AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **67(2)** (2017), Pages 259–280

Classification of coset-preserving skew-morphisms of finite cyclic groups

Martin Bachratý

Slovak University of Technology
Bratislava
Slovakia
bachraty@math.sk

Robert Jajcay*

Comenius University
Bratislava
Slovakia
robert.jajcay@fmph.uniba.sk

Dedicated to the memory of Dan Archdeacon—a friend,
a colleague, a co-author.

Abstract

The concept of a coset-preserving skew-morphism is a generalization of the widely studied t-balanced skew-morphisms of regular Cayley maps which are in turn generalizations of group automorphisms. In case of abelian groups, all skew-morphisms of regular Cayley maps are roots of coset-preserving skew-morphisms, and therefore, classification of coset-preserving skew-morphisms of finite abelian groups is the first step toward classification of all skew-morphisms of these groups. We present a characterization of coset-preserving skew-morphisms of finite cyclic groups, and devise an algorithm for their classification.

1 Introduction

Skew-morphisms were introduced in [10] to facilitate the classification of regular Cayley maps [19, 20, 18, 17, 8]. As regular Cayley maps constitute a very important subclass of orientably regular maps (2-cell embeddings of graphs into orientable

[*] Also at University of Primorska, Koper, Slovenia.

surfaces whose orientation preserving automorphism groups act regularly on their sets of darts), from their introduction, skew-morphisms received a lot of attention [4, 5, 7, 9, 13, 14, 15, 21, 22, 23]. They have also proved fundamental in several related areas of algebraic and topological graph theory [11, 12], and in finite group theory have been shown to be the key ingredient in the theory of products of groups with at least one factor being cyclic [6]. Nevertheless, being of dual algebraic and combinatorial character, skew-morphisms resist attempts at classification even for the well understood class of cyclic groups [6, 13], with the recent paper [14] achieving the classification of skew-morphisms for cyclic p-groups.

Instead of restricting the groups considered, one can choose to look for subclasses of skew-morphisms that may be more accessible to the use of algebraic techniques. One such well understood subclass is the class of t-balanced skew-morphisms [4, 16, 7, 15], which are generalizations of group automorphisms, and are in fact equal to group automorphisms on subgroups of index 2. The concept of a coset-preserving skew-morphism is a generalization of that of a t-balanced skew-morphism which preserves some of the most important algebraic characteristics of the t-balanced skew-morphisms. It is a relatively new concept originally introduced by the first of the authors of this paper in his bachelor (and later in his diploma) thesis [1].

The first research article [2] on this topic just appeared in the Proccedings of SIGMAP 2014 published by Springer. That paper contains (among other) a proof that all skew-morphisms of finite abelian groups giving rise to regular Cayley maps possess non-trivial powers (as permutations) that are coset-preserving. Thus, in addition to being closely related to group-automorphisms, coset-preserving skew-morphisms are the building stones for all skew-morphisms of regular Cayley maps of abelian groups; an additional motivation for trying to classify this class of skew-morphisms.

The main theorem of the present article represents a classification of coset-preserving skew-morphisms for finite cyclic groups. This is achieved via a careful consideration of properties of these skew-morphisms with respect to a number of general properties of skew-morphisms in Sections 2, 3 and 4 and subsequently by showing the sufficiency of these properties for the existence of a coset-preserving skew-morphism in Section 5. We conclude the paper with an algorithm based on our classification, followed by a couple of examples of its use.

2 Properties of general skew-morphisms

Given a finite group G, a permutation $\varphi : G \to G$ of order $|\varphi| = m$ (in the full symmetric group $Sym(G)$), together with a function $\pi : G \to \mathbb{Z}_m$ is said to be a *skew-morphism* of G, with an associated *power function* π, if $\varphi(1_G) = 1_G$ and

$$\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) \quad \text{for all } a, b \in G, \tag{1}$$

where $\varphi^{\pi(a)}(b)$ is the image of b under φ applied $\pi(a)$ times. Skew-morphisms possess a number of algebraic properties:

Lemma 2.1 ([10]) *Let φ be a skew-morphism of a group G of order $|\varphi| = m$ with the power function π. Then the following hold:*

(i) *The set* $\ker \pi = \{g \in G \mid \pi(g) = 1\}$ *is a subgroup of G;*

(ii) *$\pi(g) = \pi(h)$ if and only if g and h belong to the same right coset of the subgroup* $\ker \pi$ *in G;*

(iii) *the set* $\mathrm{Fix}\ \varphi = \{g \in G \mid \varphi(g) = g\}$ *is a subgroup of G;*

(iv) *$\pi(ghg^{-1}) = 1$ for all $h \in \ker \pi \cap \mathrm{Fix}\ \varphi$ and all $g \in G$;*

(v) *the group* $\ker \pi \cap \mathrm{Fix}\ \varphi$ *is a normal subgroup of* $\mathrm{Fix}\ \varphi$*;*

(vi) *for any $g \in G$ the equation $\varphi(gh) = \varphi(g)\varphi^i(h)$ holds for each $h \in G$ if and only if $i \equiv \pi(g) \pmod m$;*

(vii) *if $\pi(g) = 0$ for some $g \in G$, then φ is the identity permutation;*

(viii) *$\pi(1_G) = 1$;*

(ix) *for any $g, h \in G$ we have*

$$\pi(gh) \equiv \sum_{i=0}^{\pi(g)-1} \pi(\varphi^i(h)) \pmod m. \tag{2}$$

The equation (2) can be viewed as the definition of an extension σ of the power function π to the set of pairs $\mathbb{Z} \times G$:

$$\sigma(i, h) \equiv \sum_{i=0}^{i-1} \pi(\varphi^i(h)) \pmod m. \tag{3}$$

The extended power function will prove repeatedly useful throughout our paper, in particular in evaluating powers of φ [6]:

$$\varphi^j(gh) = \varphi^j(g)\varphi^{\sigma(j,g)}(h), \tag{4}$$

for all $j \geq 1$, and $g, h \in G$.

