 \bmod 4$, describes completely the situations when $r \equiv 3 \bmod 4$, (4.9) holds, $v_2(t) = \delta$ and $v_2(r - s) > \delta$, by Proposition 4.20.

By Proposition 4.19 we thus know that if $Q$ is not strongly isomorphic to a loop of type (C2) or (C3), then it is isomorphic to a loop $\tilde{Q}$ with $\tilde{t} = 0$. We can thus assume that $t = 0$. The only applicable types are (A2), (A3), (B2) and (B3). It is clear that no two of them can apply simultaneously. Note that the claim $v_2(r + 1) < k$ in (B2) is equivalent to the claim $s \not\equiv -1 + n/2 \bmod 2^k$, i.e. to $v_2(\sigma) < k$. Hence if $\lambda = 1$ then any situation that is excluded from (A2) and (A3) when $\kappa = 2$ is covered by (B2) and (B3), respectively. This makes for all possible situations in which a complement yielding $t = 0$ can be found without violating the initial assumption $\kappa + \lambda \leq 3$. The remaining situations are those that correspond to point (2) of Proposition 4.19, i.e. all cases with an application of Proposition 4.19 in a situation when (4.9) $v_2(t) = \delta$, $\kappa = 2$ and $v_2(r - s) = \delta$. These cases are described in detail by Propositions 4.20 and 4.21. To finish the proof we thus need to verify, by Proposition 4.19, that there is a one-to-one correspondence between these situations and those situations described by (B2) and (B3) in which $\lambda = 2$.

Note that $t = 2^\delta m$ can be assumed when Proposition 4.20 or 4.21 is being applied, by Proposition 4.18. If $r \equiv 3 \bmod 4$, then $k \geq 3$, $v_2(2h) = k - v_2(r + 1)$, by Proposition 4.20 (which implies that $v_2(r + 1) < k$). Let this be true. Then (4.9) always holds and $\delta = v_2(\sigma)$. If $s \equiv 1 \bmod 2^{k-1}$, then $v_2(r - s) = 1 = \delta$, and what we get is exactly type (B3) for $r \equiv 3 \bmod 4$. If $s \equiv -1 \bmod 2^{k-1} \bmod 2^k$, then $s \equiv -1 \bmod 2^k$ (since $v_2(\sigma) < k$), and $r \equiv -1+2^{k-1} \bmod 2^k$, by Lemma 3.4. We get exactly the condition of type (B2) for $s \equiv -1 \bmod 2^{k-1}$.

Suppose now that $r \equiv 1 \bmod 4$. Then $s \equiv 1 \bmod 2^{k-1}$, by Lemma 3.4. If $k = 2$, then $s \equiv 3 \bmod 4$, as $v_2(\sigma) < k$. Condition (4.9) holds if and only if $v_2(2h) < k$, and then $\delta = k - v_2(2h)$. Let this be true. Consider the description of case $v_2(r-s) = \delta$ in Proposition 4.21. If $k = 2$, then $\delta = 1 = v_2(2h) = v_2(r-s)$.

That gives the same parameters as type (B2) for $k = 2$. Assume $k \geq 3$. If $h$ is even, then $v_2(2h) = k - v_2(r - 1)$ (and $\delta \leq k - 2$). This gives type (B3) for $r \equiv 1 \bmod 4$. If $h$ is odd, then $r - s \equiv 2^{k-1} \bmod 2^k$, and that is exactly type (B2) for $s \equiv 1 \bmod 2^{k-1}$, $k \geq 3$. □

The following statement can be verified directly.

**Proposition 5.3.** *Let $Q = G \rtimes^3_f C$ be given in a canonical form, $k \geq 2$ and $t$ is even. Put $\sigma = s + 1 + n/\kappa$.*

(i) *If $v_2(\sigma) \geq k$, then $Q$ is of type (A2), (A3), (B4) or (D2). If $Q$ is of type (B4) or (D2), then $v_2(\sigma) \geq k$.*
(ii) *If $v_2(\sigma) < k$ and $k = 2$, then $Q$ is of type (A2), (B2) or (C2).*
(iii) *Suppose that $h$ is odd and that $v_2(\sigma) < k$. Then $Q$ is of type (A2), (A3), (B2), (B3) and (C2). If $Q$ is of type (A3) or (B3), then $s \equiv 1 \bmod 2^{k-1}$ and $r \equiv -1 \bmod 2^{k-1}$.*
(iv) *If $h$ is even and $v_2(\sigma) < k$, then $Q$ is of type (A2), (A3), (B3) or (C3).*

**Theorem 5.4.** *Let $r, s, t, h \in \mathbb{Z}$ be such that, for a given group $G$, one of the conditions (A1),...,(E1) is satisfied. If $(r+1)(s-1) \equiv t(s-1) \equiv s^2-1 \equiv 0 \bmod n$, $3 \nmid h$, $\operatorname{ord}_n(r)|2h$, $2h = |C|$, $C = \langle b\rangle$ and $f = f_s\alpha_{t,r}$, then $Q = G \rtimes^3_f C$ is always well defined. If $k \geq 1$, then*

$$k - v_2(r - (-1)^{\frac{r-1}{2}}) \leq v_2(\operatorname{ord}_n(r)).$$

Proof: The operation (2.6) is well defined if and only if $f^{2h} = \mathrm{id}_G$. By Lemma 3.4 this happens if and only if $r^{2h} \equiv 1 \bmod n$ (which is assumed) and $t(1 + r + \cdots + r^{2h-1}) \equiv 0 \bmod n$. The latter is clearly true if $t = 0$. Hence $k \geq 1$ and $t \neq 0$ can be assumed. Since $m|t$ in every of the types (A1),...,(E1), we are, in fact, asking when $v_2(1 + r + \cdots + r^{2h-1}) \geq k$. By Lemma 4.11 this is equivalent to (4.8), i.e. to $v_2(t) + v_2(h) + v_2(r + 1) \geq k$. If $t$ is odd, then there applies (E1) which assumes that $v_2(h) + v_2(r + 1) \geq k$. Let $t$ be even. The inequality clearly holds if $t = n/2$. Hence (C3) is the only case to investigate. However, in that case $v_2(t) = k - v_2(2h)$.

The concluding inequality of the theorem expresses the fact that $\operatorname{ord}_{2^k}(r)$ divides $\operatorname{ord}_n(r)$. □

The group $G$ certainly possesses, within the loop $Q = G \rtimes^3_f C$, a complement $\tilde{C}$ such that $\tilde{C} \leq \langle a, y\rangle$. A trivial example is $\tilde{C} = C$. However, in general it does not seem to be always immediately clear whether there exists a complement $\tilde{C} = \langle\tilde{a}\rangle$ such that $\tilde{a} \in Q \setminus \langle a, y\rangle$. If $t = 0$ (i.e. $[a, x] = 1$), then such a complement clearly exists if $h$ is even or if $\lambda = 1$ since then it suffices to put $\tilde{a} = ax$.

Call $Q$ *unpaired* (with respect to $G$) if it contains no complement to $G$ that would nontrivially intersect $G \setminus \langle a, y\rangle$. Clearly, this happens if and only if $(xy^i \cdot a)^{2h} \neq 1$ for every $i \in \mathbb{Z}$. By direct computation,

$$(xy^i \cdot a)^2 = x^2y^{in/\kappa}y^{t+(r-s)i} \cdot a^2 \text{ for every } i \in \mathbb{Z}. \tag{5.1}$$

If $h$ is even, then $(xy^i \cdot a)^{2h} = y^\gamma$, where $\gamma \equiv (t + (r-s)i)(1 + r^2 + \cdots + (r^2)^{h-1}) \bmod n$. Hence $v_2(\gamma) = v_2(h) + v_2(t + (r-s)i)$, by Corollary 4.11. Since $v_2(t + (r-s)i) = v_2(t + (r-s)im)$ it is clear that if $h$ is even and $m$ divides $t$, then $Q$ is unpaired if and only if

$$v_2(t + (r-s)mi) < k - v_2(h) \text{ for every } i \in \mathbb{Z}. \tag{5.2}$$

**Proposition 5.5.** *Let $Q = G \rtimes_f^3 C$ be of type (E1). Then $Q$ is unpaired if and only if $v_2(h) < k$.*

Proof: Since $t = m$ is odd and $r - s$ is even, there is $v_2(t + (r-s)mi) = 0$ for every $i \in \mathbb{Z}$. For $h$ even the statement thus follows from (5.2). Let $h$ be odd. Then $Q$ is always unpaired, since $(xy^i \cdot a)^2 \in \langle y \rangle \setminus \langle y^2 \rangle$ for every $i \in \mathbb{Z}$, by (5.1). □

**Proposition 5.6.** *Let $Q = G \rtimes_f^3 C$ be given in a canonical form. Suppose that $h$ and $t$ are even, and that $k \geq 2$. Then $Q$ is unpaired if and only if it is of type (C3).*

Proof: If $t \in \{0, n/2\}$, then the inequality (5.2) gets violated if $i$ is set to 0. Hence only the type (C3) needs to be considered. In that case $v_2(t) = k - v_2(2h)$. Furthermore, if $v_2(r-s) < k-1$, then $v_2(r-s) = v_2(r-1)$ (there is $r \equiv 1 \bmod 4$, and thus $s \equiv 1 \bmod 2^{k-1}$ by Lemma 3.4). Therefore $v_2(r-s) > k - v_2(2h)$ and $v_2(t) = v_2(t + (r-s)im)$ for every $i \in \mathbb{Z}$. This means that (5.2) is satisfied by every instance of type (C3). □

If $k \leq 1$ and $t = 0$, then $\langle xa \rangle$ is a complement to $G$ if $\lambda = 1$, and $\langle xy^m \cdot a \rangle$ if $\lambda = 2$. Hence $Q$ of type (A1) is never unpaired. For a description of unpaired quasigroups $Q$ it thus remains to investigate types with $t$ even, $h$ odd and $k \geq 2$. Then $t \in \{0, n/2\}$ and, by (5.1), we need to know whether $x^2 y^t y^{((r-s)+n/\kappa)i}$ is of an odd order for some $i \in \mathbb{Z}$. Since $x^2 y^t \in \{1, y^{n/2}\}$ it is clear that such an $i$ always exists if $v_2(n/\kappa + (r-s)) < k$. Hence $Q$ is unpaired if and only if $v_2(n/\kappa + (r-s)) \geq k$ and, at the same time, $x^2 y^t = y^{n/2}$. By inspecting the list of types we immediately obtain:

**Proposition 5.7.** *Let $Q = G \rtimes_f^3 C$ be given in a canonical form. Suppose that $h$ is odd, $t$ is even and $k \geq 2$. Then $Q$ is unpaired exactly in the following cases:*

(i) *$Q$ is of type (A2), $\kappa = 1$, $\lambda = 2$ and $v_2(r-s) \geq k$;*
(ii) *$Q$ is of type (B2) or of type (B4), and $\kappa = \lambda = 2$; and*
(iii) *$Q$ is of type (C2) or of type (D2), and $\kappa = \lambda = 1$.*

If $Q$ is not unpaired, then it is *paired* (with respect to $G$). If $Q$ is paired, then there exists $i \in \mathbb{Z}$ such that $xy^{im} \cdot a$ generates a complement to $G$ in $Q$. Setting $\tilde{a} = xy^{im} \cdot a$ yields a representation of $Q$ that, in conjunction with the original representation (which we may assume to be given in a canonical form), fully determines (when transformed to a canonical form) the class of all loops that are $G$-isomorphic to $Q$. Of course, if $Q$ is unpaired, then such a class is also fully determined by a canonical form of $Q$. But then there is only one such form.

Now, by Theorems 5.1 and 5.2 the class of loops that are strongly $G$-isomorphic to $Q$ is fully determined by $\kappa$, $\lambda$, $\{r^j \bmod n;\ \gcd(j,2h)=1\}$ and the type. If $Q$ is paired, then the paired complements yield the set $\{-sr^j(1+n/\kappa) \bmod n;$ $\gcd(j,2h)=1\}$, by Proposition 4.7. The parameter $\kappa$ is not affected by pairing, but the parameter $\lambda$ may change if $\kappa = 2$ (in fact, as we shall observe, this never happens when $h$ is even). Our next aim is to describe the *paired type* in every case. Note that the type does not change when $v_2(s+1+n/\kappa) \geq k$ (cf. (4.4) and (4.5)) since in that case $-s(1+n/\kappa) \equiv (-s)(-s) \equiv 1 \bmod 2^k$.

**Lemma 5.8.** *Assume $k \geq 2$. Let $r' \in \mathbb{Z}$ be such that $r' \equiv -rs(1+n/\kappa) \bmod n$. Then $r' \equiv s - r + n/\kappa - 1 \bmod n$. The following is true if $k \geq 3$:*

(i) *$v_2(r'-s) \geq k-1 \Leftrightarrow v_2(r+1) \geq k-1$, and*

(ii) *if $s \equiv 1 \bmod 2^{k-1}$, then $r' \equiv -r \bmod 2^{k-1}$. In particular $r \equiv \pm 1 \bmod 2^{k-1} \Leftrightarrow r' \equiv \mp 1 \bmod 2^{k-1}$.*

Proof: By Lemma 3.4, $rs \equiv r - s + 1 \bmod n$. The rest is easy. □

**Proposition 5.9.** *Let $Q$ be given in a canonical form and let it be paired. If $k \leq 1$ or if $t$ is odd, then the paired and original types always agree. This is also true if $k = 2$ and $h$ is even. If $k \geq 3$ and $h$ is even, then the types agree with the exception of the following two cases (which are switched by the pairing):*

(1) *$Q$ is of type (A) and $s \equiv 1 \bmod 2^{k-1}$ (then $r \equiv 1 \bmod 2^{k-1}$), and*

(2) *$Q$ is of type (A3), $s \equiv 1 \bmod 2^{k-1}$ and $r \equiv -1 \bmod 2^{k-1}$.*

*The parameters $\kappa$ and $\lambda$ of the paired and original type always agree.*

Proof: The value of $\lambda$ needs to be discussed only if one of the types is (B2) or (B3) since these are the only types for which the transformation to the canonical form can change the initial assumption $\kappa + \lambda \leq 3$.

If $k = 0$, then the only type is (A1). Assume $k \geq 1$. If $t$ is odd, then the only available type is (E1) since the parity of $t$ is invariant, by Proposition 2.8. Let $t$ be even. If $k = 1$, then the only available type is again (A1). Assume $k \geq 2$, and let $h$ is even. Put $\sigma = s + 1 + n/\kappa$. If $v_2(\sigma) \geq k$, then the type does not change and is different from (B2) and (B3). Hence $v_2(\sigma) < k$ may be assumed. If $k = 2$, then the only available type is (A2), by Proposition 5.3. Suppose thatf $k \geq 3$.

Let there be $s \equiv -1 + 2^{k-1} + n/\kappa \bmod 2^k$. Then $v_2(r-s) \geq k-1$ is always true, by Lemma 3.4, and hence (A2) is the only available type once more.

Let us have $s \equiv 1 \bmod 2^{k-1}$. We need to consider types (A2), (A3) and (B3), by Propositions 5.3 and 5.6. In all these types $\langle ax \rangle$ is a complement to $G$ since $[a,x] = 1$ and $h$ is even. In type (B3) there is $v_2(r+1) < k-1$ since $v_2(r+1) = k-1$ implies that $h$ is odd.

Define $r'$ so that $r' \equiv -rs(1+n/\kappa) \bmod n$. If $Q$ is of type (B3), then $r \not\equiv \pm 1 \bmod 2^{k-1}$, and hence $r' \not\equiv \pm 1 \bmod 2^{k-1}$ as well, by Lemma 5.8. Furthermore, $r \not\equiv r' \bmod 4$ implies that $\rho' = (-1)^{(r'-1)/2}$ is equal to $-\rho$, where $\rho = (-1)^{(r-1)/2}$, and thus $v_2(r-\rho) = v_2(-r+\rho) = v_2(r'-\rho')$, by Lemma 5.8. Therefore (B3) is paired with itself when $h$ is even, and there is no change to $\lambda$ since $T_{ax} \restriction G = f_s\alpha_{0,r'}$, by (4.5) and (4.4).

If $Q$ is of type (A3), then $v_2(r' - s) < k-1$ unless $r \equiv -1 \bmod 2^{k-1}$, by Lemma 5.8. If $r \equiv -1 \bmod 2^{k-1}$, then we get the switch that is described in the statement. □

Put $z = b^h = a^h$, and set $\bar{f} = T_z \restriction G$. Then $\bar{f} = (f_s)^h \alpha_{\bar{t},\bar{r}}$, where

$$\bar{t} \equiv t(1 + r + \cdots + r^{h-1}) \bmod n \text{ and } \bar{r} \equiv r^h \bmod n, \tag{5.3}$$

by Lemma 3.4. The properties of $\bar{r}$ and $\bar{t}$ will be used extensively in the ensuing section. Here we shall need only the fact that $\bar{r} \equiv r \bmod 2^k$ if $h$ is odd.