Skew-morphisms of abelian groups have even more algebraic properties (which do not have to be satisfied by skew-morphisms of non-abelian groups).

Lemma 2.2 ([4]) *Let φ be a skew-morphism of an abelian group A of order $|\varphi| = m$ with the power function π. Then the following hold:*

(i) *The skew-morphism φ preserves* $\ker \pi$ *setwise, i.e.,* $\varphi(\ker \pi) = \ker \pi$*;*

(ii) *the restriction of φ to* $\ker \pi$ *is a group automorphism of* $\ker \pi$*;*

(iii) *for each $a \in A$, the number $\pi(a)$ is congruent to 1 modulo the length of every non-trivial orbit of φ on* $\ker \pi$*;*

(iv) *if $a \in A$ is stabilized by φ, i.e, $\varphi(a) = a$, then $\pi(a) = 1$.*

3 Properties of general coset-preserving skew-morphisms

Clearly, group automorphisms are skew-morphisms with $\pi(a) = 1$, for all $a \in G$ and $\ker \pi = G$. A *t-balanced skew-morphism* [4] is a skew-morphism φ whose kernel is a subgroup of G of index two preserved by φ with the property $\pi(a) = t$ for all a in the complement of $\ker \pi$ in G. The restriction of φ to $\ker \pi$ is necessarily a group automorphism of $\ker \pi$, and thus t-balanced skew-morphisms are as close to being group automorphisms (without actually being group automorphisms) as possible. Interestingly, every t-balanced skew-morphism raised to the $(t+1)$-st power becomes a group automorphism [7]. All t-balanced skew-morphisms preserve the cosets of their kernels, i.e., map elements from a coset of $\ker \pi$ to an element from the same coset.

This simple observation leads us to the definition of the key topic of this article: A skew-morphism φ of G of order m is said to be *coset-preserving* if $\pi(\varphi(a)) \equiv \pi(a) \pmod{m}$, for all $a \in G$. Thus, automorphisms and t-balanced skew-morphisms are always coset-preserving, but there exist many coset-preserving skew-morphisms whose kernels are of much larger index than 2 in G. For a variety of examples of coset-preserving skew-morphisms, the reader is advised to consult [2] or the examples at the end of our paper. For reader's convenience, we include Table 1 that summarizes information contained in Conder's lists of skew-morphisms [3] with regard to the distribution of the above classes in the full sets of skew-morphisms for cyclic groups of order up to 30. The four sets Auto $\mathbb{Z}_n$, t–bal $\mathbb{Z}_n$, CP Skew $\mathbb{Z}_n$ and Skew $\mathbb{Z}_n$ denote the set of automorphisms, the set of t-balanced skew-morphisms, the set of coset-preserving skew-morphisms, and the set of all skew-morphisms for $\mathbb{Z}_n$, respectively. Orders of groups for which Skew $\mathbb{Z}_n$ = Auto $\mathbb{Z}_n$ (i.e., groups, whose only skew-morphisms are automorphisms), are left out of the list. For example, groups of prime order as well as some groups of order a product of two distinct primes or a square of a prime have been shown to have this property in [6].

If φ is not a coset-preserving skew-morphism of G, then G contains elements b for which $\pi(\varphi(b)) \not\equiv \pi(b) \pmod{m}$. To study such elements, the paper [2] introduces the concept of periodicity. For an arbitrary element $a \in G$ we define the *periodicity* p_a of a as the smallest positive integer such that $\pi(a) = \pi(\varphi^{p_a}(a))$. Note that p_a is well defined as $p_a \leq |\mathcal{O}_a| < \infty$, where $\mathcal{O}_a$ denotes the orbit of a under φ. In the case when G is abelian, $p_a = p_b$ for any two elements in the same orbit of φ [2]. Thus, for abelian groups, we can define the periodicity $p_{\mathcal{O}}$ of an orbit $\mathcal{O}$ of φ as the periodicity of any element in $\mathcal{O}$. For a skew-morphism φ of an arbitrary group G we define the periodicity p_φ of φ as the smallest common multiple of the periodicities of all elements in G. In the case of abelian groups, p_φ equals the least common multiple of periodicities of all orbits of φ. The most important properties of the periodicity of the skew-morphisms of abelian groups are summarized in the following lemma.

Lemma 3.1 ([2]) *Let φ be a skew-morphism of an abelian group A with the power function π. Then the following hold:*

(i) *If a, b belong to the same orbit of φ, then $p_a = p_b$;*

n	$\lvert$Skew $\mathbb{Z}_n\rvert$	$\lvert$CP Skew $\mathbb{Z}_n\rvert$	$\lvert$t-bal $\mathbb{Z}_n\rvert$	$\lvert$Auto $\mathbb{Z}_n\rvert$
6	4	4	2	2
8	6	6	2	4
9	10	6	0	6
10	8	8	4	4
12	8	8	4	4
14	12	12	6	6
16	20	20	12	8
18	30	14	8	6
20	24	24	8	8
21	24	24	0	12
22	20	20	10	10
24	24	24	16	8
25	68	20	0	20
26	24	24	12	12
27	85	30	0	18
28	24	24	12	12
30	32	32	24	8

Table 1: The distribution of skew-morphisms for some small cyclic groups

(ii) *if $\pi(a) = \pi(b)$ for some a, $b \in A$, then $\pi(\varphi(a)) = \pi(\varphi(b))$ and $p_a = p_b$;*

(iii) *if a belongs to* $\ker \pi$*, then $p_a = 1$;*

(iv) *the number p_a divides both $|\mathcal{O}_a|$ and $|\varphi|$;*

(v) *the values $\pi(a)$ and $\pi(\varphi^j(a))$ are the same for some positive integer j if and only if $p_a \mid j$;*

(vi) *the periodicity p_a of $a \in A$ divides $\sigma(p_a, b)$ for each $b \in \mathcal{O}_a$;*

(vii) *if a and b belong to the same orbit of φ, then $\sigma(p_a, a) = \sigma(p_a, b)$ and $\sigma(jp_a, b) = j \cdot \sigma(p_a, b)$ for any positive integer j;*

(viii) *the periodicity p_{ab} of the product of elements a, $b \in A$ divides the least common multiple of the periodicities of a and b, i.e., $p_{ab} \mid \mathrm{lcm}(p_a, p_b)$,*
in particular, $p_{a_1 a_2 \dots a_\ell} \mid \mathrm{lcm}(p_{a_1}, p_{a_2}, \dots, p_{a_\ell})$ for $a_1, \dots, a_\ell \in A$;

(ix) *φ^{p_φ} is a coset-preserving skew-morphism, and if a and b belong to the same orbit of φ and $\overline{\pi}$ is the power function of φ^{p_φ}, then $\overline{\pi}(a) = \overline{\pi}(b)$;*

(x) *p_φ is the order of the skew morphism induced by φ on the factor group $G/\ker \pi$.*

If G is a finite abelian group, and φ is a skew-morphisms of G with at least one orbit that generates G, then φ^{p_φ} is a *non-trivial* coset-preserving skew-morphism [2].

Obviously, every skew-morphism of a finite cyclic group G possesses a generating orbit; simply the orbit of any generator of G. This means that each non-trivial skew-morphism of a finite cyclic group possesses a non-trivial power which is a coset-preserving skew-morphism (e.g., Example 5.7), and thus, coset-preserving skew-morphisms play a fundamental role in the classification of skew-morphisms of finite cyclic groups.

Theorem 3.2 **([2])** *Let φ be a non-trivial skew-morphism of a cyclic group $\mathbb{Z}_n$. Then $p_\varphi = p_g$ for any generator g of $\mathbb{Z}_n$ and φ^{p_φ} is a non-trivial coset-preserving skew-morphism of $\mathbb{Z}_n$.*

The above theorem implies that the classification of coset-preserving skew-morphisms together with the classification of the roots of coset-preserving skew-morphisms of finite cyclic groups which are also skew-morphisms would yield a classification of all skew-morphisms of finite cyclic groups. In what follows, we complete the first part of such classification, namely, we classify coset-preserving skew-morphisms of finite cyclic groups.

It is easy to see that a skew-morphism φ is coset-preserving if and only if its periodicity $p_\varphi = 1$. The next lemma will help us considerably simplify the calculations involving the power functions of coset-preserving skew-morphisms.

Lemma 3.3 **([2])** *Let A be a finite abelian group, and let $\varphi : A \to A$ be a non-trivial coset-preserving skew-morphism of order m with the power function π. Then π is a homomorphism from A into the multiplicative group $\mathbb{Z}_m^*$, and φ^i is a coset-preserving skew-morphism for every integer i.*

Thus, for a coset-preserving skew-morphism φ of an abelian group A we can compute the power function of the product of two elements as $\pi(ab) \equiv \pi(a)\pi(b) \pmod{m}$. Consequently, if $A = \mathbb{Z}_n$, $\pi(a) = \pi(1)^a$ for any non-zero element $a \in \mathbb{Z}_n$.

4 Properties of coset-preserving skew-morphisms of cyclic groups

Recall that the order of the kernel of a t-balanced skew-morphism φ of G must be at least half of the order of G. While this is not true for coset-preserving skew-morphisms in general, the next lemma asserts that in cyclic groups the kernels cannot be significantly smaller than $|G|$. While the lower bound stated in our lemma is the best we were able to prove in general, as demonstrated in Example 5.7, additional arithmetic considerations of the order of the cyclic group may allow for further improvements.