**Lemma 5.10.** *Suppose that $Q$ is given in a canonical form. Then $\bar{r}^2 \equiv 1 \bmod n$, and $\bar{t} = 0$ if $t = 0$. Assume that $k \geq 2$.*

(i) *If $h$ is even, then $\bar{t} \equiv 0 \bmod n$ if $t = n/2$. Furthermore, $\bar{r} \equiv 1 \bmod 4$ and $\bar{r} \equiv 1 \bmod 2^{k-1}$.*
(ii) *If $h$ is odd, then $\bar{r} \equiv r \bmod 2^k$ and $r^2 \equiv 1 \bmod 2^k$. Furthermore, $\bar{t} = t$ if $t \in \{0, n/2\}$, and $\bar{t}$ is odd if $t = m$.*

Proof: The statement follows from (5.3) since $r^{2h} \equiv \bar{r}^2 \equiv 1 \bmod n$. In particular, if $h$ is even and $k \geq 2$, then $\bar{r}$ is a square modulo $2^k$, and thus $\bar{r} \equiv 1 \bmod 4$ (and hence $\bar{r} \equiv 1$ or $\bar{r} \equiv 1 + 2^{k-1} \bmod 2^k$). If $h$ is odd and $k \geq 2$, then $r \equiv r^{2h+1} \equiv \bar{r}r^{h+1} \equiv \bar{r}(r^2)^{(h+1)/2} \bmod n$, and there is $r^2 \equiv 1 \bmod 2^k$ since, clearly, $\mathrm{ord}_{2^k}(r^2)$ divides the odd integer $h$. □

**Lemma 5.11.** *Assume that $h$ is odd, $t$ even and $k \geq 2$. Let $Q$ be given in a canonical form. Then $Q$ is paired to a loop that is strongly $G$-isomorphic to a loop of type (C2) if and only if $\lambda = 2$, and*

(1) *$Q$ is of type (A2), $\kappa = 1$, $s \equiv -1 + 2^{k-1} \bmod 2^k$ and $r \equiv -1 \bmod 2^k$; or*
(2) *$Q$ is of type (A3), $\kappa = 1$, $s \equiv 1 \bmod 2^{k-1}$, $k \geq 3$, $r \equiv -1 \bmod 2^k$; or*
(3) *$Q$ is of type (B3), $\lambda = 2$, $s \equiv 1 \bmod 2^{k-1}$, $k \geq 3$, $r \equiv -1 + 2^{k-1} \bmod 2^k$.*

Proof: The pairing is symmetric. Hence we may start from a loop of type (C2). Our starting assumptions thus include that $\kappa \neq \lambda$, by Proposition 5.7. In the proof the value of $\lambda$ is that of (C2). The value in the paired type will be denoted by $\lambda'$. Of course, $\lambda' = \lambda$ if $\kappa = 1$.

If $s \equiv -1 \bmod 2^{k-1}$, then $s \equiv -1 + 2^{k-1} \bmod 2^k$ and $\kappa = 1$ since $v_2(r-s) \geq k$, $v_2(r+1) < k$ and $v_2(s+1+n/\kappa) < k$, by the assumptions of (C2). In particular, if $k = 2$, then $r \equiv s \equiv 1 \bmod 4$ and $\kappa = 1$.

Set $r' = -sr(1 + n/\kappa)$. By Lemma 5.8, $r' \equiv n/\kappa - 1 \bmod 2^k$. Thus $s \equiv -1 \bmod 2^{k-1}$ gives $r' \equiv -1 \bmod 2^k$, and the only possibility for the paired type is that of (A2) (case (1) of the statement).

For the rest of the proof it can be assumed that $s \equiv 1 \bmod 2^{k-1}$ and $k \geq 3$. Suppose first that $\kappa = 1$. Then $r' \equiv -1 \bmod 2^k$, $v_2(r' - s) = 1$, and (A3) in the form of case (2) is the only possibility.

Let there be $\kappa = 2$. Then $r' \equiv -1 + 2^{k-1} \bmod 2^k$. Thus $v_2(r' - s) = 1 = k - v_2(r' + 1) = v_2(2h)$, and (B3) is the only possibility. What remains is to determine $\lambda'$. The question is what are the complements $\langle \tilde{a} \rangle$, $\tilde{a} = a \cdot xy^i$, and what are the possible choices of $\tilde{x} = xy^j$ such that $[\tilde{a}, \tilde{x}] = 1$. Now, $(xy^i \cdot a)^2 = y^{(i+1)n/2} y^{(r-s)i} \cdot a^2$ by (5.1). Since $\langle \tilde{a} \rangle$ should be a complement to $G$, the integer $i$ has to be odd as $v_2(r-s) \geq k$. By (4.4) and (4.5) $T_{\tilde{a}}(xy^j) = xy^\gamma$ where $\gamma \equiv s(n/2 + ir(s+1+n/2)) + sr'j \bmod n$. Hence $\gamma \equiv 2i - j \bmod 2^{k-1}$. If $T_{\tilde{a}}(xy^j) = xy^j$, then $2i - j \equiv j \bmod 2^{k-1}$. Thus $i \equiv j \bmod 2^{k-2}$, and $j$ is odd. Hence $[\tilde{a}, \tilde{x}] = 1$ implies that $(\tilde{x})^2 = y^{n/2}$, and we see that case (3) really has $\lambda' = 2$. □

If $k \geq 2$, $h$ is odd, $t$ is even and $s \not\equiv -1 + n/\kappa \bmod 2^k$, then Lemma 5.11 describes all cases when pairing induces a change of $t$. Also, Lemma 5.11 states that $t = 0$ in at least one of the paired types. In the cases that are not covered by Lemma 5.11 it is therefore possible to determine the paired type by Lemma 5.8 in a straightforward way, using only the values of $r$ and $s$ modulo $2^k$. By doing this a characterization of classes up to a $G$-isomorphism gets finished in all cases when $k \geq 2$, $t$ is even and $h$ is odd (the other cases are covered by Propositions 5.5, 5.6 and 5.9). For each value of $s$ modulo $2^k$ (i.e. $1$, $1 + 2^{k-1}$, $-1$ and $-1 + 2^{k-1}$) the result is presented below in a tabular form where in each row there are specified the values of $r \bmod 2^k$ and of $t$ with respect to a canonical form (note that $r^2 \equiv 1 \bmod 2^k$, by Lemma 5.10). The classes up to a $G$-isomorphism corresponding to these parameters will be called a *$G$-type* and will be denoted by a small letter $\mathrm{x} \in \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \dots\}$ (for each value of $s$ modulo $2^k$ the letters are used independently — the full information is thus carried by a pair $(s \bmod 2^k, \mathrm{x})$). If $m = 1$, then the $G$-type describes a class up to a $G$-isomorphism completely. For $m > 1$ we also need to know what are the values $s$ and $r$ modulo $m$.

| $G$-type | $r \bmod 2^k$ | $t$ | $\kappa$ | $\lambda$ | type |
|---|---|---|---|---|---|
| a1 | $-1$ | 0 | 1 | 1 | (A2) |
| a2 | $-1{+}2^{k-1}$ | 0 | 1 | 1 | (A2) |
| b1 | $-1$ | 0 | 1 | 2 | (A2) |
| b2 | $-1{+}2^{k-1}$ | $\frac{n}{2}$ | 1 | 2 | (C2) |
| c0 | $-1{+}2^{k-1}$ | 0 | 1 | 2 | (A2) |
| d3 | $-1{+}2^{k-1}$ | 0 | 2 | 1 | (A2) |
| e3 | $-1$ | 0 | 2 | 1 | (B4) |
| f0 | $-1$ | 0 | 2 | 2 | (B4) |
| g0 | $-1{+}2^{k-1}$ | $\frac{n}{2}$ | 1 | 1 | (C2) |
| h3 | $-1{+}2^{k-1}$ | $\frac{n}{2}$ | 2 | 1 | (D2) |

| $G$-type | $r \bmod 2^k$ | $t$ | $\kappa$ | $\lambda$ | type |
|---|---|---|---|---|---|
| a3 | $-1$ | 0 | 1 | 1 | (A2) |
| b0 | $-1$ | 0 | 1 | 2 | (A2) |
| c1 | $-1$ | 0 | 2 | 1 | (A2) |
| c2 | $-1{+}2^{k-1}$ | 0 | 2 | 1 | (B2) |
| d3 | $-1{+}2^{k-1}$ | 0 | 1 | 1 | (A2) |
| e3 | $-1{+}2^{k-1}$ | 0 | 1 | 2 | (A2) |
| f0 | $-1{+}2^{k-1}$ | 0 | 2 | 2 | (B2) |
| g0 | $-1$ | $\frac{n}{2}$ | 1 | 1 | (D2) |
| h3 | $-1$ | $\frac{n}{2}$ | 1 | 2 | (D2) |

Table 1. Canonical forms for $h$ odd, $k \geq 2$, $t$ even where either $s \equiv -1 + 2^{k-1} \bmod 2^k$ (the columns on the left), or $s \equiv -1 \bmod 2^k$ (the columns on the right). If $k = 2$ and $m = 1$, then the eligible $G$-types are a, g if $s = 1$, and a, d, g if $s = 3$.

The rows of the tables are labelled x$i$, where x is the $G$-type and $i \in \{0, 1, 2, 3\}$. If $i = 0$, then the corresponding loops are unpaired. If $i = 3$, then they are paired with a loop that yields the same parameter values modulo $2^k$ (this happens if and only if $s \equiv -1 + n/\kappa \bmod 2^k$). In the other cases there are two different pairs $(r \bmod 2^k, t)$ and they are related by pairing. One of them is labelled as x1, and the other as x2. Call x$i$ a *G-subtype*.

The tables for $s \equiv -1 \bmod 2^k$ and $s \equiv -1+2^{k-1} \bmod 2^k$ include the case $k = 2$ (Table 1), while the tables for $s \equiv 1 \bmod 2^k$ and $s \equiv 1 + 2^{k-1} \bmod 2^k$ assume that $k \geq 3$ (Table 2).

Group case (2.7) belongs to $G$-type d, $s \equiv -1 + 2^{k-1}$. $G$-type d may be thus omitted when $s = 1$ and $k = 2$.

| $G$-type | $r \bmod 2^k$ | $t$ | $\kappa$ | $\lambda$ | type |
|---|---|---|---|---|---|
| a1 | $1$ | $0$ | $1$ | $1$ | (A2) |
| a2 | $-1$ | $0$ | $1$ | $1$ | (A3) |
| b0 | $1$ | $0$ | $1$ | $2$ | (A2) |
| c1 | $1$ | $0$ | $2$ | $1$ | (A2) |
| c2 | $-1+2^{k-1}$ | $0$ | $2$ | $1$ | (B3) |
| d1 | $1+2^{k-1}$ | $0$ | $1$ | $1$ | (A2) |
| d2 | $-1+2^{k-1}$ | $0$ | $1$ | $1$ | (A3) |
| e1 | $1+2^{k-1}$ | $0$ | $1$ | $2$ | (A2) |
| e2 | $-1+2^{k-1}$ | $0$ | $1$ | $2$ | (A3) |
| f1 | $-1$ | $0$ | $1$ | $2$ | (A3) |
| f2 | $1$ | $\frac{n}{2}$ | $1$ | $2$ | (C2) |
| g1 | $-1$ | $0$ | $2$ | $1$ | (A3) |
| g2 | $1+2^{k-1}$ | $0$ | $2$ | $1$ | (B2) |
| h0 | $1+2^{k-1}$ | $0$ | $2$ | $2$ | (B2) |
| i1 | $-1+2^{k-1}$ | $0$ | $2$ | $2$ | (B3) |
| i2 | $1$ | $\frac{n}{2}$ | $2$ | $1$ | (C2) |
| j0 | $1$ | $\frac{n}{2}$ | $1$ | $1$ | (C2) |

| $G$-type | $r \bmod 2^k$ | $t$ | $\kappa$ | $\lambda$ | type |
|---|---|---|---|---|---|
| a1 | $1$ | $0$ | $1$ | $1$ | (A2) |
| a2 | $-1+2^{k-1}$ | $0$ | $1$ | $1$ | (A3) |
| b1 | $1$ | $0$ | $1$ | $2$ | (A2) |
| b2 | $-1+2^{k-1}$ | $0$ | $1$ | $2$ | (A3) |
| c1 | $1+2^{k-1}$ | $0$ | $1$ | $1$ | (A2) |
| c2 | $-1$ | $0$ | $1$ | $1$ | (A3) |
| d0 | $1+2^{k-1}$ | $0$ | $1$ | $2$ | (A2) |
| e1 | $1+2^{k-1}$ | $0$ | $2$ | $1$ | (A2) |
| e2 | $-1+2^{k-1}$ | $0$ | $2$ | $1$ | (B3) |
| f1 | $-1$ | $0$ | $2$ | $1$ | (A3) |
| f2 | $1$ | $0$ | $2$ | $1$ | (B2) |
| g1 | $-1$ | $0$ | $1$ | $2$ | (A3) |
| g2 | $1+2^{k-1}$ | $\frac{n}{2}$ | $1$ | $2$ | (C2) |
| h0 | $1$ | $0$ | $2$ | $2$ | (B2) |
| i1 | $-1+2^{k-1}$ | $0$ | $2$ | $2$ | (B3) |
| i2 | $1+2^{k-1}$ | $\frac{n}{2}$ | $2$ | $1$ | (C2) |
| j0 | $1+2^{k-1}$ | $\frac{n}{2}$ | $1$ | $1$ | (C2) |

TABLE 2. Canonical forms for $h$ odd, $k \geq 3$, $t$ even where either $s \equiv 1 \bmod 2^k$ (columns on the left), or $s \equiv 1 + 2^{k-1} \bmod 2^k$ (columns on the right).

## 6. Classification up to isomorphism

Put $z = a^h = b^h$ and define $\bar{r}$ and $\bar{t}$ so that $T_z \restriction G = f_s \alpha_{\bar{t},\bar{r}}$. Some of the properties of $\bar{r}$ and $\bar{t}$ have been mentioned in Lemma 5.10.

**Lemma 6.1.** *Let $h$ and $n$ be even and let $Q$ be given in a canonical form. Then:*

(i) $\bar{t} \equiv n/2 \bmod n$ *if and only if $Q$ is of type (C3);*

(ii) $\bar{r} \equiv 1 + n/2 \bmod n$ *if and only if there hold both* $v_2(2h) = k - v_2(r - (-1)^{(r-1)/2})$ *and* $r^h \equiv 1 \bmod m$. *If* $\bar{r} = 1 + n/2$, *then* $\bar{t} = 0$, $k \geq 3$, $s \equiv 1 \bmod 2^{k-1}$ *and* $r \not\equiv \pm 1 \bmod 2^{k-1}$; *and*

(iii) *if* $k = 2$, *then* $r^h \equiv -1 \bmod m$ *if and only if* $\bar{r} \equiv -1 + 2m \bmod n$. *Let this be true. Then* $p \equiv 1 \bmod 4$ *whenever* $p|m$ *is a prime,* $s \equiv 1 \bmod 2m$, *and* $r^j \not\equiv -1 \bmod n$ *for every* $j \in \mathbb{Z}$. *Furthermore, there exists* $i \in \mathbb{Z}$ *such that* $-r + 2m = r^i$, $\gcd(i, 2h) = 1$.

Proof: By Lemma 5.10, $\bar{t} \equiv 0 \bmod n$ if $t \in \{0, n/2\}$, and $\bar{t}$ is odd if $t$ is odd. Therefore (C3) is the only type to consider if $\bar{t} = n/2$, by Theorems 5.1 and 5.2. By (5.3), $\bar{t} \equiv t(1+r+\dots+r^{h-1}) \bmod n$. By Lemma 4.11, $v_2(\bar{t}) = v_2(h)+v_2(t)+1$ since $r \equiv 1 \bmod 4$. Therefore, by the conditions of (C3), $v_2(\bar{t}) = k - 1$. There is $m|\bar{t}$, and so $\bar{t} = n/2$.

Put $\gamma = v_2(2h)$. The first claim of point (ii) is immediate for $k \geq 3$ since $\bar{r} \equiv 1 + n/2 \bmod n$ if and only if $m$ divides $\bar{r} - 1$ and $\mathrm{ord}_{2^k}(r) = 2^\gamma$. There cannot be $k = 1$ since $\bar{r}$ is odd, and there cannot be $k = 2$ since $\bar{r} \equiv 1 \bmod 4$. From $r \equiv \pm 1 \bmod 2^{k-1}$ it follows that $\gamma \leq 1$, a contradiction to $h$ being even. Therefore $v_2(r+1) < k-1$, and so $s \not\equiv -1 \bmod 2^{k-1}$, by Lemma 3.4. Furthermore, $\bar{t} \in \{0, n/2\}$ by Lemma 5.10 and the previous part of the proof, with $\bar{t} = n/2$ if and only if $Q$ is of type (C3). In such a case $k - v_2(r-1) < \gamma = v_2(2h)$, and so $\bar{r} \not\equiv 1 + n/2 \bmod n$.

Assume $n = 4m$. Then $r^h \equiv -1 + 2m \bmod n$ trivially implies that $r^h \equiv -1 \bmod m$. Let the latter be true. Then $\bar{r}$ is congruent modulo $n$ to one of $m-1$, $2m-1$, $3m-1$ and $n-1$. The only possible case is that of $2m-1$ since $\bar{r} \equiv 1 \bmod 4$. Assume that $p|m$ is a prime. Then $-1 \equiv r^h \bmod p$ is a square, and hence $p \equiv 1 \bmod 4$. To show that $s \equiv 1 \bmod 2m$ it suffices to prove that $s \equiv 1 \bmod m$ since $s$ is odd. If there is a prime power $q|m$ such that $s \not\equiv 1 \bmod q$, then $s \equiv -1 \bmod q$. From $(s-1)(r+1) \equiv 0 \bmod q$ there follows that then $r \equiv -1 \bmod q$, and $r^h \equiv 1 \bmod q$ ($h$ is even), a contradiction.

Assume that $r^j \equiv -1 \bmod n$ for some $j \in \mathbb{Z}_n$. Then $j$ has to be odd since $n = 4m$. Thus $r^j \equiv r^h \equiv -1 \bmod m$, where $h$ is even and $j$ is odd. That is a contradiction. Finally, note that $r^{h+1} \equiv r(2m-1) \equiv -r + 2m \bmod n$ and that $(r^{h+1})^{h-1} = r^{h^2-1} = r^{-1}$. □

We are now ready to solve completely the isomorphism problem for the case of $h$ even. The solution builds upon Theorems 5.1 and 5.2, and upon Propositions 5.5 and 5.6 (recall that a type with $t = 0$ is always paired). It is presented in Theorems 6.2 and 6.3. These two theorems have a common proof that follows the statement of Theorem 6.3.

**Theorem 6.2.** *Let* $h$ *be even. Loops* $G \rtimes^3_f C \cong G \rtimes^3_{\tilde{f}} C$, *each of them in a canonical form, that are not* $G$*-isomorphic exist if and only if (a)* $k = 2$, *(b)* $r^h \equiv \tilde{r}^h \equiv -1 \bmod m$, *(c)* $r$ *and* $\tilde{r}$ *may be chosen to that* $r + \tilde{r} \equiv 0 \bmod n$, *and*

(1) *either* $s \equiv 1 \bmod n$, $\kappa = 2$, *one loop is of type (D2) and the other of type (B4) (with* $\lambda = 2$*);*
(2) *or* $s \equiv 1 + 2m \bmod n$, $\lambda = 2$, $\kappa = 1$, *and both loops are of type (A2).*

**Theorem 6.3.** *Let $h$ be even. Loops $G \rtimes^3_f C \cong \tilde{G} \rtimes^3_{\tilde{f}} C$, each of them in a canonical form, such that $G \ncong \tilde{G}$ exist if and only if (a) $k \geq 3$, (b) $r^h \equiv 1 \bmod m$, (c) $r$ and $\tilde{r}$ may be chosen so that $r = \tilde{r}$, and*

1. *either both loops are of type (C3) and $(\kappa, \lambda) \neq (\tilde{\kappa}, \tilde{\lambda})$; or*
2. *$\lambda = \tilde{\lambda}$, $\kappa \neq \tilde{\kappa}$, one of the loops is of type (A3), and the other of type (B3) (in such a case $r \not\equiv \pm 1 \bmod 2^{k-1}$ and $s \equiv 1 \bmod 2^{k-1}$).*

Proof: Let $Q = G \rtimes^3_f C$ be given in a canonical form. Our task is to investigate alternative expressions $Q = \tilde{G} \rtimes^3_{\tilde{f}} \tilde{C}$ such that $\tilde{G} \neq G$, and to determine those that do not yield a canonical form that is $G$-isomorphic to the original form given by $f$. Recall that $z$ is defined as $a^h$. Suppose first that $\langle \tilde{y} \rangle = \langle y \rangle$. Since $|G : \langle y \rangle| = 2$, we must have $\tilde{G} \leq \{u \in Q;\ u^2 \in \langle y \rangle\} \leq \langle x, y, z \rangle$. If $u \in Q \setminus \langle z, y \rangle$, then $u^h \in \langle z, y \rangle$ since $h$ is even. Thus $\tilde{G} \neq \langle z, y \rangle$. Therefore $\tilde{G} = \langle y, zx \rangle$, and $\langle a \rangle$ is a complement to $\bar{G}$. Hence we can assume that $\tilde{r} = r$, and this allows us to assume $k \geq 1$, by Theorem 5.1. There cannot be $t$ odd since in such a case $\bar{t}$ is odd as well, by Lemma 5.10, and so $(zx)^2 \notin \langle y^2 \rangle$. Assume that $t$ is even. If $t = 0$, then $(zx)^2 = x^2$, and so $\tilde{\lambda} = \lambda$ if $\kappa = \tilde{\kappa} = 1$. If $k \leq 1$, then the only available type is (A1), and Theorem 5.1 can be used again. Hence we can assume that $k \geq 2$ and that $t$ is even. We have $(zx)y(zx)^{-1} = y^{\bar{r}(-1+n/\kappa)}$ which means that $\bar{r} \in \{1, 1+n/2\}$ and that $\bar{r} = 1 + n/2$ if and only if $\tilde{\kappa} \neq \kappa$. By Lemma 6.1, $\bar{t} = n/2$ if and only if $Q$ is of type (C3). In all other cases $\bar{t} = 0$, by Lemma 5.10. Furthermore, by setting $\tilde{C} = \langle a \rangle$ we also obtain that $\tilde{t} = t$ since $a(zx)a^{-1} = zxy^t$.

Assume that $\bar{t} = n/2$. Then $\bar{r} = 1$, by point (ii) of Lemma 6.1. Now, $(zx)^2 = x^2 y^{n/2}$, and therefore $\tilde{\lambda} \neq \lambda$ if $\kappa = 1$. Of course, $\tilde{G}$ induces type (C3) as well.

Assume now that $\bar{t} = 0$. Then $(zx)^2 = x^2$. If $\bar{r} = 1$, then $(zxy)^2 = (xy)^2$. Hence only the case $\bar{r} = 1 + n/2$ needs to be considered. Therefore $2 \in \{\kappa, \tilde{\kappa}\}$, and we can assume that $\kappa = 2$ without loss of generality. The loop $G \rtimes^3_f C$ has to be of type (B3), by Lemma 6.1 and Theorem 5.2. Theorem 5.2 also implies that $\tilde{G}$ induces type (A3). From $(zx)^2 = x^2$ it follows that $\tilde{\lambda} = \lambda$.

By Proposition 2.8, $\langle y \rangle$ is invariant if $k = 0$ or if $t$ is odd. Hence we can assume that $k \geq 1$ and that $t$ is even. If $k = 1$, then $r$ determines the isomorphism type of $Q$ because of the decomposition $Q = Q_m \times \langle y^m \rangle$ (cf. Lemma 2.7). The same argument applies when $k = \kappa = 2 \leq v_2(t)$ and $r \equiv s \equiv 1 \bmod 4$. Hence we can assume that $k \geq 2$ and that $Q' = \langle y^2 \rangle$, by Proposition 2.8. Therefore $\tilde{G} \leq \langle x, y, z \rangle$. The case $y \in \tilde{G}$ has been already handled. Let us have $y \notin \tilde{G}$.

As argued in the first paragraph of the proof, $\tilde{G}$ cannot contain $z$ since $\langle \tilde{y}, z \rangle$ does not possess a complement. There are only two subgroups properly between $\langle y^2 \rangle$ and $\langle x, y, z \rangle$ that contain neither $y$ nor $z$, namely $\langle yz, xz, xy, y^2 \rangle$ and $\langle x, yz, y^2 \rangle$. The group $\tilde{G}$ has to be equal to one of them. In both cases $\langle a \rangle$ can serve as a complement.

Suppose that $\langle \tilde{y} \rangle = \langle yz, y^2 \rangle$. Then $[yz, y^2] = 1$, and so $\bar{r} \equiv 1 \bmod n/2$. Let us first consider the case $\bar{r} \equiv 1 + n/2 \bmod n$. Then $\bar{t} = 0$ and $k \geq 3$, by Lemma 6.1. Put $\tilde{y} = y^{1+n/4} z$. Then $\tilde{y}^2 = y^2$. From Lemma 6.1 and Theorem 5.2 it follows that $Q$ is of type (A3) or (B3). This means that $s \equiv 1 \bmod 2^{k-1}$, and we can thus assume that $r \equiv 1 \bmod 4$, by Lemma 5.8 (note that pairing does not change the type of $Q$, by Proposition 5.9 and Lemma 6.1). Furthermore, the type of $Q$ implies that $t = 0$, and so $[x, z] = 1$. Set $\tilde{x} = x$ if $\tilde{G} = \langle x, \tilde{y}\rangle$ and $\tilde{x} = xz$ if $\tilde{G} = \langle xz, \tilde{y}\rangle$. Then $\tilde{x}^2 = x^2$ and $[\tilde{x}, a] = 1$. Thus $\tilde{\lambda} = \lambda$ and $\tilde{t} = 0 = t$. Furthermore, if $i \equiv 1 \bmod 4$, then $\tilde{y}^i = y^{i-1}\tilde{y} = y^i y^{n/4} z = y^{i(1+n/4)}z$. Hence $\tilde{r} = r$. Now, $\tilde{y}^{-1} = y^{-1-n/4}zy^{n/2}$. Thus $x\tilde{y}x^{-1} = y^{-1-n/4+n/\kappa}z = \tilde{y}^{-1}y^{n/2+n/\kappa}$. The case $\tilde{G} = \langle \tilde{y}, x\rangle$ hence results in a change of $\kappa$ and fully corresponds to the switch between (B3) and (A3) as described in point (2) of Theorem 6.3. In the case $\tilde{G} = \langle \tilde{y}, xz\rangle$ there is $(xz)\tilde{y}(xz^{-1}) = (x\tilde{y}x^{-1})y^{n/2} = \tilde{y}^{-1}y^{n/\kappa}$, and thus $\tilde{G} \cong G$.

Let us now have $\bar{r} = 1$. Set $\tilde{y} = yz$ and let there be $\tilde{x} \in \{x, xz\}$, according to the choice of $\tilde{G}$. We have $\tilde{y}^{-1} = y^{-1}z$, $\tilde{y}^2 = y^2$, $\tilde{y}^r = y^r z = a\tilde{y}a^{-1}$, $[a, \tilde{x}] = [a, x]$ and $x\tilde{y}x^{-1} = (xz)\tilde{y}(xz)^{-1} = \tilde{y}^{-1+n/\kappa}$. Thus $\tilde{r} = r$, $\tilde{\kappa} = \kappa$ and $\tilde{t} = t$. The case $\tilde{x} = x$ yields $\tilde{\lambda} = \lambda$, and hence only the case $\tilde{x} = xz$ is worth consideration. If $\bar{t} = 0$, then $\tilde{x}^2 = x^2$. The change of $\lambda$ thus occurs if and only if $Q$ is of type (C3).

To finish the proof it remains to consider the case when $\tilde{y} \notin \langle yz, y^2\rangle$. Then $\tilde{y} \in \langle xyz, y^2\rangle$ or $\tilde{y} \in \langle xz, y^2\rangle$. Furthermore, $yz$ has to be of order dividing 4. From $(yz)^2 = y^{1+\bar{r}}$ and $\bar{r} \equiv 1 \bmod 4$ it follows that $k = 2$. From $(yz)^2 \in \{1, y^{n/2}\}$ it follows that $\bar{r} \equiv -1 \bmod n$ or that $\bar{r} \equiv -1 + 2m \bmod n$. The former possibility is excluded by $\bar{r} \equiv 1 \bmod 4$. The latter possibility is equivalent to $r^h \equiv -1 \bmod m$, by Lemma 6.1. Note that $[x, z] = 1$, that $s \equiv 1 \bmod 2m$ and that $-r + 2m$ can be used in place of $r$, all by Lemma 6.1. By Proposition 5.6 the loop $Q$ is paired. By Proposition 5.9 the pairing does not change the type. Put $\sigma = s + 1 + n/\kappa$. Then $\sigma \in \{2, 2m+2\}$, and for $r' \equiv -sr(1 + n/\kappa) \equiv r(1 - \sigma) \bmod n$ we obtain that $r' \in \{-r, -r + 2m\}$. Below we shall show that $\tilde{G}$ always is of the same type as $G$ and that $\tilde{\lambda} = \lambda$. The question is whether $\tilde{r}^i \in \{r, r'\}$ for some $i \in \mathbb{Z}$, $\gcd(i, 2h) = 1$. Suppose that $\tilde{r} = r + 2m$ (below we shall show that such a choice is always possible when the loops are not $G$-isomorphic). By Lemma 6.1 there exists $j \in \mathbb{Z}$, $\gcd(j, 2h) = 1$ such that $-r + 2m = r^j$. If $r' = -r$, then $\tilde{r} \equiv (r')^j \bmod n$, which means that the loops are $G$-isomorphic. If $r' = -r + 2m = r^j$, then there is $\tilde{r}^i \equiv r^j \equiv r' \bmod n$ for no integer $i$, since otherwise there would be $r^{i-1} \equiv -1 \bmod m$, and that is not possible by Lemma 6.1. Hence in the situation with $\tilde{r} = r + 2m$ and $r' = -r + 2m$ both loops are not $G$-isomorphic.

Assume first that $\tilde{G} = \langle x, xyz, y^2\rangle$. Then $(xyz)y^2(xyz)^{-1} = xy^{-2}x = y^2$. Therefore $\langle xyz, y^2\rangle$ is always a commutative group. It is cyclic if and only if the order of $xyz$ is divisible by 4. Now, $(xyz)^2 = xyx \cdot zyz = y^{-1+n/\kappa}y^{-1+n/2}x^2$ is equal to $y^{-2}x^2$ if $\kappa = 2$, and to $y^{-2+n/2}x^2$ if $\kappa = 1$. To get the divisibility we must have $x^2 = 1$ if $\kappa = 2$, and $x^2 = y^{n/2}$ if $\kappa = 1$. In other words, the group $\langle xyz, y^2\rangle$ is cyclic if and only if $\kappa \neq \lambda$. Let it be true and put $\tilde{y} = xy^{-1}z$. Then $\tilde{y}^2 = xy^{-1}xzy^{-1}z = y^{1+n/\kappa}x^2y^{1+n/2} = y^2$, and if $i$ is odd, then $\tilde{y}^i = y^{i-1}\cdot xy^{-1}z = xy^{1-i}y^{-1}z = xy^{-i}z$. Thus $x\tilde{y}x^{-1} = xy^{1+n/\kappa}z = \tilde{y}^{-1+n/\kappa}$ and $\tilde{G} \cong G$. Set $\tilde{x} = x$. This gives $\tilde{t} = t$. Furthermore, $a\tilde{y}a^{-1} = y^t xy^{-rs}z = \tilde{y}^{sr-t}$. From

$(s-1)(r+1) \equiv 0 \bmod n$ it follows that $\tilde{r} \equiv 1+(r-s)+t \bmod n$, i.e. $\tilde{r} \equiv r+t \bmod n$ if $s \equiv 1 \bmod n$, and $\tilde{r} \equiv r+t+n/2$ if $s \equiv 1+2m \bmod n$.

Suppose that $t = 0$ and $s = 1+2m$. Then $Q$ is of type (A2), by Theorem 5.2, and $\tilde{r} = r+2m$. If $\kappa = 2$, then $r' = -r$ which means that $\tilde{G}$ induces a $G$-isomorphic form. If $\kappa = 1$, then $r' = -r+2m$. This is case (2) of Theorem 6.2.