Lemma 4.1 *Let φ be a coset preserving skew-morphism of $\mathbb{Z}_n$ of order m with power function π. Then $|\ker \pi| > \sqrt{n}$.*

Proof: The most important ingredient to this proof is the observation that all generating orbits of a skew-morphism φ are of the same size equal to the order of φ (e.g., [2, 9]). By means of contradiction, assume that $|\ker \pi| \leq \sqrt{n}$ for a coset-preserving skew-morphism φ of $\mathbb{Z}_n$. It follows that φ is not an automorphism, and therefore $1 \notin \ker \pi$. Since φ is coset-preserving, the entire orbit $\mathcal{O}_1$ is contained in the coset $1 + \ker \pi$, and therefore $|\mathcal{O}_1| \leq |\ker \pi| \leq \sqrt{n}$. On the other hand, $\pi : \mathbb{Z}_n \to \mathbb{Z}_m^*$ by Lemma 3.3, and thus $|\mathbb{Z}_m^*| < m = |\varphi|$. Since $|\varphi| = |\mathcal{O}_1|$, we obtain

$$|\mathbb{Z}_m^*| < m = |\varphi| = |\mathcal{O}_1| \leq |\ker \pi| \leq \sqrt{n}.$$

However, different cosets of $\ker \pi$ receive different π values from $\mathbb{Z}_m^*$, and therefore by the pigeonhole principle, the index of $\ker \pi$ in $\mathbb{Z}_n$, $|\mathbb{Z}_n : \ker \pi|$, cannot exceed $|\mathbb{Z}_m^*|$. Hence $n = |\mathbb{Z}_n| = |\ker \pi| \cdot |\mathbb{Z}_n : \ker \pi| < \sqrt{n} \cdot (\sqrt{n} - 1)$; a contradiction. □

The key to the classification of coset-preserving skew-morphisms of finite cyclic groups lies in finding necessary and sufficient parameters that uniquely determine such skew-morphisms. In the forthcoming paragraphs, we determine a set of parameters together with some arithmetic conditions that must be satisfied by all coset-preserving skew-morphisms of cyclic groups. In Section 5 we use these parameters and conditions to build a permutation that we finally prove to be a coset-preserving skew-morphism with the corresponding set of parameters. Thus, the parameters and conditions derived in this section are necessary and sufficient for the existence of the skew-morphisms we are interested in here.

Let φ be a non-trivial coset-preserving skew-morphism of a finite cyclic group G. From now on, we will use the following notation. The equation $a = b$, with $a, b \in \mathbb{Z}$, will mean that a and b are equal as integers. We will understand the congruence $a \equiv b$ without a specified modulus as a congruence modulo $|G|$, usually denoted by n. In all other cases, the modulus will be specified. We will denote the size of $\ker \pi$ by d, $d = |\ker \pi|$.

There are *five important numerical parameters* associated with φ.

- The *first parameter* of φ is the order n of G, i.e., φ is a skew-morphism of $G \cong \mathbb{Z}_n$.

- The *second parameter* $k \in \mathbb{Z}_n$ of φ is the smallest non-zero element of $\ker \pi$; necessarily a generator of $\ker \pi$. It was shown in [6] that the kernel of a skew-morphism of any finite group is non-trivial, hence, $k \geq 1$, and $k \mid n$.

- The *third parameter* h of φ is the difference between the elements $\varphi(1)$ and 1 modulo $n = |G|$, i.e., $h \equiv \varphi(1) - 1$, or equivalently, $\varphi(1) \equiv 1 + h$. As φ is not trivial and the orbit of 1 is generating, we have $|\mathcal{O}_1| = |\varphi| > 1$, and therefore $h \neq 0$. Moreover, $h \in \ker \pi$ as φ is coset-preserving, and thus, h is one of the non-zero elements of $\ker \pi$: k, $2k$, $\ldots$, $(d-1)k$.

- The *fourth parameter* s of φ is the smallest positive integer satisfying $\varphi(k) \equiv s \cdot k$. Note that this congruence always has a solution, since $\varphi(k) \in \ker \pi =$

$\{0,\, k,\, 2k,\, \ldots,\, (d-1)k\}$. Since the restriction of φ to $\ker\pi$ is a group automorphism, $(d,s)=1$, and the restriction of φ to $\ker\pi$ is the multiplication by s, $\varphi(b) \equiv s \cdot b$, for all $b \in \ker\pi$.

- The *fifth parameter* e of φ is the value $\pi(1)$. Note that by Lemma 3.3, $\pi(a) \equiv \pi(1)^a \equiv e^a \pmod{|\varphi|}$, for each $a \in \mathbb{Z}_n$. As k is the smallest element of $\ker\pi$, the elements $1, 2, 3, \ldots, k$ belong to different cosets of $\ker\pi$, and therefore the values $e^1,\, e^2,\, \ldots,\, e^k$ are pairwise distinct modulo $|\varphi|$ with $e^k \equiv 1 \pmod{|\varphi|}$ (since k belongs to the kernel). Thus, the order of e in the multiplicative group $\mathbb{Z}^*_{|\varphi|}$ equals k.

We claim that φ is completely determined by its five parameters $(n;\, k,\, h,\, s,\, e)$. First, for any $a \in \mathbb{Z}_n$, applying (4) in the fourth step and (3) in the fifth yields:

$$\begin{aligned}\varphi(a) &\equiv \varphi(1+(a-1)) \equiv \varphi(1) + \varphi^e(a-1) \equiv \varphi(1) + \varphi^e(1+(a-2)) \equiv \\ &\equiv \varphi(1) + \varphi^e(1) + \varphi^{\sigma(e,1)}(a-2) \equiv \varphi(1) + \varphi^e(1) + \varphi^{e^2}(a-2).\end{aligned}$$

By an easy induction argument,

$$\varphi(a) \equiv \varphi(1) + \varphi^e(1) + \varphi^{e^2}(1) + \cdots + \varphi^{e^{a-1}}(1), \text{ for each } a \in \mathbb{Z}_n. \qquad (5)$$