Suppose that $t = n/2$ and $s = 1$. Then $Q$ is of type (D2), $\kappa = 2$, $r \equiv 1 \bmod 4$, $\tilde{r} = r+2m$ and $r' = -r+2m$. Hence $\tilde{G}$ induces a form that is not $G$-isomorphic to the original form. However, the obtained form is not canonical (there is $\tilde{r}' \equiv 3 \bmod n$ and $\tilde{t} = n/2$). The corresponding canonical form is that of (B4) with $\lambda = 2$, i.e. case (1) of Theorem 6.2.

We can now turn to the case $\tilde{G} = \langle xz, xy, y^2 \rangle$. Then $(xz)y^2(xz)^{-1} = xy^{-2}x^{-1} = y^2$. The group $\langle xz, y^2 \rangle$ is cyclic. From $(xz)^2 = x^2$ it follows that it is cyclic if and only if $\lambda = 2$. Let this be true and set $\tilde{y} = xzy^{m+1}$ and $\tilde{x} = y^m z$. Then $\tilde{y}^2 = zxy^{m+1}xzy^{m+1} = zy^{-1-m}zy^{n/2}y^{1+m} = y^{n/2}(y^{m+1})^2 = y^2$. If $i$ is odd, then $\tilde{y}^i = xzy^{m+1}y^{i-1} = xzy^{m+i}$. Furthermore, $\tilde{x}^2 = y^m y^{m(-1+2m)} = y^{2m}$ and $\tilde{x}\tilde{y}\tilde{x}^{-1} = y^m(xzy^{-m-1})y^{-m} = xy^{-m}y^{n/\kappa}zy^{n/2}y^{-1} = xzy^m y^{-1}y^{n/\kappa} = \tilde{y}^{-1}y^{n/\kappa}$. Therefore $\tilde{G} \cong G$. Now, $a\tilde{x}a^{-1} = y^{rm}z$. Thus $\tilde{t} = n/2$ if $r \equiv 3 \bmod 4$, and $\tilde{t} = 0$ if $r \equiv 1 \bmod 4$. Furthermore, $a\tilde{y}a^{-1} = xzy^t y^{sr(m+1)} = \tilde{y}^{\tilde{r}}$, where $\tilde{r} \equiv sr(m+1) - m + t \bmod n$. Thus $\tilde{r} \equiv r+t \bmod n$ if $r \equiv 1 \bmod 4$, and $\tilde{r} \equiv r+t+n/2 \bmod n$ if $r \equiv 3 \bmod 4$.

If $t = n/2$ then $Q$ is of type (D2), $\kappa = 1$, $s = 1+2m$ and $r \equiv 3 \bmod n$, by Theorem 5.2 (recall that $\lambda = 2$). In this case $\tilde{t} = 2m = t$ and $\tilde{r} = r$, and no change occurs. We can thus assume that $t = 0$ and that $r \equiv 3 \bmod 4$. Then $\tilde{t} = n/2$ and $\tilde{r} = r+2m \equiv 1 \bmod 4$. Let there be $\kappa = 1$. The original form is (A2). The form induced by $\tilde{G}$ cannot be that of (D2) since $\tilde{r} \equiv 1 \bmod 4$. Hence it is (A) again. If $s = 1$, then $r' = -r$, and there exists a $G$-isomorphism, while for $s = 1+2m$ there is $r' = -r+2m$, and we get an instance of case (2) from Theorem 6.2.

Finally, assume that $\kappa = 2$. If $s = 1$, then the original form is (B4), and we get (D2). That corresponds to case (1) of Theorem 6.2. If $s = 1+n/2$, then $\tilde{G}$ induces a $G$-isomorphic form since $r' = -r$. □

Let $h$ be odd. As we shall observe, the solution of the isomorphism problem is easy if $k \leq 1$ or if $t$ is odd. Assume that $t$ is even and that $k \geq 2$. Then $|Q/\langle x, y, z \rangle| = h$ and $\langle x, y, z \rangle / Q'$ is of order 8 or 16 where the latter case takes place if and only if $Q' = \langle y^4 \rangle$, by Proposition 2.8. In that case, $y^2 Q'$ is the only nontrivial square of $\langle x, y, z \rangle / Q'$ (or, in fact, of $Q/Q'$). Hence $\langle y^2 \rangle$ is invariant in every situation. There is $\langle y^2 \rangle < \langle y \rangle < G < \langle x, y, z \rangle$, and therefore $\langle y^2 \rangle < \langle \tilde{y} \rangle < \tilde{G} < \langle x, y, z \rangle$, for every alternative expression $\tilde{G} \rtimes_{\tilde{f}}^{3} \tilde{C}$. It is relatively easy to see (cf. Lemma 6.18 for details) that $\langle \tilde{y} \rangle \neq \langle y \rangle$ may occur only when $s \equiv 1 \bmod n/2$. If $\langle \tilde{y} \rangle = \langle y \rangle$, then the situations to investigate are $\tilde{G} = \langle xz, y \rangle$ and $\tilde{G} = \langle y, z \rangle$ (cf. Lemmas 6.11 and 6.13). No other situation with $\tilde{G} \neq G$ and $\langle \tilde{y} \rangle = \langle y \rangle$ is possible since $\langle x, y, z \rangle / \langle y^2 \rangle$ is elementary abelian. If $s \equiv 1 \bmod n/2$ and $\langle \tilde{y} \rangle \neq \langle y \rangle$, then there cannot be $y \in \tilde{G}$ since $\langle y \rangle$ is the only cyclic subgroup of index two in $G$. Furthermore, it can be shown (Lemma 6.18) that either $\langle \tilde{y} \rangle = \langle xz, y^2 \rangle$ or $\langle \tilde{y} \rangle = \langle xy \cdot z, y^2 \rangle$ or $\langle \tilde{y} \rangle = \langle yz, y^2 \rangle$. Each of these three choices yields two different possibilities for the choice of $\tilde{G} \neq G$ since $\tilde{G} \neq G$ implies that $y \notin \tilde{G}$. A detailed investigation of conditions under which any of the possibilities described above really yields an alternative expression is a subject of the ensuing lemmas (up to Lemma 6.17).

The task is as follows. Take a $G$-type as specified by Tables 1 and 2, consider a subgroup $G_1$ of $\langle x, y, z \rangle$ that might serve as $\tilde{G}$ (it is thus of index two and contains $y^2$), and — when the corresponding necessary conditions are satisfied — specify the $G$-type and the value of $\tilde{r}$. There might be many values of $\tilde{r}$ to choose from, but relative go $G_1 = \tilde{G}$ it suffices to determine only one value since the question of multiple choices of $\tilde{C}$ and $\tilde{r} \in \tilde{C}$ has been fully solved in Sections 5 and 6.

Some $G$-types have two subtypes since they have two classes of complements to $G$. Only after choosing one of the subtypes we may fix not only $x$ and $y$ but also $z$. A choice of a $G$-subtype where there are two subtypes available will be done systematically: for $s \equiv 1 \bmod 2^{k-1}$, $k \geq 3$ (Table 2) always choose the case with $r \equiv 1 \bmod 2^{k-1}$. For $s \equiv -1 \bmod 2^{k-1}$, $k \geq 2$ (Table 1) choose the case with $v_2(r-s) \geq k$. By *strong $G$-type* we shall understand this narrowing of a $G$-type to the chosen $G$-subtype. If there is only one subtype, then the notions of $G$-type and strong $G$-type coincide. Each strong $G$-type determines the value $r \bmod 2^k$ uniquely.

As has been explained above, there are 8 alternatives for a choice of $\tilde{G}$ and $\langle \tilde{y}. \rangle$ such that $\tilde{G} \neq G$. They can be listed as $\langle xz, y \rangle$ and $\langle z, y \rangle$ with $\langle \tilde{y} \rangle = \langle y \rangle$; $\langle xz, xy, y^2 \rangle$ and $\langle xz, yz, y^2 \rangle$ with $\langle \tilde{y} \rangle = \langle xz, y^2 \rangle$; $\langle xz, yz, y^2 \rangle$ and $\langle x, yz, y^2 \rangle$ with $\langle \tilde{y} \rangle = \langle yz, y^2 \rangle$; $\langle x, yz, y^2 \rangle$ and $\langle xy, z, y^2 \rangle$ with $\langle \tilde{y} \rangle = \langle xy \cdot z, y^2 \rangle$.

This seems to give a formidable number of situations to consider since each of the 8 alternatives must be matched to each of the 36 $G$-types in Tables 1 and 2. However, as we shall see, a match exists in only some of the cases. Furthermore, some alternatives may be handled by a reduction to other cases by employing a composition of two constructions. Nevertheless, the number of computations to perform remains high. We shall proceed by considering, step by step, each of the 8 alternatives and match it, one at a time, to the four lists of (strong) $G$-types (Tables 1 and 2). For every such pair (i.e. an alternative and a list) there will be described a construction that yields an alternative expression in each of the eligible cases.

By a *$G$-shift* we shall understand a set of pairs (x, y) where x is a $G$-type considered in its strong canonical form (i.e. the form associated with the corresponding strong $G$-type) and y is the $G$-type that has been obtained by a construction mentioned in the preceding paragraph. We do not claim that the construction always yields the subtype that has been chosen in the definition of a strong $G$-type. If it yields the other (non-strong) subtype, we shall say that the $G$-shift *deviates* at x. If in the construction there is no deviation, we shall say that the $G$-shift is *undeviated.*

In a $G$-shift we do not list the situations in which the construction yields a $G$-isomorphic situation. Thus no $G$-shift contains a pair of a form $(\mathrm{x}, \mathrm{x})$. In fact, some constructions always yield $G$-isomorphic alternative expressions. In such a case the $G$-shift is empty.

Recall that the isomorphism type of an alternative expression is fully described by the $G$-type and by $\tilde{r} \bmod m$. Hence if a construction that is expressed by a $G$-shift is not used further on in a composition of constructions, then the information about deviation is not needed. However, if a composition is applied, the deviated $G$-types have to be transformed first to their strong form.

**Lemma 6.4.** *Let $h$ be odd and suppose that $\varepsilon \in \{-1, 1\}$ and $\eta \in \{0, 1\}$. Then $\bar{r} \equiv \varepsilon + \eta n/2 \bmod n$ if and only if $r \equiv \varepsilon + \eta 2^{k-1} \bmod 2^k$ and $r^h \equiv \varepsilon \bmod m$.*

Proof: By Lemma 5.10, $r \equiv \bar{r} \bmod 2^k$. The statement thus follows from the Chinese Remainder Theorem. □

**Lemma 6.5.** *Let $h$ be odd, $k \geq 2$, $t$ even and $s \equiv 1 \bmod n/2$. Each of the groups $\langle xz, y^2 \rangle$ and $\langle xy \cdot z, y^2 \rangle$ is abelian if and only if $\bar{r} \equiv -1 \bmod n/2$. The group $\langle yz, y^2 \rangle$ is abelian if and only if $\bar{r} \equiv 1 \bmod n/2$.*

Proof: By Proposition 2.2, $y^2 \in N$. Hence $[xz, y^2] = 1 \Leftrightarrow y^2 = x(zy^2z)x^{-1}$, i.e. $y^2 = y^{-2\bar{r}}$. Of course, $2 \equiv -2\bar{r} \bmod n$ is the same as $\bar{r} \equiv -1 \bmod n/2$. Similarly, $x(y(zy^2z)y^{-1})x^{-1} = y^{-2\bar{r}}$ and $y(zy^2z)y^{-1} = y^{2\bar{r}}$ are to be equal to $y^2$, respectively. □

**Lemma 6.6.** *Let $h$ be odd, $k = 2$, $t$ even and $s \equiv 1 \bmod 2m$. Suppose that $Q$ is in a canonical form.*

(i) *If $\bar{r} \equiv -1 \bmod 2m$, then $\langle xz, y^2 \rangle$ is cyclic if and only if $x^2y^t = y^{n/2}$.*
(ii) *If $\bar{r} \equiv -1 \bmod 2m$, then $\langle xy \cdot z, y^2 \rangle$ is cyclic if and only if $x^2y^ty^{n/\kappa} = y^{\bar{r}+s}$.*
(iii) *If $\bar{r} \equiv 1 \bmod 2m$, then $\langle yz, y^2 \rangle$ is cyclic if and only if $\bar{r} \equiv 1 \bmod 4m$.*

Proof: Elements (i) $(xz)^2 = x^2y^t$, (ii) $(xy^m \cdot z)^2 = xy^{sm}xy^ty^{\bar{r}m} = x^2y^{(\bar{r}-s)m}y^ty^{n/\kappa}$ and (iii) $(y^mz)^2 = y^{(\bar{r}+1)m}$ are always equal to 1 or $y^{n/2}$, respectively, with the latter value being attained if and only if the corresponding group is cyclic. Note that $(\bar{r} - s)m \equiv 2m + \bar{r} + s \bmod n$ if $\bar{r} \equiv -1 \bmod 2m$. □

From here on up to Lemma 6.17 we shall assume that $Q$ is given in a *strong canonical form*, i.e. that the canonical form is that of a strong $G$-type if $h$ is odd, $t$ even and $k \geq 2$. Note that the condition $\bar{r} \equiv -1 \bmod m$ is the same as the condition $\bar{r} \equiv -1 \bmod 2m$ since $\bar{r}$ is odd.

**Lemma 6.7.** *If $h$ is odd, $k = 2$, $t$ is even, $s \equiv 1 \bmod 2m$, $\bar{r} \equiv -1 \bmod 2m$ and $x^2y^t = y^{2m}$, then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle xz, xy, y^2 \rangle$, $\tilde{a} = a$ and $\tilde{y} \in \langle xz, y^2 \rangle$. The alternative expressions can be constructed in such a way that $\tilde{r} \equiv r \bmod m$ and that the $G$-shift is equal to $\{(\mathrm{h}, \mathrm{b}), (\mathrm{f}, \mathrm{g}), (\mathrm{g}, \mathrm{f})\}$ with deviation at* h *if $s = 1$, and to $\{(\mathrm{b}, \mathrm{f})\}$ if $s = 1 + 2m$, with no deviation.*

Proof: Put $\tilde{y} = xy^{m-1} \cdot z$. Then $\tilde{y}^2 = y^2$, $(\tilde{y})^i = xy^{m-i} \cdot z$ for every odd $i$, and $\bar{r}s \equiv \bar{r} - s + 1 \bmod n$, by Lemma 3.4. By a Moufang law, $(xy)(xy^{m-1} \cdot z)(xy) = (xy \cdot xy^{m-1})(xy^{\bar{r}s} \cdot z)y^t = f_s(xy \cdot xy^{m-1} \cdot xy^{-1})z \cdot y^{\bar{r}+1}y^t = (xy^{1-m} \cdot z)y^{\bar{r}+1}y^t x^2 = \tilde{y}^{-1}y^{\bar{r}+1}$. Hence $T_{xy}(\tilde{y}) = \tilde{y}^{-1} \cdot y^{\bar{r}+1}y^{n/\kappa}x^2$. This determines the value of $\tilde{\kappa}$. The values of $\tilde{\lambda}$ and $\tilde{t}$ depend upon the choice of $\tilde{x} \in \{xy^m, y^m z\}$. For $\tilde{x} = xy^m$ we get $\tilde{t} \equiv t + s + \bar{r} + 2m \bmod n$ since $a(xy^m)a^{-1} = xy^t y^{srm} = xy^{-m}y^{(\bar{r}+s)+t}$. If $\tilde{x} = y^m z$, then $\tilde{t} \equiv 2m + (\bar{r}+1) \bmod n$. Finally, $\tilde{r} \equiv r + t + (\bar{r}+1) + 2m \bmod n$ since $a\tilde{y}a^{-1} = xy^t y^{\bar{r}m-r} \cdot z = xy^{m-\tilde{r}} \cdot z = \tilde{y}^{\tilde{r}}$. This data directly determines the $G$-shift. The verification is straightforward. □

**Lemma 6.8.** *If $h$ is odd, $k = 2$, $t$ is even, $s \equiv 1 \bmod 2m$, $\bar{r} \equiv -1 \bmod 2m$ and $x^2y^ty^{n/\kappa} = y^{\bar{r}+s}$, then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle x, x \cdot yz, y^2 \rangle$, $\tilde{a} = a$ and $\tilde{y} \in \langle xy \cdot z, y^2 \rangle$. The alternative expressions can be chosen in such a way that $\tilde{r} \equiv r \bmod m$ and that the $G$-shift is equal to $\{(\mathrm{g}, \mathrm{f})\}$ if $s = 1$, and to $\{(\mathrm{b}, \mathrm{f}), (\mathrm{f}, \mathrm{b}), (\mathrm{c}, \mathrm{d}), (\mathrm{d}, \mathrm{c})\}$ if $s = 1 + 2m$. Both $G$-shifts are undeviated.*

Proof: Set $\tilde{y} = xy^{-1} \cdot z$. Then $\tilde{y}^2 = x^2y^{s-\bar{r}}y^ty^{n/\kappa} = y^2$, and $\tilde{y}^i = xy^{-i} \cdot z$ for every odd $i$. The value of $\tilde{\kappa}$ follows from $x\tilde{y}x^{-1} = (x \cdot xy^{-1}) \cdot xzy^tx^2 = \tilde{y}^{-1}x^2y^{\bar{r}+1}$. Furthermore, $\tilde{r} \equiv r + t + s - 1 \bmod n$ since $T_a(\tilde{y}) = xy^{t-rs} \cdot z$. If $\tilde{x} = x$, then $\tilde{t} = t$. If $\tilde{x} = y^m z$, then $\tilde{t} \equiv 2m + (\bar{r}+1) \bmod n$. The rest is a straightforward verification. □

**Lemma 6.9.** *If $h$ is odd, $k \geq 2$, $t$ even, $s \equiv 1 \bmod n/2$ and $\bar{r} \equiv 1 \bmod n$, then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle xz, yz, y^2 \rangle$, $\tilde{a} = a$ and $\tilde{y} \in \langle yz, y^2 \rangle$. The alternative expressions can be constructed in such a way that $\tilde{r} = r$ and that the $G$-shift is empty if $s \equiv 1 + n/2 \bmod n$, while for $s \equiv 1 \bmod n$ the $G$-shift is equal to $\{(\mathrm{b}, \mathrm{h}), (\mathrm{h}, \mathrm{b}), (\mathrm{g}, \mathrm{h})\}$ if $k = 2$, and to $\{(\mathrm{f}, \mathrm{i}), (\mathrm{i}, \mathrm{f}), (\mathrm{j}, \mathrm{i})\}$ if $k \geq 3$. Both $G$-shifts are undeviated.*

Proof: Set $\tilde{y} = yz$. Then $\tilde{y}^2 = y^2$, and $\tilde{y}^i = y^iz$ for every odd $i$. We have $(xz \cdot \tilde{y})(xz)^{-1} = xy^s \cdot x^{-1}zy^t = \tilde{y}^{-1}y^ty^{n/\kappa}$ and $a\tilde{y}a^{-1} = \tilde{y}^r$. If $\tilde{x} = xz$, then $\tilde{t} = t$. If $t = 0$, then $\tilde{\kappa} = \kappa$, $\tilde{\lambda} = \lambda$ and so the alternative expression induces an automorphism of $Q$ that sends $G$ upon $\tilde{G}$. Hence it can be assumed that $t = n/2$. Tables 1 and 2 carry no $G$-type with $r \equiv 1 \bmod 2^k$, $t = n/2$ and $s \equiv 1 + 2^{k-1} \bmod 2^k$. Hence $s \equiv 1 \bmod n$. Then $\tilde{t} = n/2$ also in the case when $\tilde{x} = xy^m$, and so we can assume that $\tilde{t} = n/2$. The $G$-shift expresses the change of $\kappa$ within those strong canonical forms that have $t = n/2$. □

**Lemma 6.10.** *If $h$ is odd, $k \geq 3$, $t$ is even, $s \equiv 1 \bmod n/2$ and $\bar{r} \equiv 1 + n/2 \bmod n$, then there exists an alternative expression of $Q$ with $\tilde{G} = \langle xz, yz, y^2 \rangle$, $\tilde{a} = a$ and $\tilde{y} \in \langle yz, y^2 \rangle$. The alternative expressions can be chosen in such a way that $\tilde{r} = r$, and that the $G$-shift is empty if $s \equiv 1 \bmod n$, while for $s \equiv 1 + n/2 \bmod n$ the $G$-shift is equal to $\{(\mathrm{g}, \mathrm{i}), (\mathrm{i}, \mathrm{g}), (\mathrm{j}, \mathrm{i})\}$ and is undeviated.*

Proof: Set $\tilde{y} = y^{1+n/4}z$. Then $\tilde{y}^2 = y^2$ and $\tilde{y}^i = y^{i+n/4}z$ for every odd $i$. Hence $(xz \cdot \tilde{y})(xz)^{-1} = xy^{s(1-n/4)} \cdot x^{-1}zy^t = \tilde{y}^{-1}y^{t+n/\kappa}$, $a\tilde{y}a^{-1} = \tilde{y}^r$ and if $\tilde{x} = xz$, then $\tilde{t} = t$. For $t = 0$ we thus get an isomorphic situation, and hence there can be assumed that $t = n/2$. This yields $s \equiv 1 + n/2 \bmod n$ since for $s \equiv 1 \bmod n$ there exists no $G$-type with $r \equiv 1 + 2^{k-1} \bmod 2^k$ and $t = n/2$. If $\tilde{x} = xy^m$, then $\tilde{t} = n/2$ as well. Hence the $G$-shift expresses the change of $\kappa$ within the $G$-types with $t = n/2$. □

**Lemma 6.11.** *Let $h$ be odd. If $t$ is odd, then there exists no alternative expression of $Q$ with $\tilde{G} = \langle xz, y\rangle$. If $k \le 1$ and such an expression exists, then there also exists $\Psi \in \mathrm{Aut}(Q)$ such that $\Psi(G) = \tilde{G}$. If $k \ge 2$ and $t$ is even, then an alternative expression with $\tilde{G} = \langle xz, y\rangle$ exists if and only if $s \equiv \bar{r} \bmod n/2$ (which implies that $r \equiv s \bmod 2^{k-1}$). If this is true, then the alternative expressions can be constructed in such a way that $\tilde{r} = r$, $\tilde{a} = a$, and the G-shift is equal to*

(i) $\{(\mathrm{b},\mathrm{g}),(\mathrm{e},\mathrm{a}),(\mathrm{f},\mathrm{b}),(\mathrm{g},\mathrm{b})\}$ *if $s \equiv -1 + 2^{k-1} \bmod 2^k$, with deviation at* e *and* f*;*

(ii) $\{(\mathrm{d},\mathrm{c}),(\mathrm{e},\mathrm{f}),(\mathrm{f},\mathrm{e}),(\mathrm{g},\mathrm{h}),(\mathrm{h},\mathrm{g})\}$ *if $s \equiv -1 \bmod 2^k$, with deviation at* d*;*

(iii) $\{(\mathrm{d},\mathrm{g}),(\mathrm{e},\mathrm{h}),(\mathrm{f},\mathrm{j}),(\mathrm{g},\mathrm{d}),(\mathrm{h},\mathrm{e}),(\mathrm{j},\mathrm{f})\}$ *if $s \equiv 1 \bmod 2^k$ and $k \ge 3$; and*

(iv) $\{(\mathrm{a},\mathrm{f}),(\mathrm{b},\mathrm{h}),(\mathrm{f},\mathrm{a}),(\mathrm{g},\mathrm{j}),(\mathrm{h},\mathrm{b}),(\mathrm{j},\mathrm{g})\}$ *if $s \equiv 1 + 2^{k-1} \bmod 2^k$ and $k \ge 3$.*

*The G-shifts of (iii) and (iv) are undeviated.*

Proof: By direct computation, $(xy^m \cdot z)^2 = x^2 y^{(-s+\bar{r})m} y^{t+n/\kappa}$, $(xz)^2 = x^2 y^t$ and $xz \cdot y \cdot (xz)^{-1} = y^{-\bar{r}s} y^{n/\kappa} = y^{-1} y^{s-\bar{r}+n/\kappa}$. Hence an alternative expression with $\tilde{G} = \langle xz, y\rangle$ never exists if $t$ is odd, while for $t \in \{0, n/2\}$ it exists if and only if $\bar{r} \equiv s \bmod n$ when $k \le 1$, and $\bar{r} \equiv s \bmod n/2$ when $k \ge 2$. We can assume that $\tilde{a} = a$, and thus $\tilde{r} = r$. If $\tilde{x} = xz$, then $\tilde{t} = t$. If $\tilde{x} = xy^m \cdot z$, then $\tilde{t} \equiv s - \bar{r} + t \bmod n$. If $k \le 1$, then the existence of $\Psi \in \mathrm{Aut}(Q)$ follows from Theorem 5.1. Assume that $k \ge 2$. If $\tilde{r} - s \equiv 0 \bmod n$ and $t = 0$, then we get an isomorphic expression of $Q$. This reduces the number of situations to be considered. The rest is straightforward. □

**Lemma 6.12.** *Let $h$ be odd. If $k \ge 1$ and $t$ is odd, then there exists no alternative expression of $Q$ such that $\tilde{G} = \langle y, z\rangle$. If $k \le 1$ and $t = 0$, then such an expression exists if and only if $\bar{r} \equiv -1 \bmod n$. In such a case $\tilde{G} = \Psi(G)$ for some $\Psi \in \mathrm{Aut}(Q)$.*

Proof: There must be $zyz = y^{-1}$ since $\kappa = \tilde{\kappa} = 1$ (by the assumptions of the lemma). Hence $\bar{r} \equiv -1 \bmod n$. If $k \le 1$ and $t = 0$, put $\tilde{a} = xa^{h+1}$. Then $\tilde{a}^2 = a^2$, and so $\langle \tilde{a}\rangle$ is a complement to $\tilde{G}$. We have $\tilde{r} = r$ as $\tilde{a}y\tilde{a}^{-1} = a^{h+1}y^{-1}a^{-h-1} = (y^{-r^h})^r = y^r$. The existence of $\Psi$ follows from Theorem 5.1.

Assume now that $k \ge 1$ and that $t$ is odd. The goal is to prove that $\tilde{G} = \langle y, z\rangle$ has no cyclic complement in $Q$. If such complement had existed, it would be generated by $\tilde{a} \in \langle y\rangle a$ or $\tilde{a} \in x\langle y\rangle \cdot a$. Since $(y^i a)^h \in \langle y\rangle z \subseteq \tilde{G}$, for every $i \in \mathbb{Z}$, we must have $\tilde{a} \in x\langle y\rangle \cdot a$. For a while put $\bar{Q} = Q/\langle y^2\rangle$. Then $\bar{Q}$ is a group with $\bar{y} \in Z(\bar{Q})$ and $[\bar{a}, \bar{x}] = \bar{y}$. Therefore $(\bar{x}\bar{a})^2 = (\bar{x}\bar{y}\bar{a})^2 = \bar{y}\bar{a}^2$, and so $(\bar{x}\bar{a})^{2h} = (\bar{x}\bar{y}\bar{a})^{2h} = \bar{y}$. That contradicts the existence of a complement. □

**Lemma 6.13.** *Let $h$ be odd, $k \ge 2$ and $t$ even. Then an alternative expression of $Q$ such that $\tilde{G} = \langle y, z\rangle$ exists if and only if $\bar{r} \equiv -1 \bmod n/2$, with an exception* *of the case $\lambda = 2$, $\kappa = 1$, $t = 0$ and $v_2(r-s) \geq k$ (in which case no alternative expression exists). The alternative expressions can be constructed in such a way that $\tilde{r} \equiv -rs \bmod m$ if $\lambda = 2$, $\kappa = 1$ and $v_2(r-s) = k-1$ (this corresponds to $G$-type* b *if $s \equiv -1 + 2^{k-1} \bmod 2^k$ and to $G$-types* e *and* h *if $s \equiv -1 \bmod 2^k$), and $\tilde{r} \equiv r \bmod m$ in the other cases, with the $G$-shift being equal to*

(i) $\{(\mathrm{b},\mathrm{f}), (\mathrm{f},\mathrm{g}), (\mathrm{a},\mathrm{e}), (\mathrm{e},\mathrm{a}), (\mathrm{g},\mathrm{f})\}$ *if $s \equiv -1 + 2^{k-1} \bmod 2^k$; and*

(ii) $\{(\mathrm{c},\mathrm{d}), (\mathrm{d},\mathrm{c}), (\mathrm{e},\mathrm{f}), (\mathrm{h},\mathrm{g})\}$ *if $s \equiv -1 \bmod 2^k$.*

*Both $G$-shifts are undeviated. There are no strong canonical forms with $r \equiv -1 \bmod 2^{k-1}$ if $k \geq 3$ and $s \equiv 1 \bmod 2^{k-1}$.*

PROOF: Suppose that $\tilde{G} = \langle y, z \rangle$. Then $zyz^{-1} = y^{-1+n/\tilde{\kappa}}$. Hence $\bar{r} \equiv -1 \bmod n/2$. Let this be true. The first step is to prove the nonexistence of a cyclic complement to $\langle y, z \rangle$ if $\lambda = 2$, $\kappa = 1$, $t = 0$ and $r - s \equiv 0 \bmod 2^k$. Start from the contrary and assume that $\tilde{C} = \langle \tilde{a} \rangle$. Put $\tilde{z} = \tilde{a}^h$. Since $\tilde{z} \in \langle x, y, z \rangle$ and $\tilde{z} \notin \tilde{G} \cup G$, there must exist an integer $i$ such that $\tilde{z} = xy^i \cdot z$. This is a contradiction since $\tilde{z}^2 = y^{n/2} y^{i(\bar{r}-s)} \neq 1$ as $v_2(\bar{r} - s) \geq k$.

Hence if $\lambda = 2$, then the $G$-types to be investigated are b and f if $s \equiv -1 + 2^{k-1} \bmod 2^k$, and e, f and h if $s \equiv -1 \bmod 2^k$. Suppose first that $\lambda = \kappa = 2$. Then the $G$-type is equal to f, for both values of $s$. Therefore $t = 0$ and $r - s \equiv 2^{k-1} \bmod 2^k$. Put $\tilde{a} = xy^m a^{h+1}$ and $\tilde{z} = \tilde{a}^h$. We have $[a^{h+1}, y^m] = 1$, $\tilde{a}^2 = (xy^m)^2 a^{2h+2} = a^2$, $\tilde{z} = xy^m a^{h+1} a^{h-1} = xy^m$, $\tilde{a} y \tilde{a}^{-1} = xy^m \cdot y^{\bar{r}r} \cdot y^{-m} x^{-1} = xy^{(\bar{r}+1-1)r} x^{-1} = y^r y^{\bar{r}+1+n/2}$, and $[\tilde{a}, z] = [xy^m, z] = y^{m(r-s)} = y^{n/2}$. If $s \equiv -1 + 2^{k-1} \bmod 2^k$, set $\tilde{x} = z$. This gives $G$-type g since $\tilde{t} = n/2$, $\tilde{\kappa} = 1$ and $\tilde{\lambda} = 1$. If $s \equiv -1 \bmod 2^k$, set $\tilde{x} = y^m z$. This yields no change of $G$-type since $\tilde{r} = r$, $\tilde{\kappa} = 2$, $(y^m z)^2 = y^{m(1+\bar{r})} = y^{n/2}$ and $[\tilde{a}, y^m z] = [xy^m, y^m z] = 1$.

Let us have $\lambda = 2$ and $\kappa = 1$. Set $\tilde{a} = xy^m \cdot a$. Then $\tilde{a}^2 = x^2 y^t y^{(r-s)m} \cdot a^2 = a^2$ in all three cases. There is $(xy^m \cdot a) \cdot y (xy^m \cdot a)^{-1} = (xy^{m+r} \cdot a)(x^{-1} y^{mrs} y^t \cdot a^{-1}) = y^{-rs}$. Thus $\tilde{r} = -rs$. There is $\tilde{\kappa} = 2$ for $G$-types b and e, and $\tilde{\kappa} = 1$ for $G$-type h as $zyz^{-1} = y^{\bar{r}}$. Set $\tilde{x} = y^m z$. There is $\tilde{x}^2 = y^{m(1+\bar{r})}$, and so $\tilde{\lambda} = 1$ for $G$-type h, and $\tilde{\lambda} = 2$ for $G$-types b and e. Furthermore, $\tilde{a} \cdot \tilde{x} \cdot \tilde{a}^{-1} = xy^{m(1+rs)} a^{h+1} \cdot x^{-1} y^{mrs} y^t a^{-1} = y^{-m(s+1)} y^t \cdot y^m z$. Hence $\tilde{t} = 0$ for $G$-types b and e, and $t = n/2$ if the $G$-type is equal to h. The contribution to the $G$-shift is hence equal to $\{(\mathrm{b},\mathrm{f}), (\mathrm{e},\mathrm{f}), (\mathrm{h},\mathrm{g})\}$.

It remains to treat the cases with $\lambda = 1$. Put $\tilde{a} = xa^{h+1}$. Then $\tilde{a}^2 = a^2$, $\tilde{z} = \tilde{a}^h = x$ and $\tilde{a} y \tilde{a}^{-1} = xy^{(\bar{r}+1-1)r} x^{-1} = xy^{-r} x^{-1} y^{\bar{r}+1} = y^r y^{\bar{r}+1+n/\kappa}$. Clearly, $y^{n/\tilde{\kappa}} = y^{\bar{r}+1}$.