Thus $\varphi(a)$ is uniquely determined for any $a \in \mathbb{Z}_n$ by the action of φ on the orbit $\mathcal{O}_1$ of 1 and the parameter e. We proceed to show that $\mathcal{O}_1$ is uniquely determined by the parameters h and s. We begin by showing that the following equation holds

$$\varphi^i(1) \equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h, \text{ for each positive integer } i. \qquad (6)$$

It clearly holds for $i=1$ by the definition of h. To prove the general claim, we proceed by induction. Suppose (6) holds for all $i < N$. Since $h \in \ker\pi$, so is any of its multiples, and hence, $(s^0h + s^1h + \cdots + s^{N-2}h)$ belongs to $\ker\pi$. Thus, $\pi(s^0h + s^1h + \cdots + s^{N-2}h) = 1$ and $\varphi(s^0h + s^1h + \cdots + s^{N-2}h) \equiv s \cdot (s^0h + s^1h + \cdots + s^{N-2}h)$. Finally,

$$\begin{aligned}\varphi^N(1) &\equiv \varphi(\varphi^{N-1}(1)) \equiv \varphi(1 + s^0h + s^1h + \cdots + s^{N-2}h) \equiv \\ &\equiv \varphi((s^0h + s^1h + \cdots + s^{N-2}h) + 1) \equiv \varphi(s^0h + s^1h + \cdots + s^{N-2}h) + \varphi(1) \equiv \\ &\equiv s^1h + s^2h + \cdots + s^{N-1}h + 1 + h,\end{aligned}$$

as claimed. Equation (6) clearly yields that the choice of s and h determines the action of φ on $\mathcal{O}_1$.

We will call a five-tuple of parameters $(n;\, k,\, h,\, s,\, e)$ of a coset-preserving skew-morphism φ the *parameter set of* φ and denote it by $\operatorname{Par}\varphi$. It follows directly from the definition of the parameter set that two non-trivial coset-preserving skew-morphisms of cyclic groups with different parameter sets are not equal, as two coset-preserving skew-morphisms φ and φ' of cyclic groups with different parameter sets are either associated with different groups, or have different kernels $\ker\pi \neq \ker\pi'$, or have different values $\varphi(1)$ and $\varphi'(1)$, or have different values at elements of $\ker\pi$ and

$\ker \pi'$, or have different values of their power functions at 1, respectively (depending on in which of the five parameters $(n;\ k,\ h,\ s,\ e)$ they differ). On the other hand, two non-trivial coset-preserving skew-morphisms ψ and ψ' of cyclic groups with the same parameter sets are equal, as they are uniquely determined by their parameters and the equations (5) and (6). All these observations are summed up in the following theorem.

Theorem 4.2 *Let φ and ψ be non-trivial coset-preserving skew-morphisms of cyclic groups with the parameter sets* $\operatorname{Par}\varphi$ *and* $\operatorname{Par}\psi$*. Then $\varphi = \psi$ if and only if* $\operatorname{Par}\varphi = \operatorname{Par}\psi$*.*

The parameters $(n;\ k,\ h,\ s,\ e)$ satisfy a number of necessary conditions (a slightly different list appears already in [2]).

Theorem 4.3 *Let φ be a non-trivial coset-preserving skew-morphism of a cyclic group with the parameter set* $\operatorname{Par}\varphi = (n;\ k,\ h,\ s,\ e)$*. Then the following hold:*

(i) *All five parameters are positive integers;*

(ii) *the parameter k divides n and $k < n$;*

(iii) *if $d = \frac{n}{k}$, then $s < d$ and $(s, d) = 1$;*

(iv) *the parameter h belongs to the set $\{k,\ 2k,\ \ldots,\ (d-1)k\}$;*

(v) *if r denotes the smallest positive integer such that $1 \equiv 1 + s^0h + s^1h + \cdots + s^{r-1}h$, then r is the order of φ; in particular, $e < r$ and the order of e in $\mathbb{Z}_r^*$ equals k;*

(vi) $s \cdot k \equiv \sum\limits_{i=0}^{k-1} (1 + s^0h + \cdots + s^{e^i-1})$;

(vii) $s^{e-1} \equiv 1 \pmod{d}$.

Proof: Properties (i), (ii), (iii), (iv) and (v) follow directly from the definitions of the corresponding parameters and the preceding discussion. The congruence (vi) holds, since $\varphi(k) \equiv sk$ by the definition of s and k, while, $\varphi(k) \equiv \varphi(1) + \varphi^e(1) + \varphi^{e^2}(1) + \cdots + \varphi^{e^{k-1}}(1)$, by (5), and

$$\varphi(1) + \varphi^e(1) + \varphi^{e^2}(1) + \cdots + \varphi^{e^{k-1}}(1) \equiv \sum_{i=0}^{k-1} (1 + s^0h + \cdots + s^{e^i-1})$$

by repeated applications of (6).

To prove (vii), consider the following calculation:

$$\varphi(k) + \varphi(1) \equiv \varphi(k+1) \equiv \varphi(1+k) \equiv \varphi(1) + \varphi^e(k).$$

Thus, $\varphi(k) \equiv \varphi^e(k)$, and hence $sk \equiv s^ek$. Since $n = kd$, it follows that $s \equiv s^e \pmod{d}$, or equivalently, $1 \equiv s^{e-1} \pmod{d}$ as $(s, d) = 1$ by (iii).

Finally, the order of φ is equal to the length of the orbit of 1 under φ which can be easily seen to be equal to the integer r defined in (v). □

5 Building a skew-morphism from a parameter set

We say that parameters $(n;\ k,\ h,\ s,\ e)$ are *admissible*, if they satisfy all the conditions of Theorem 4.3, which we will refer to as Conditions (i) through (vii).