If $\tilde{x}$ is chosen as $z$, then $\tilde{t} = t$ and $\tilde{\lambda} = 1 = \lambda$. If $\tilde{r} + 1 + n/\kappa \equiv 0 \bmod n$, then $\tilde{r} \equiv r \bmod n$ and also, by inspection of Table 1, $\kappa = \tilde{\kappa}$. Therefore in these cases there exists $\Psi \in \mathrm{Aut}(Q)$ such that $\Psi(G) = \tilde{G}$. Let us have $\tilde{r} + 1 + n/\kappa \equiv n/2 \bmod n$. Then $\tilde{r} \equiv r + n/2 \bmod n$. The $G$-types to consider are a, e and g if $s \equiv -1 + 2^{k-1} \bmod 2^k$, and c and d if $s \equiv -1 \bmod 2^k$. If $t = 0$, then the choice of $\tilde{x} = z$ switches a with e, and c with d. If $t = n/2$, then the $G$-type is equal to g and $s \equiv -1 \bmod 2^k$. Set $\tilde{x} = y^m z$. Then $\tilde{\lambda} = 2$, $\tilde{t} = 0$, and the resulting $G$-type is f. □

**Lemma 6.14.** *Suppose that $h$ is odd, $k \geq 2$, $t$ is even, $s \equiv -1 + 2^{k-1} \bmod 2^k$, $\bar{r} \equiv -1 \bmod n$, $t = 0$, $\kappa = 1$, $\lambda = 2$ (i.e. the $G$-subtype* b1). *Then there exists an alternative expression with $\tilde{G} = \langle y, z\rangle$, $\tilde{r} \equiv -rs \bmod n$, $\tilde{t} = n/2$, $\tilde{\kappa} = 1$, $\tilde{\lambda} = 1$ (i.e. the $G$-type* g).

Proof: We are in a similar situation as in the part of proof of Lemma 6.13 that discusses the case $\lambda = 2$ and $\kappa = 1$. Like in that proof set $\tilde{a} = xy^m \cdot a$ and observe that $\tilde{a} = a^2$. Thus $\langle \tilde{a}\rangle$ is a complement to $\tilde{G} = \langle y, z\rangle$. Furthermore, $(xy^m \cdot a)y(xy^m \cdot a)^{-1} = y^{-rs}$ gives $\tilde{r} = -rs$, and $zyz^{-1} = y^{\bar{r}} = y^{-1}$ yields $\tilde{\kappa} = 1$. Set $\tilde{x} = xy^m$. Then $\tilde{x}^2 = y^{m(1+\bar{r})} = 1$, and thus $\lambda = 1$. Finally, $\tilde{a}\tilde{x}\tilde{a}^{-1} = y^{-m(s+1)}y^t \cdot \tilde{x} = y^{n/2}\tilde{x}$. Therefore $\tilde{t} = n/2$. □

**Lemma 6.15.** *If $h$ is odd, $k = 2$, $t$ is even, $s \equiv 1 \bmod 2m$, $\bar{r} \equiv -1 \bmod 2m$ and $x^2y^t = y^{2m}$, then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle x, z, y^2\rangle$ and $\tilde{y} \in \langle xz, y^2\rangle$. There is $\tilde{r} \equiv r \bmod m$ with the exceptions of* (a) *$G$-type* h, *$s = 1$, and* (b) *$G$-type* e, *$s = 1 + n/2$, for which $\tilde{r} \equiv -rs \bmod m$. If $s = 1$, then the $G$-shift is equal to* $\{(\mathrm{h}, \mathrm{g})\}$, *while for $s = 1 + n/2$ it is equal to* $\{(\mathrm{b}, \mathrm{f}), (\mathrm{e}, \mathrm{f})\}$.

Proof: By Lemma 6.7 for every $Q$ that satisfies conditions of this statement it is possible to find an alternative expression $G_1 \rtimes^3_{f_1} \langle a\rangle$ such that $G_1 = \langle xz, xy, y^2\rangle$, $\langle y_1\rangle = \langle xz, y^2\rangle$ and $r_1 \equiv r \bmod m$. Strong $G$-types that fulfil the conditions are c, f, g and h if $s \equiv 1 \bmod n$, and b, e, f and g if $s \equiv 1 + n/2 \bmod n$. By Lemma 6.7, $G_1$ is of $G$-type c, g, f, b if $s = 1$, and of $G$-type f, e, f and g if $s = 1 + n/2$, respectively. The presentation of $G_1$ expresses a strong $G$-type, with the exception of $G$-type b, where the subtype b1 is obtained. By applying the constructions of Lemmas 6.13 and 6.14 to $G_1$ we get the $G$-shifts $\{(\mathrm{h}, \mathrm{g})\}$ and $\{(\mathrm{b}, \mathrm{f}), (\mathrm{e}, \mathrm{f})\}$. □

**Lemma 6.16.** *If $h$ is odd, $\kappa = 2$, $t$ is even, $s \equiv 1 \bmod 2m$, $\bar{r} \equiv -1 \bmod 2m$ and $x^2y^ty^{n/\kappa} = y^{\bar{r}+s}$, then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle xy, z, y^2\rangle$, $\tilde{y} \in \langle xz, y^2\rangle$ and $\tilde{r} \equiv r \bmod m$. The $G$-shift is equal to* $\{(\mathrm{f}, \mathrm{g})\}$ *if $s = 1$, and to* $\{(\mathrm{b}, \mathrm{f}), (\mathrm{f}, \mathrm{b})\}$ *if $s = 1 + n/2$.*

Proof: Proceed like in the proof of Lemma 6.15, composing the construction of Lemma 6.8 (the first step) with the construction of Lemma 6.13 (the second step). For $Q$ that satisfies conditions of this statement there exists an alternative expression $G_1 \rtimes^3_{f_1} \langle a\rangle$ such that $G_1 = \langle x, x \cdot yz, y^2\rangle$, $\langle y_1\rangle = \langle xy \cdot z, y^2\rangle$, $\tilde{a} = a$ and $r_1 = r$. If $s = 1$, then the eligible strong $G$-types c, d, f, g are transformed first to c, d, f, f, and then to c, d, g, g, yielding the $G$-shift $\{(\mathrm{f}, \mathrm{g})\}$. If $s = 1 + n/2$, then the eligible strong $G$-types b, c, f, g are transformed first to f, d, b, g, and then to f, c, b, g, yielding the $G$-shift $\{(\mathrm{b}, \mathrm{f}), (\mathrm{f}, \mathrm{b})\}$. □

The last alternative to consider is the case of $\tilde{G} = \langle x, yz, y^2\rangle$, $\langle \tilde{y}\rangle = \langle yz, y^2\rangle$. Then $\bar{r} \equiv 1 \bmod n/2$ by Lemma 6.5, and $\bar{r} \equiv 1 \bmod n$ if $\kappa = 2$, by Lemma 6.6. As we shall see in Lemma 6.18, there is $s \equiv 1 \bmod n/2$, and thus $\bar{r} \equiv s \bmod n/2$. Since $s \equiv 1 \bmod n/2$, only the $G$-types of Table 2 are relevant if $k \geq 3$, while for $k = 2$ there applies Table 1. Therefore $G_1 = \langle xz, yz, y^2\rangle$ with $a_1 = a$ and $r_1 = r$

may be constructed, by means of Lemmas 6.9 and 6.10 in every case when there might exist an alternative expression with $\tilde{G} = \langle x, yz, y^2\rangle$ and $\langle \tilde{y}^2\rangle = \langle yz, y^2\rangle$. Such an alternative expression can be, in every case again, obtained from $G_1$ by the construction of Lemma 6.11.

**Lemma 6.17.** *Let $h$ be odd, $k \geq 2$, $t$ even, $s \equiv 1 \bmod n/2$, $\bar{r} \equiv 1 \bmod n/2$, and let there be $\bar{r} \equiv 1 \bmod n$ if $k = 2$. Then there exists an alternative expression of $Q$ such that $\tilde{G} = \langle x, yz, y^2\rangle$, $\tilde{y} \in \langle yz, y^2\rangle$, $\tilde{r} = r$ and $\tilde{a} = a$. The $G$-shift is equal to*

(i) $\{(\mathrm{b},\mathrm{h}),(\mathrm{g},\mathrm{h}),(\mathrm{h},\mathrm{g})\}$ *if $s \equiv 1 \bmod n$ and $k = 2$;*
(ii) $\{(\mathrm{d},\mathrm{c}),(\mathrm{e},\mathrm{f}),(\mathrm{f},\mathrm{c})\}$ *if $s \equiv 1 + n/2 \bmod n$ and $k = 2$;*
(iii) $\{(\mathrm{d},\mathrm{g}),(\mathrm{e},\mathrm{h}),(\mathrm{f},\mathrm{i}),(\mathrm{g},\mathrm{d}),(\mathrm{h},\mathrm{e}),(\mathrm{i},\mathrm{j}),(\mathrm{j},\mathrm{i})\}$ *if $s \equiv 1 \bmod n$ and $k \geq 3$; and*
(iv) $\{(\mathrm{a},\mathrm{f}),(\mathrm{b},\mathrm{h}),(\mathrm{f},\mathrm{a}),(\mathrm{g},\mathrm{i}),(\mathrm{h},\mathrm{b}),(\mathrm{i},\mathrm{j}),(\mathrm{j},\mathrm{i})\}$ *if $s \equiv 1+n/2 \bmod n$ and $k \geq 3$.*

Proof: In case (i) the eligible $G$-types are a, b, c, d, g, h and the construction of Lemma 6.9 turns them into a, h, c, d, h, b, respectively. In case (ii) there are eligible $G$-types d, e and f, and Lemma 6.9 turns them into d, e and f. In cases (iii) and (iv) all $G$-types are eligible, and the constructions of Lemmas 6.9 and 6.10 yield a $G$-shift $\{(\mathrm{f},\mathrm{i}),(\mathrm{i},\mathrm{f}),(\mathrm{j},\mathrm{i})\}$ in case (iii), and a $G$-shift $\{(\mathrm{g},\mathrm{i}),(\mathrm{i},\mathrm{g}),(\mathrm{j},\mathrm{i})\}$ in case (iv). The rest follows from Lemma 6.11. □

**Lemma 6.18.** *Suppose that $h$ is odd and that $Q = G \rtimes_f^3 C$ is given in a strong canonical form. Let there exist an alternative expression $Q = \tilde{G} \rtimes_{\tilde{f}}^3 \tilde{C}$ such that $\tilde{G} \neq \Psi(G)$ for every $\Psi \in \mathrm{Aut}(Q)$. Then $k \geq 2$ and $t$ is even. If $y \in \tilde{G}$, then $\tilde{G} = \langle xz, y\rangle$ or $\tilde{G} = \langle y, z\rangle$.*

*Assume that $y \notin \tilde{G}$. Then $s \equiv 1 \bmod n/2$ and either $\langle \tilde{y}\rangle = \langle yz, y^2\rangle$, or $\langle \tilde{y}\rangle = \langle xz, y^2\rangle$, or $\langle \tilde{y}\rangle = \langle xy \cdot z, y^2\rangle$. If $\langle \tilde{y}\rangle = \langle yz, y^2\rangle$, then $\bar{r} \equiv 1 \bmod n/2$, and $\bar{r} \equiv 1 \bmod n$ if $k = 2$.*

*If $\langle \tilde{y}\rangle = \langle xz, y^2\rangle$, then $k = 2$, $\bar{r} \equiv -1 \bmod n/2$ and $x^2y^t = y^{n/2}$. If $\langle \tilde{y}\rangle = \langle xy \cdot z, y^2\rangle$, then $k = 2$, $\tilde{r} \equiv -1 \bmod n/2$ and $xy^ty^{n/\kappa} = y^{\tilde{r}+s}$.*

Proof: Recall that $\tilde{G} \leq \langle x, y, z\rangle$ since $u^2 \in \langle y^2\rangle$ for every $u \in G$. By Proposition 2.8, $\langle y\rangle = Q' = \langle \tilde{y}\rangle$ if $n$ is odd or if $t$ is odd. Since $\langle x, y, z\rangle/\langle y\rangle$ is a Klein group, there is $\tilde{G} = \langle y, z\rangle$ or $\tilde{G} = \langle y, xz\rangle$ if $\langle y\rangle = \langle \tilde{y}\rangle$. By Lemmas 6.11 and 6.12 in these cases $k \geq 2$.

Assume that $y \notin \tilde{G}$. Then $t$ is even and $k \geq 1$. Now, $C = \langle b\rangle$ and $b^2$ is of an odd order. The group $Q/\langle y^2\rangle$ is abelian, and hence $\langle x, y, z\rangle \cap \langle y, b^2\rangle = \langle y\rangle$. If $s \not\equiv 1 \bmod n/2$, then $\langle y, b^2\rangle = \langle \tilde{y}, \tilde{b}^2\rangle = C_Q(A)$, by Lemma 2.12, and thus $\langle y\rangle = \langle \tilde{y}\rangle$.

Suppose that $s \equiv 1 \bmod n/2$ and that $y \notin \tilde{G}$. Our next step will be to refute the case $k = 1$. If $k = 1$ and $s \equiv 1 + n/2 \bmod n$, then $\langle y\rangle = \langle \tilde{y}\rangle$ since $y^m$ is the only central involution in $\langle x, y, z\rangle$ as $z \notin N$, by Proposition 2.2. Let there be $s = 1 = \kappa$. It may be assumed that $t = 0$, by Theorem 5.1. It can be verified easily that $y^m$ is the only central involution of $Q$ unless $\bar{r} \equiv \pm 1 \bmod n$. Let this be true and denote by $Z$ the group generated by central involutions of $Q$. Then

$Z = \langle y^m, z\rangle$ if $\bar{r} \equiv 1 \bmod n$, and $Z = \langle y^m, xz\rangle$ if $\bar{r} \equiv -1 \bmod n$. In both cases $Q = \langle x, y^2, b^2\rangle \times Z$. Since $y = y^{m+1}y^m$, we see that $\tilde{y}$ is a product of a power of $y^2$ with a central involution. Hence there exists $\Psi \in \operatorname{Aut}(Q)$ such that $\Psi(\langle y\rangle) = \langle \tilde{y}\rangle$; in fact $\Psi(y) = \tilde{y}$ for some $\Psi \in \operatorname{Aut}(Q)$.

Hence we can assume that $k \geq 2$. If $\tilde{y} \in \langle yz, y^2\rangle$, then the conditions on $\bar{r}$ follow from Lemmas 6.5 and 6.6. Now, $\langle y\rangle$ is the only cyclic subgroup of $G$ with $|G : \langle y\rangle| = 2$. Hence $\langle \tilde{y}\rangle \neq \langle x, y^2\rangle$ and $\langle \tilde{y}\rangle \neq \langle xy, y^2\rangle$. The group $\langle x, y, z\rangle/\langle y^2\rangle$ contains 7 nontrivial elements. Each of them might determine $\langle \tilde{y}\rangle$. As we have seen there can be $\tilde{y} \in \langle xz, y^2\rangle$, $\tilde{y} \in \langle yz, y^2\rangle$ and $\tilde{y} \in \langle x \cdot yz, y^2\rangle$. The case $\langle y\rangle = \langle z, y^2\rangle$ cannot occur since $\langle xz, y^2\rangle$ contains two different involutions, say $z$ and $y^{n/2}$.

Recall that the given canonical form corresponds to a strong $G$-type, and let there be $\tilde{y} \in \langle xz, y^2\rangle$ or $\tilde{y} \in \langle xy \cdot z, y^2\rangle$. Then $\bar{r} \equiv -1 \bmod n/2$ by Lemma 6.5. However, for $k \geq 3$ this never occurs since then $\bar{r} \equiv 1 \bmod 2^{k-1}$ for every strong $G$-type. The rest follows from Lemma 6.6. □

By a *complete invariant* we understand any invariant that determines fully an isomorphism class (assuming that $n$, $h$ and $s$ are known). Recall that the parity of $t$ is an invariant if $n$ is even, by Proposition 2.8.