Our goal in this section is to show that given an admissible five-tuple of parameters $(n;\ k,\ h,\ s,\ e)$, one can construct a coset-preserving skew-morphism φ of $\mathbb{Z}_n$ such that $\operatorname{Par}\varphi = (n;\ k,\ h,\ s,\ e)$.

We first employ equations (5) and (6) to define a permutation of $\mathbb{Z}_n$. Let $d = \frac{n}{k}$, and suppose that there exists at least one positive i such that $1 \equiv 1+s^0h+s^1h+\cdots+s^{i-1}h$. Let r be the smallest of such i's. (Note that, so far, we have no assurance that such an r exists.) Recall our convention that instead of $a \equiv b \pmod{n}$ we will simply write $a \equiv b$, and let us define a permutation $\tau : \mathbb{Z}_n \to \mathbb{Z}_n$ in two steps as follows.

First let $\tau(0) \equiv 0$ and let

$$\tau^i(1) \equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h, \text{ for each positive integer } i. \tag{7}$$

To argue the existence of the above mentioned r, as well as that formula (7) actually defines an orbit of a permutation on $\mathbb{Z}_n$, we will need the following lemma.

Lemma 5.1 *Let $(n;\ k,\ h,\ s,\ e)$ be an admissible parameter set. Then the following hold:*

(i) *The sum $1 + s^0h + s^1h + \cdots + s^{j-1}h$ is non-zero modulo n for each $j \geq 1$;*

(ii) *there exists a positive integer i such that $1 \equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h$;*

(iii) *Values $1+s^0h+s^1h+\cdots+s^{i-1}h$ and $1+s^0h+s^1h+\cdots+s^{j-1}h$ are congruent modulo n if and only if $i \equiv j \pmod{r}$.*

Proof: Condition (iv) asserts that $k \mid h$, and therefore, $1+s^0h+s^1h+\cdots+s^{j-1}h \equiv 1 \pmod{k}$, for all $j \geq 1$. The first assertion of our lemma now follows from the fact that k also divides n.

Next, recall that $n = dk$ and that $(d, s) = 1$, and suppose that $1 \not\equiv 1 + s^0h + s^1h + \cdots + s^{i-1}h$ for all $i \geq 1$. Clearly, there must exist two positive integers $i < j$ such that

$$1 + s^0h + s^1h + \cdots + s^{i-1}h \equiv 1 + s^0h + s^1h + \cdots + s^{j-1}h.$$

By subtracting the left side of this congruence from both sides we obtain

$$0 \equiv s^ih + \cdots s^{j-1}h \equiv s^i(s^0h + s^1h + \cdots + s^{j-i-1}h).$$

As $k \mid h$, we have $k \mid s^0h+s^1h+\cdots+s^{j-i-1}h$. It follows that $s^0h+s^1h+\cdots+s^{j-i-1}h = \ell_1k$, for some positive integer ℓ_1, and our congruence can be replaced by the equation $\ell_2n = s^i\ell_1k$, with ℓ_1, ℓ_2 positive integers. Therefore, $\ell_2d = s^i\ell_1$. Since $(d, s) = (d, s^i) = 1$, we have $d \mid \ell_1$, and thus, $n = dk$ divides $l_1k = s^0h + s^1h + \cdots + s^{j-i-1}h$.

This means that congruence from the property (ii) has at least one positive solution, namely $j - i$.

To conclude the proof, observe that all values $1+s^0h$, $1+s^0h+s^1h$, $\ldots$, $1+s^0h+s^1h+\cdots+s^{r-1}h \equiv 1$ are distinct modulo n, as the congruence $1+s^0h+s^1h+\cdots+s^{i-1}h \equiv 1+s^0h+s^1h+\cdots+s^{j-1}h$ for some $0 < i < j < r$ would be contrary to the minimality of r. The rest of the proof follows the lines typical for arguments involving the smallest number with some divisibility property. □

Employing Lemma 5.1 yields the congruence $1 \equiv \tau^r(1)$, and hence we can view the cycle $(1,\, \tau(1),\, \ldots,\, \tau^{r-1}(1))$ as a cycle of τ. Let $Y = \{0,\, 1,\, \tau(1),\, \ldots,\, \tau^{r-1}(1)\}$. We define τ for all the remaining elements of $\mathbb{Z}_n \setminus Y$ using equation (5):

$$\tau(a) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1), \text{ for each } a \in \mathbb{Z}_n \setminus Y. \tag{8}$$

This establishes τ as a well-defined mapping $\tau : \mathbb{Z}_n \to \mathbb{Z}_n$. The following lemma lists other important properties of τ.

Lemma 5.2 *Let $(n;\, k,\, h,\, s,\, e)$ be a set of admissible parameters, and let τ, r and d be defined as above. Then the following hold:*

(i) $\tau^r(1) \equiv 1$;

(ii) $\tau^i(1) \equiv \tau^j(1)$ *if and only if* $i \equiv j \pmod r$;

(iii) $\tau(a) \equiv a \pmod k$ *for each* $a \in \mathbb{Z}_n$;

(iv) $\tau^{e^{lk}}(1) \equiv \tau(1)$ *for each positive integer* l;

(v) $\tau(lk) \equiv slk$ *for any positive integer* l;

(vi) $\tau(lk) \equiv \tau^{e^i}(lk)$ *for any positive integers* l *and* i;

(vii) $\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{b-1}}(1)$, *for each pair* a, b *of positive integers congruent modulo* n;

(viii) $\tau(\tau^i(1)) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^i(1)-1}}(1)$ *for each positive integer* i;

(ix) $\tau(a+lk) \equiv \tau(a)+slk$ *for any non-negative integer* a *and any positive integer* l.