**Theorem 6.19.** *Let $h$ be odd. Put $R_0 = \{r^j \in \mathbb{Z}_n;\ \gcd(j, 2h) = 1\}$ and $\{R_1 = \{-sr^j \in \mathbb{Z}_n;\ \gcd(j, 2h) = 1\}$.*

(i) *If $k = 0$, then $R_0 \cup R_1$ is a complete invariant.*

(ii) *If $k = 1$ and $t$ is even, then $R_0 \cup R_1$ together with the value of $\lambda \in \{1, 2\}$ form a complete invariant.*

(iii) *If $k \geq 1$ and $t$ is odd, then $R_0$ and $\lambda \in \{1, 2\}$ form a complete invariant.*

Proof: Use Theorem 5.1, Proposition 5.5 and Lemma 6.18. □

Let $h$ be odd, $t$ even and $k \geq 2$. Let $Q$ be expressed in a form that corresponds to a strong $G$-type x. By definition, a strong $G$-type is represented by a subtype, say x$i$, $i \in \{0, 1, 2, 3\}$. Put $R = \{r^j \in \mathbb{Z}_m^*;\ \gcd(j, 2h) = 1\}$. Note that $R$ is intentionally defined relative to $m$ since $r \bmod 2^k$ is determined by x$i$. By results of Section 5 the class of all loops that are $G$-isomorphic to $Q$ is fully determined by x$i$ and $R$ if $i \in \{0, 1, 2\}$, while for $i = 3$ the set $R$ has to be replaced by $R \cup -sR$ (where $-sR$ is also considered modulo $m$). For $i = 3$ it may happen that the conditions on $s$ are such that $-sR = R$, and that explains why in the discussion of simple blocks below the set $-sR$ is not mentioned.

For given $s$, $m$, $h$ and $R$ the solution of isomorphism problem might seem to require just an equivalence upon the corresponding set of $G$-types. However, that does not cover all cases since a change from a strong $G$-type to another strong $G$-type might induce a switch from $R$ to $-sR$. To describe succinctly both situations (i.e. without a switch and with a switch) we define the notion of an *iso-equivalence* that will be regarded as a union of *simple* and *split* blocks, where a simple block is a list of strong $G$-types, say $B = \{\mathrm{x}_1, \dots, \mathrm{x}_p\}$, while a split block is a pair $[B_0, B_1]$ such that $B_0 = \{\mathrm{x}_1, \dots, \mathrm{x}_p\}$ and $B_1 = \{\mathrm{y}_1, \dots, \mathrm{y}_q\}$ are sets of strong $G$-types such that $B_0 \cap B_1$ are exactly those $G$-types x from $B_0 \cup B_1$ that yield a subtype x3.

A complete invariant of $Q$ is either a simple block $B$ from a corresponding iso-equivalence, together with set $R$, or a split block $[B_0, B_1]$ together with a pair $[R_0, R_1]$ where $r_j \in R_j$ are the values of $r$ associated with each of the strong $G$-types $\mathrm{x} \in B_j$, $j \in \{0,1\}$.

The description of an iso-equivalence depends on $n$, $s$, $h$ and $\bar{r} \equiv r^h \bmod m$. While $r$ is not determined uniquely, $\bar{r}$ is the same for all choices of $r \in R$. The construction of every iso-equivalence is such that whenever $n$, $s$, $h$ and $\bar{r}$ satisfy the given conditions for one $G$-type, then corresponding conditions are satisfied by all $G$-types that occur in the given block of the iso-equivalence. For split blocks Theorems 6.20 and 6.21 give conditions (which are equivalent) for both $r_0 \in R_0$ and $r_1 \in R_1$. In this context it is important to keep in mind that $r_0^h \equiv s \bmod m$ is equivalent to $r_1^h \equiv -1 \bmod m$ since $-\bar{r}s \equiv s - \bar{r} - 1 \bmod n$.

What follows is a description of iso-equivalence in all possible circumstances. It is given without a proof since this is a direct consequence of Lemmas 6.7–6.18. In fact Lemmas 6.14–6.17 may be avoided since the isomorphisms established in these statements can be achieved, as we have observed, by composing constructions described in Lemmas 6.7–6.13.

**Theorem 6.20.** *Let $h$ be odd, $t$ even, $k \geq 2$, and suppose that $s \not\equiv 1 \bmod n/2$. All nontrivial blocks of iso-equivalence are as follows.*

(i) $s \equiv -1 + 2^{k-1} \bmod 2^k$.

  (a) $s \neq -1+n/2$. *Split blocks* $[\{\mathrm{e}\}, \{\mathrm{a},\mathrm{e}\}]$ *and* $[\{\mathrm{f}\}, \{\mathrm{b}\}]$ *if* $r_0^h \equiv s \bmod m$ *and* $r_1^h \equiv -1 \bmod m$. *Simple block* $\{\mathrm{f},\mathrm{g}\}$ *if* $r^h \equiv -1 \bmod m$. *Simple block* $\{\mathrm{b},\mathrm{g}\}$ *if* $r^h \equiv s \bmod m$.

  (b) $s = -1 + n/2$. *Simple blocks* $\{\mathrm{a},\mathrm{e}\}$ *and* $\{\mathrm{b},\mathrm{f},\mathrm{g}\}$ *if* $r^h \equiv -1 \bmod m$.

(ii) $s \equiv -1 \bmod 2^k$. *Split blocks* $[\{\mathrm{d}\}, \{\mathrm{c},\mathrm{d}\}]$, $[\{\mathrm{e},\mathrm{f}\}, \{\mathrm{e}\}]$ *and* $[\{\mathrm{g},\mathrm{h}\}, \{\mathrm{h}\}]$ *if* $r_0^h \equiv s \bmod m$ *and* $r_1^h \equiv -1 \bmod m$.

(iii) $s \equiv 1 \bmod 2^{k-1} \bmod 2^k$ *and* $k \geq 3$. *Simple blocks* $\{\mathrm{d},\mathrm{g}\}$, $\{\mathrm{e},\mathrm{h}\}$, $\{\mathrm{f},\mathrm{j}\}$ *if* $s \equiv r^h \bmod m$.

(iv) $s \equiv 1 + 2^{k-1} \bmod 2^k$ *and* $k \geq 3$. *Simple blocks* $\{\mathrm{a},\mathrm{f}\}$, $\{\mathrm{b},\mathrm{h}\}$, $\{\mathrm{j},\mathrm{g}\}$ *if* $s \equiv r^h \bmod m$.

**Theorem 6.21.** *Let $h$ be odd, $t$ even, $k \geq 2$, and $s \equiv 1 \bmod n/2$. The nontrivial blocks of iso-equivalence are as follows.*

(i) $s = 1, m \neq 1$ *and* $k = 2$. *Split blocks* $[\{\mathrm{e}\}, \{\mathrm{a},\mathrm{e}\}]$, $[\{\mathrm{f}\}, \{\mathrm{b}\}]$, $[\{\mathrm{b},\mathrm{g},\mathrm{h}\}, \{\mathrm{h}\}]$ *if* $r_0^h \equiv 1 \bmod m$ *and* $r_1^h \equiv -1 \bmod m$. *Simple block* $\{\mathrm{f},\mathrm{g}\}$ *if* $r^h \equiv -1 \bmod m$.

(ii) $s = 1 + n/2$, $m \neq 1$ *and* $k = 2$. *Split blocks* $[\{\mathrm{c}\}, \{\mathrm{c},\mathrm{d}\}]$, $[\{\mathrm{e},\mathrm{f}\}, \{\mathrm{e}\}]$ *and* $[\{\mathrm{g},\mathrm{h}\}, \{\mathrm{h}\}]$ *if* $r_0^h \equiv 1 \bmod m$ *and* $r_1^h \equiv -1 \bmod m$. *Simple block* $\{\mathrm{b},\mathrm{f}\}$ *if* $r^h \equiv -1 \bmod m$.

(iii) $s = 1$ *and* $k \geq 3$. *Simple blocks* $\{\mathrm{d},\mathrm{g}\}$, $\{\mathrm{e},\mathrm{h}\}$ *and* $\{\mathrm{f},\mathrm{i},\mathrm{j}\}$ *if* $r^h \equiv 1 \bmod m$.

(iv) $s = 1 + n/2$ *and* $k \geq 3$. *Simple blocks* $\{\mathrm{a},\mathrm{f}\}$, $\{\mathrm{b},\mathrm{h}\}$ *and* $\{\mathrm{g},\mathrm{i},\mathrm{j}\}$ *if* $r^h \equiv 1 \bmod m$.

## 7. The case of quaternions

Let $G = \langle x, y; x^4 = 1, x^2 = y^2, xyx = y\rangle \cong Q_8$. It is well known that $\mathrm{Aut}(G)$ is isomorphic to the group of cube rotations (to see this identify all $u \in G$, $|u| = 4$ with cube sides in such a way that $u$ and $u^{-1}$ correspond to opposite sides). Thus $|\mathrm{Aut}(G)| = 24$ and there are 4 conjugation classes of nontrivial automorphisms, represented by

$$\begin{aligned}
\sigma_1 &= (xy\ yx)\ (x\ y)\ (x^{-1}\ y^{-1}),\\
\sigma_2 &= (x\ y\ x^{-1}\ y^{-1}),\\
\sigma_3 &= \sigma_2^2 = (x\ x^{-1})\ (y\ y^{-1}),\ \text{ and}\\
\sigma_4 &= (x\ y\ xy)\ (x^{-1}\ y^{-1}yx).
\end{aligned}$$

There are 48 permutations of $\{x^{\pm 1}, y^{\pm 1}, (xy)^{\pm 1}\}$ that respect the inverses, and these permutations are either automorphisms of $G$, or compositions $J\alpha$, where $\alpha \in \mathrm{Aut}(G)$ and $J : G \to G, u \mapsto u^{-1}$. Clearly, these are all semiautomorphisms of $G$ (they correspond to the group of all cube automorphisms).

Let us first mention the structure of groups $G \rtimes C$ where $|C| = 2h$, $C = \langle a\rangle$ and $3 \nmid h$. Clearly it may be assumed that $aua^{-1} = \sigma_i(u)$ for an $i \in \{0, 1, 2, 3\}$, where $\sigma_0 = \mathrm{id}_G$. Thus $h$ is even if $i = 2$. Denote as $G_i$ the group $G \rtimes C$ that is induced by $\sigma_i$, $0 \le i \le 3$ (the integer $h$ is a parameter of $G_i$).

**Proposition 7.1.** *If $0 \le i < j \le 3$, then $G_i \not\cong G_j$. A group $G_i$ can be expressed as $D_8 \rtimes C$ exactly in these cases.*

(i) *$i = 2$ and $h/2$ is odd. In such a case $G_2$ is isomorphic to the group of type (E1) in which $r = 1 = t$.*

(ii) *$i = 3$ and $h$ is odd. In such a case $G_2$ is isomorphic to the group of $G$-type* g *(with $r = 1$ and $t = 2$).*

Proof: It can be established easily that $G_0' = \langle y^2\rangle = G_3'$, $G_1' = \langle xy\rangle = G_2'$ and that $Z(G_i)$ is for $i = 0, 1, 2, 3$ equal to the product of $\langle y^2\rangle$ with $C$, $\langle a^2\rangle$, $\langle a^4\rangle$ and $\langle a^2\rangle$, respectively. Hence $G_i \not\cong G_j$, $0 \le i < j \le 3$.

A group $D_8 \rtimes C$ contains at least 7 different involutions. It is easy to verify that groups $G_i$ always contain a smaller number of involutions, with the exception of the two cases described in the statement.

In case (i) set $\tilde a = a$, $\tilde y = yx$ and $\tilde x = a^2x$. In case (ii) set $\tilde a = a$, $\tilde y = yx$ and $\tilde x = ax$. □

Proposition 7.1 elucidates the relationship of groups studied in earlier sections to the group of quaternions. Note that the only group of order $16h$, $h$ odd, from the earlier classification that cannot be obtained via $Q_8$ is the group of $G$-type a, Table 1.

Let us turn to the nonassociative case.

A semidirect product $G \rtimes^3_{J\alpha} C$, $\alpha \in \mathrm{Aut}(G)$ is a Moufang loop if and only if $\alpha^3(u)u^{-1} \in Z(G)$ for every $u \in G$, by [3, Proposition 7.6]. Now, $\sigma_1^3(x)x^{-1} = xy$ and $\sigma_2^3(x)x^{-1} = yx$. With respect to Proposition 1.1 we can thus state.

**Proposition 7.2.** *Let $Q$ be a finite Moufang loop of order coprime to three such that $Q = GC$, $G \cap C = 1$, $G \trianglelefteq Q$, $G \cong Q_8$ and $C$ is cyclic. Then $Q \cong G \rtimes^3_J C$ or $Q \cong G \times^3_\gamma C$ where $\gamma = (xy\ yx)$. The permutation $\gamma$ is equal to $J\sigma$, where $\sigma = \sigma_3$ is the inner automorphism of $xy$.*

Let $C = \langle a \rangle$ be finite of order $2h$. The loop $G \rtimes^3_J C$ is an instance of the well-known Chein construction [1]. The operations of loops from Proposition 7.2 are described by Table 3.

| | $j$ even | $j$ odd |
|---|---|---|
| $i$ even | $uv \cdot a^{i+j}$ | $vu \cdot a^{i+j}$ |
| $i$ odd | $uv^{-1} \cdot a^{i+j}$ | $v^{-1}u \cdot a^{i+j}$ |

| | $j$ even | $j$ odd |
|---|---|---|
| $i$ even | $uv \cdot a^{i+j}$ | $vu \cdot a^{i+j}$ |
| $i$ odd | $u\gamma(v) \cdot a^{i+j}$ | $\gamma(v)u \cdot a^{i+j}$ |

Table 3. Multiplication of $ua^i$ with $va^j$ where $u, v \in G = Q_8$, in $G \rtimes^3_J C$ (on the left) and in $G \times^3_\gamma C$, $\gamma = (xy\ yx)$ (on the right).

**Proposition 7.3.** *Let $Q = G \rtimes^3_J C$ or $Q = G \rtimes^3_\gamma C$, where $G \cong Q_8$ and $C = \langle a \rangle$, $|a| = 2h$. Then $N(Q) = Z(G)\langle a^2 \rangle = Z(Q)$, $A(Q) = Z(G)$, $Q/A(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times C$ and $Q/N(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Furthermore, $G \rtimes^3_J C \not\cong G \rtimes^3_\gamma C$.*

Proof: The formula for $N(Q)$ is a special case of a general formula from [3, Proposition 7.6]. For the rest only the nonexistence of an isomorphism requires a comment. Let us consider the number of squares in both loops. Clearly, $va^{4i}$ and $a^{2i}$ is a square for every $i \in \mathbb{Z}$ and $v \in Z(G)$. The question is whether $x^2a^{2i}$, $i$ odd is a square or not. Let $i$ be odd and $u \in G$. Then $(ua^i)^2$ is equal to $a^{2i}$ in $G \rtimes^3_J C$ and to $\sigma(u^{-1})u \cdot a^{2i}$ in $G \rtimes^3_J C$. Note that $\sigma(x^{-1})x = x^2$. □

What remains is to connect loops $G \rtimes^3_J C$ and $G \rtimes^3_\gamma C$ to loops studied in the previous sections. This means to determine when one of these loops is isomorphic to $D_8 \rtimes^3_f C$ for a semiautomorphism $f$. If $h$ is even, then $a^h \in Z(Q)$ and $\langle x, y, a^h \rangle$ clearly carries no copy of $D_8$. Assume that $h$ is odd and put $z = a^h$. In case of $G \rtimes^3_\gamma C$ there are only five involutions in $\langle x, y, z \rangle$, and hence it cannot carry a copy of $D_8$. In case $G \rtimes^3_J C$ set $\tilde{y} = y$, $\tilde{x} = xz$ and $\tilde{a} = a$. Then $\langle \tilde{x}, \tilde{y} \rangle \cong D_8$, $C$ is a complement to $\langle \tilde{x}, \tilde{y} \rangle$, and from $aya^{-1} = y^{-1}$ and $a(xz)a^{-1} = x^{-1}z$ it follows that $r = -1$ and $t = 2$. We can state:

**Proposition 7.4.** *Suppose that $G \cong Q_8$, $C = \langle a \rangle$, $|C| = 2h$. The loop $G \rtimes^3_\gamma C$ is never isomorphic to a loop of form $D_8 \rtimes^3_f C$. This is also true for a loop $G \rtimes^3_J C$ if $h$ is even. If $h$ is odd, then $G \rtimes^3_J C$ is isomorphic to a loop of $G$-type* g *from Table 1.*

Let us mention that if $h$ is odd, then there are two further isomorphism classes of nonassociative loops $D_8 \rtimes_f^3 C$ ($G$-types a and d from Table 1, i.e. loops with $t = 0$ and $r = \pm 1$).

## 8. Guide

This paper solves the isomorphism problem for Moufang loops $Q$ of finite order coprime to 3 such that $Q = GC$, $G$ and $C$ are groups, $G \cap C = 1$, $C$ is cyclic, $G$ is noncommutative of order $2n$, with defining relations $y^n = 1$, $xyx^{-1} = y^{-1+n/\kappa}$, $x^2 = y^{n/\lambda}$, where $\kappa, \lambda \in \{1, 2\}$, $\kappa = 2$ being possible only when $4|n$, and $\lambda = 2$ only when $2|n$.

If $\kappa = 2$, then $\lambda = 1$ may be assumed. If $\kappa = 2$ and $\lambda = 1$, then replacing $x$ with $x' = xy$ gives a presentation for which $\lambda = 2$.

It is assumed throughout the paper that $n = 2^k m$ where $m$ is odd. The noncommutativity of $G$ implies that $n \geq 4$ and that if $n = 4$, then $G \cong Q_8$ or $G \cong D_8$.

It is also assumed that $C = \langle a \rangle$ and that $|C| = 2h$. If $Q$ is nonassociative, then there exists no loop $Q$ with $|C|$ odd (Proposition 2.2). If $Q$ is a group, then $|C|$ might be odd, but such groups are not considered in this paper.

If $G \ncong Q_8$, then an automorphism $\alpha \in \mathrm{Aut}(G)$ is determined by $\alpha(y) = y^r$, $r \in \mathbb{Z}_n^*$, and by $\alpha(x) = xy^t$. Such an automorphism exists for any $t \in \kappa\mathbb{Z}_n$ and $r \in \mathbb{Z}_n^*$. It is denoted by $\alpha_{t,r}$.

By general theory [4], [3] the operation of $Q$ is fully determined by a semiautomorphism $f$ of $G$. If $G \ncong Q_8$, then $f$ has to be equal to $f_s\alpha$, $\alpha = \alpha_{t,r} \in \mathrm{Aut}(G)$, $f_s(y^i) = y^i$ and $f_s(xy^i) = xy^{is}$ for all $i \in \mathbb{Z}_n$, and $s^2 \equiv 1 \bmod n$. The operation of $Q$ can be then described by

$$ua^i \cdot va^j = \begin{cases} uf^i(v) \cdot a^{i+j} & \text{if } j \text{ is even} \\ u * f^i(v) \cdot a^{i+j} & \text{if } j \text{ is odd} \end{cases} \tag{8.1}$$

for any $u, v \in G$ and $i, j \in \mathbb{Z}$ where $u * v = f_s((f_s(u)f_s(v))$. It is always possible to choose $f$ in such a way that $f^{2h} = \mathrm{id}_G$. The loop is denoted as $G \rtimes_f^3 C$.

Necessary conditions for a loop defined by (8.1) to be Moufang are $(s-1)(r+1) \equiv t(s-1) \equiv 0 \bmod n$, by Lemma 3.4. If these conditions hold and if $|f|$ divides $2h$, then (8.1) yields a Moufang loop.

It may be always assumed (Corollary 4.15) that $m|t$. If this is true and if $t$ is even then the condition of $f^{2h} = \mathrm{id}_G$ may be replaced by condition $\mathrm{ord}_n(r)|2h$ (where $\mathrm{ord}_n(r)$ is the order of $r$ in $\mathbb{Z}_n^*$). By the Chinese Remainder Theorem this can be also expressed as a conjunction of $\mathrm{ord}_m(r)|2h$ and $k - v_2(r - (-1)^{(r-1)/2}) \leq v_2(2h)$.

The value $s \in \mathbb{Z}_n^*$ is an invariant of $Q$ (Proposition 2.15), and $s = 1$ if and only if $Q$ is a group. If $s \neq 1$, then $n$ (and thus also $h$, $k$ and $m$) are invariants as well, by Corollary 2.10. For $s = 1$ this is nearly true too, with an only one exception, which is described by (2.7).

The value of $r$ can be replaced by a value $r^i$ whenever $\gcd(i, 2h) = 1$ (Proposition 3.7). Hence when we say below that an isomorphism class is *determined* (amongst others) by $r$ we mean that $\{r^i; \gcd(i, 2h) = 1\}$ is one of invariants of the isomorphism class. However, when we add that $r$ is *reflected* then the invariant is equal to $\{r^i, (r')^i; \gcd(i, 2h) = 1\}$, where $r' \equiv -sr(1+n/\kappa) \bmod n$ is called the *reflexion* of $r$.

As an example of classification let us state:

**Theorem 8.1.** *Assume that $k \geq 3$, $h$ is even, $t$ is even and $r^h \equiv 1 \bmod m$. Then the isomorphism classes are uniquely determined by $s$, $t$, $r$, $\kappa$ and $\lambda$ as follows:*

(1) $s \equiv 1 \bmod 2^{k-1}$, $t = 0$, $r \equiv 3 \bmod 4$, $\kappa+\lambda \leq 3$, *and* $v_2(2h) > k - v_2(r+1)$ *if* $\kappa = 2$;

(2) $s \equiv 1 \bmod 2^{k-1}$, $t = 2^{k-v_2(2h)}m$, $r \equiv 1 \bmod 4$, $\kappa = \lambda = 1$, $k - v_2(r-1) < v_2(2h) < k$;

(3) $s \equiv -1 + n/\kappa + n/2 \bmod 2^k$, $t = 0$, $r \equiv -1 \bmod 2^k$, $\kappa + \lambda \leq 3$;

(4) $s \equiv -1 + n/\kappa \bmod 2^k$, $t = 0$, $v_2(r-s) = k-1$, $\kappa \in \{1, 2\}$, $\lambda \in \{1, 2\}$, $r$ *is reflected; and*

(5) $s \equiv r \equiv -1 + n/\kappa \bmod 2^k$, $t \in \{0, n/2\}$, $\kappa + \lambda \leq 3$, $r$ *is reflected.*

PROOF: Use Theorem 5.2, Proposition 5.6, Proposition 5.9 and Theorem 6.3. By the latter theorem type (C3) may be reduced to $\kappa = \lambda = 1$. Then it coincides with case (2). By Theorem 6.3 type (B3) does not have to be considered.

Assume $s \equiv 1 \bmod 2^{k-1}$. Type (A2) can be reduced to type (A3) through pairing, by Proposition 5.9. Because of pairing, $r \equiv 3 \bmod 4$ may be assumed for all instances of type (A3), by Proposition 5.6. No other type is relevant if $s \equiv 1 \bmod 2^{k-1}$.

Assume $s \equiv -1 \bmod 2^{k-1}$. Then $r \equiv -1 \bmod 2^{k-1}$, by Lemma 3.4. Put $\sigma = -s + 1 + n/\kappa$. If $v_2(\sigma) = k - 1$, then by pairing it may be achieved that $r \equiv -1 \bmod 2^k$, and that yields case (3) (these loops are of type (A2)). Assume $v_2(\sigma) = k$. For $v_2(r - s) = k - 1$ combine types (A2) and (B4) to get case (4). The remaining instances of type (A2) correspond to case (5). □

What happens if $r^h \not\equiv 1 \bmod m$, while the other conditions of Theorem 8.1 are satisfied? Then Theorem 6.3 implies that in case (2) (the type (C3)) values $(\kappa, \lambda) = (1, 2)$ and $(\kappa, \lambda) = (2, 1)$ have to be also admitted since they yield different isomorphism classes. Furthermore, type (B3) then yields isomorphism classes of their own, and so the classification has to be extended, if $r^h \not\equiv 1 \bmod m$, by case

(6) $s \equiv 1 \bmod 2^{k-1}$, $t = 0$, $\kappa = 2$, $\lambda \in \{1, 2\}$, $v_2(2h) = k - v_2(r+1)$.

Otherwise the classification done in Theorem 8.1 remains intact.

A classification solving the isomorphism problem for $k = 2$, $h$ even and $t$ even appears in Theorem 8.2. No explicit proof seems to be necessary since this is a direct application of Theorems 5.2 and 6.2. Note that pairing can be used freely and does not result in a change of type, by Propositions 5.6 and 5.9. The only relevant types are (A2), (B4) and (D2). Case $\kappa = 2$, $m = 1$ is excluded because of the requirement that $G$ is nonabelian.

**Theorem 8.2.** *Assume $k = 2$, $t$ even, $h$ even, $\kappa \neq 2$ if $m = 1$, and $G \not\cong Q_8$. Then $Q$ is isomorphic to a loop that satisfies exactly one of the following conditions.*

(1) *$r \equiv 1 \bmod 4$, $\kappa + \lambda \leq 3$, $t = 0$, and either $s \equiv 1 \bmod 4$, $\kappa = 1$ or $s \equiv 3 \bmod 4$, $\kappa = 2$.*

(2) *$\lambda \in \{1, 2\}$, $t = 0$, $r$ is reflected, and either $s \equiv 3 \bmod 4$, $r \equiv 1 \bmod 4$, $\kappa = 1$, or $s \equiv 1 \bmod 4$, $r \equiv 3 \bmod 4$, $\kappa = 2$.*

(3) *$t \in \{0, n/2\}$, $\kappa + \lambda \leq 3$, $r$ is reflected, and either $s \equiv r \equiv 3 \bmod 4$, $\kappa = 1$, or $s \equiv r \bmod 3$, $\kappa = 2$.*

*If $r^h \not\equiv -1 \bmod m$ or if $2(s - 1) \not\equiv 0 \bmod n$, then the values of $s$, $\kappa$, $\lambda$, $h$, $m$ and $r$ fulfilling (1), (2) or (3) determine an isomorphism class uniquely. For $r^h \equiv -1 \bmod m$ and $2(s-1) \equiv 0 \bmod n$ this is achieved by removing case $t = n/2$, $\kappa = 2$ from (3) if $s = 1$, and case $\lambda = 2$, $\kappa = 1$ from (2) if $s = 1 + n/2$.*

Propositions 7.1, 7.2 and 7.3 solve completely the isomorphism problem for $G \cong Q_8$, $h$ even (no such loop is isomorphic to a loop described in Theorem 8.2).

From Theorems 5.1, 6.2, 6.3 and 6.9 we immediately get:

**Theorem 8.3.** *Assume that $k \leq 1$ and that $t$ is even if $k = 1$. Then it may be assumed that $t = 0$. If $t = 0$, then an isomorphism class is determined by $r$, where $r$ is reflected, and by $\lambda$, $1 \leq \lambda \leq k + 1$.*

If $G \not\cong Q_8$ and $k \geq 1$, then the parity of $t$ is invariant. The structure of $Q$ is easy to describe (cf. Theorem 8.4 below) if $t$ is odd. All loops with $t$ odd that can also be obtained as an extension of $Q_8$ are described in Proposition 7.1 (they have $k = 2$ and are groups). Using Theorems 5.1, 6.2, 6.3 and 6.19, and Proposition 5.5 we can state:

**Theorem 8.4.** *Loops $Q$ with $k \geq 1$ and $t$ odd exist if and only if $\kappa = 1$, $s \equiv 1 \bmod 2^k$, $v_2(h) + v_2(r + 1) \geq k$ and $\mathrm{ord}_m(r) | 2h$. It may be assumed that $t = m$. If this is true, then the loop is determined up isomorphism only by $\lambda$ and $r$. The parameter $r$ is reflected if and only if $v_2(h) \leq k$.*

What remains is the case of $h$ odd, $t$ even and $k \geq 2$. If $n = 4$, then either $G \cong Q_8$ or $G \cong D_8$. If $Q \cong D_8$, then $Q$ is isomorphic to a loop with $(s, r, t)$ equal to $(1, 1, 0)$, $(1, 1, 2)$, $(3, 1, 0)$, $(3, 3, 0)$ and $(3, 3, 2)$ where each of the triples gives, together with $h$, a complete invariant. From these five cases those with $t = 0$ cannot be obtained by extending $Q_8$, while for those with $t = 2$ this is possible. The solution for the isomorphism problem when $G \cong Q_8$ and $h$ is odd may be found in Propositions 7.1, 7.2 and 7.3.

Assume now that $n \neq 4$. Then $Q$ is isomorphic to a loop with parameters given by Table 1 and Table 2 (all of them have to satisfy $r^{2h} \equiv 1 \bmod m$ and no other condition is needed to guarantee the existence).

There are four different situations described in the tables, depending upon the value of $s$ modulo $2^k$. For each of these four values the loops are classified by their $G$-type x. Such a $G$-type may have two subtypes, x1 and x2. In such a case if a loop of a $G$-subtype x1 is determined by $r \in \mathbb{Z}_n^*$, then its reflexion $r' \equiv -sr(1 + n/\kappa) \bmod n$ determines an isomorphic loop of subtype x2.

If a $G$-type x has only one subtype, then the subtype is either x0 or x3. In case of x0 the parameter $r$ is unreflected, i.e. the isomorphism type is the same exactly for all values $r^i$, $\gcd(i, 2h) = 1$, while in case of x3 it is reflected, i.e. the isomorphism type is the same exactly for all values $r^i$ and $(r')^i$, $\gcd(i, 2h) = 1$.

If $s = 1$ and $k = 2$, then $G$-type d is to be excluded in order to avoid the duplicity of (2.7).

If $h$ is odd, $k \geq 2$, $n > 4$ and $t$ is even, then every loop with such parameters is isomorphic to a loop with parameters equal to one of the $G$-types of Table 1 and Table 2. In case of Table 1 no two loops with different $G$-type may be isomorphic if $r^h \not\equiv -1 \bmod m$ and $(r')^h \not\equiv -1 \bmod m$. A similar condition for Table 2 is $r^h \not\equiv s \bmod m$. When such a condition holds, then each isomorphism class is determined only by the $G$-type, by $h$, and by $r$ (rules how $G$-subtypes influence the reflexion of $r$ have been described above).

If one of $r^h$ or $(r')^h$ gives $-1$ modulo $m$ (Table 1) or if $r^h$ gives $s$ (Table 2), then classification up to isomorphism is obtained by fusing several $G$-types (while the interpretation of parameter $r$ remains unaffected). Rules for the fusion are expressed by Theorems 6.20 and 6.21. To explain the meaning of these two statements first note that they refer to what is called a strong $G$-type. If a $G$-type consists of only one subtype, then the notion of (ordinary) and strong $G$-type coincide. If there are $G$-subtypes x1 and x2, then a strong $G$-type x is defined by selecting one of these two subtypes (the parameter $r$ is then considered with respect to the selected subtype). The selection of the subtype is done uniformly: in Table 1 choose the subtype with $v_2(r - s) \geq k$ and in Table 2 the subtype with $r \equiv 1 \bmod 4$.

A simple block $\{x, y, \dots\}$ (in the sense of Theorems 6.20 and 6.21) means that the $G$-types of the block are fused and that the parameter $r$ has the same meaning for all these $G$-types in a same way. A split block $[\{x, \dots\}, \{y, \dots\}]$ means that the $G$-types $x, \dots, y, \dots$ are fused, and that loops of $G$-types $x, \dots$ determined by parameter $r = r_0$ yield loops isomorphic to those of $G$-types $y, \dots$ that are determined by the reflected parameter $r' = r_1$.

Note that Theorems 6.20 and 6.21 do not list trivial blocks explicitly. Assume that $n = 2^k \geq 3$ and $|C| = 2$. Then $t$ may be odd if and only if $Q$ is a group, by Theorem 8.4, and there exist two isomorphism type (they differ by the value of $\lambda$). Assume that $t$ is even (then $t$ may be chosen to be 0 or $n/2$). From Theorems 6.20 and 6.21 it follows immediately that there are 6 isomorphism types if $s = n - 1$ or $s = 1$ (the group case) or $s = 1 + n/2$, and that there are 5 isomorphism types if $s = -1 + n/2$.

It is clear that further research should include a classification of nonsplit extensions (which, in fact, might not be too complicated), a description of cases where 3 divides the order of $Q$, and then an overview of results for small orders, including a comparison with classifications published in [2] and [6]. The case of $|Q|$ divisible by three became accessible after Gagola extended the construction of the semidirect product in such a way that it includes this case as well [5].

## References

[1] Chein O., *Moufang loops of small order, I.*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[2] Chein O., *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197.

[3] Drápal A., *On extensions of Moufang loops by a cyclic factor that is coprime to three*, Comm. Algebra, (in print) http://dx.doi.org/10.1080/00927872.2016.1233202.

[4] Gagola S.M., III, *Cyclic extensions of Moufang loops induced by semi-automorphisms*, J. Algebra Appl. **13** (2014), no. 4, Article ID 1350128.

[5] Gagola S.hM., III, *Describing cyclic extensions of Bol loops*, Quasigroups and Related Systems **23** (2015), 31–39.

[6] Goodaire E.R., May S., Raman M., *The Moufang Loops of Order Less Than 64*, Nova Science Publishers, Inc., Commack, NY, 1999.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Praha 8, Czech Republic

*E-mail:* drapal@karlin.mff.cuni.cz

(*Received* June 24, 2015, *revised* May 30, 2016)