Proof: Properties (i) and (ii) follow immediately from Lemma 5.1. To prove the property (iii), first note that it holds for all elements of Y as $\tau^i(1) \equiv 1 \pmod k$ for each positive integer i by (7). Thus, considering an $a \notin Y$, we have

$$\tau(a) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a-1}}(1) \equiv 1 + \cdots + 1 \equiv a \pmod k$$

by (8). Property (iv) is a straightforward consequence of Condition (v) and property (ii) of this lemma, as $e^{lk} \equiv (e^k)^l \equiv 1 \pmod r$. To prove property (v), first observe that for any positive integer l, the product lk does not belong to $Y \setminus \{0\}$ and that the claim clearly holds for $lk \equiv 0$, thus we may apply (8)

$$\tau(lk) = \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{lk-1}}(1).$$

Repeated application of property (iv) of this lemma yields

$$\tau(lk) = l \cdot (\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{k-1}}(1)).$$

Since Condition (vi) establishes $\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{k-1}}(1) = s \cdot k$, we have $\tau(lk) = slk$. Given any positive integer i, $\tau^i(lk) \equiv 0 \pmod{k}$, by property (iii) of this lemma. Thus, by property (v), we have $\tau^i(lk) \equiv s^i lk$ for any positive integer i. Also recall that $s^{e-1} \equiv 1 \pmod{d}$ by Condition (vii). It follows that $s^{e^i-1} \equiv 1 \pmod{d}$ for any positive integer i as $e - 1 \mid e^i - 1$. Thus $s^{e^i} \equiv s^{e^i-1}s \equiv s \pmod{d}$, or equivalently, for any positive integer we have $s^{e^i} = s + jd$ for some integer j. Summing up, we obtain

$$\tau^{e^i}(lk) \equiv s^{e^i}lk \equiv (s + jd) \cdot lk \equiv slk + jdlk \equiv slk,$$

where $jdlk \equiv 0$ due to $n = dk$; which proves (vi).

To prove (vii), suppose without loss of generality that $a \leq b$, i.e., $b = a + ln$ for some non-negative integer l, and consider the following calculation:

$$\begin{aligned}
&\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{a+ln-1}}(1) \equiv \\
&\equiv \Big(\tau(1) + \tau^{e}(1) + \cdots + \tau^{e^{ln-1}}(1)\Big) + \Big(\tau^{e^{ln}}(1) + \tau^{e^{ln+1}}(1) + \cdots + \tau^{e^{a+ln-1}}(1)\Big) \equiv \\
&\equiv \tau(ln) + \Big(\tau^{e^0}(1) + \tau^{e^1}(1) \cdots + \tau^{e^{a-1}}(1)\Big) \equiv \tau(0) + \tau(a) \equiv \tau(a),
\end{aligned}$$

where the key equality $\tau^{e^{ln}}(1) + \tau^{e^{ln+1}}(1) + \cdots + \tau^{e^{a+ln-1}}(1) \equiv \tau^{e^0}(1) + \tau^{e^1}(1) \cdots + \tau^{e^{a-1}}(1)$ follows from (iv).

As an additional consequence of (vii), note that formula (8) will yield the same result whenever we replace an element $a \in \mathbb{Z}_n$ by any other non-negative integer congruent to a modulo n. Thus, in the remaining part of this proof, we do not need to check the condition $a \in \mathbb{Z}_n$ when calculating $\tau(a)$.

We proceed to prove (viii) by induction on i. It clearly holds for $i = 0$ as $\tau(\tau^0(1)) \equiv \tau(1)$. Now suppose that

$$\tau(\tau^i(1)) \equiv \tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^i(1)-1}}(1)$$

for all $i < j$. We divide the sum

$$\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^j(1)-1}}(1)$$

into two parts:

$$\tau(1) + \tau^{e}(1) + \tau^{e^2}(1) + \cdots + \tau^{e^{\tau^{j-1}(1)-1}}(1)$$

and

$$\tau^{e^{\tau^{j-1}(1)}}(1)+\tau^{e^{\tau^{j-1}(1)+1}}(1)+\tau^{e^{\tau^{j-1}(1)+2}}(1)+\cdots+\tau^{e^{\tau^{j}(1)-1}}(1).$$

The first sum equals $\tau(\tau^{j-1}(1))=\tau^{j}(1)$ by our induction's assumption. Employing property (iv) and formula (7) yields that the second sum equals

$$\tau^{e^1}(1)+\tau^{e^2}(1)+\ldots\tau^{e^{s^{j-1}h-1}}+\tau(1)$$

as $k \mid h$. Since $s^{j-1}h\notin Y\setminus\{0\}$, the above sum equals $\tau(s^{j-1}h)$ by (8). Applying (7) and the property (v), we obtain

$$\tau^{j}(1)+\tau(s^{j-1}h)=1+s^0h+s^1h+\cdots+s^{j-1}h+s^jh=\tau^{j+1}(1)=\tau(\tau^{j}(1))$$

which completes induction, and thus the proof of (viii).

In addition, note that thanks to property (viii), formula (8) can be applied to all non-zero elements of $\mathbb{Z}_n$ (not just the elements in $\mathbb{Z}_n\setminus Y$).

Finally, property (ix) follows directly from properties (iv) and (v) as

$$\tau(a+lk)\equiv\tau(lk)+\tau^{e^{lk}}(1)+\tau^{e^{lk+1}}(1)+\cdots+\tau^{e^{lk+a-1}}(1)\equiv slk+\tau(a).$$

□

We can now proceed to show that τ is indeed a bijection. As $\mathbb{Z}_n$ is finite, it is sufficient to show that τ is an injection. Note that each element a of $\mathbb{Z}_n$ can be written uniquely as $a=\overline{a}+l_ak$ where $\overline{a}\in\{0,\,1,\,\ldots,\,k-1\}$ and $l_a\in\{0,\,1,\,\ldots,\,d-1\}$. Suppose that $\tau(a)\equiv\tau(b)$ for some $a,\,b\in\mathbb{Z}_n$. Then, applying Lemma 5.2 (ix), we obtain the following series of congruencies modulo n:

$$\tau(a)\equiv\tau(b)\quad\Longrightarrow\quad\tau(\overline{a}+l_ak)\equiv\tau(\overline{b}+l_bk)\quad\Longrightarrow\quad\tau(\overline{a})+sl_ak\equiv\tau(\overline{b})+sl_bk.$$

Hence, $\tau(\overline{a})\equiv\tau(\overline{b}) \pmod{k}$, and therefore, $\overline{a}\equiv\overline{b} \pmod{k}$, by Lemma 5.2 (iii). Since $\overline{a},\,\overline{b}\in\{0,\,1,\,\ldots,\,k-1\}$, we have proved $\overline{a}=\overline{b}$. Consequently, $sl_ak\equiv sl_bk$, or equivalently, $sk(l_a-l_b)\equiv 0$. As $n=kd$, $(d,s)=1$ and $l_a,\,l_b\in\{0,\,1,\,\ldots,\,d-1\}$, it follows that $l_a-l_b\equiv 0 \pmod{d}$, and thus, $l_a=l_b$. As we have shown that $\tau(a)\equiv\tau(b)$ implies $a=\overline{a}+l_a\equiv\overline{b}+l_b=b$, τ must be a permutation of $\mathbb{Z}_n$.

Next, we show that the permutation τ is a coset-preserving skew-morphism of $\mathbb{Z}_n$ with the parameter set $\operatorname{Par}\tau=(n;\,k,\,h,\,s,\,e)$.

First, to prove that τ is a skew-morphism, for any given $a\in\mathbb{Z}_n$, we must prove the existence of a positive integer i_a for which $\tau(a+b)\equiv\tau(a)+\tau^{i_a}(b)$, for all $b\in\mathbb{Z}_n$. We prove this by showing that the above equations hold for $i_a=e^a$. To prove the correctness of our choice of i_a, we rely on the following lemma. It states that it is sufficient to verify our claim for the elements $a,b\in\{0,\,1,\,\ldots,\,k-1\}$.

Lemma 5.3 *Let $a,\,b\in\{0,\,1,\,\ldots,\,k-1\}$ and suppose that $\tau(a+b)\equiv\tau(a)+\tau^{e^a}(b)$. Then, $\tau(\overline{a}+\overline{b})\equiv\tau(\overline{a})+\tau^{e^a}(\overline{b})$, for all $\overline{a},\,\overline{b}\in\mathbb{Z}_n$ that satisfy $a\equiv\overline{a} \pmod{k}$ and $b\equiv\overline{b} \pmod{k}$.*

Proof: As $a \equiv \overline{a} \pmod{k}$ and $b \equiv \overline{b} \pmod{k}$, there exist $l_1, l_2 \in \{0, 1, \ldots, d-1\}$ such that $\overline{a} = a + l_1 k$ and $\overline{b} = a + l_1 k$. Thus, to prove the claim, we must show that

$$\tau(a + l_1 k \,+\, b + l_2 k) \equiv \tau(a + l_1 k) + \tau^{e^a}(b + l_2 k). \tag{9}$$

Applying Lemma 5.2 (ix), (v) and (vi) to the left side of (9), we obtain

$$\begin{aligned}\tau(a + l_1 k + b + l_2 k) &\equiv \tau(a + b \,+\, l_1 k + l_2 k) \equiv \tau(a+b) + s l_1 k + s l_2 k \equiv \\ &\equiv \tau(a) + \tau^{e^a}(b) + \tau(l_1 k) + \tau(l_2 k) \equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + \tau^{e^a}(l_2 k).\end{aligned}$$

On the other hand, repeated applications of Lemma 5.2 (ix) to the right side of (9) yield

$$\begin{aligned}\tau(a + l_1 k) + \tau^{e^a}(b + l_2 k) &\equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + s^{e^a} \cdot l_2 k \equiv \\ &\equiv \tau(a) + \tau(l_1 k) + \tau^{e^a}(b) + \tau^{e^a}(l_2 k),\end{aligned}$$

which completes the proof of our claim. □

Using induction on b, we proceed to verify for each $b \in \{1, \ldots, k-1\}$ that $\tau(1+b) \equiv \tau(1) + \tau^{e}(b)$, and also that

$$\tau^{i}(b) \equiv \tau^{i}(1) + \tau^{ie}(1) + \cdots + \tau^{ie^{b-1}}(1), \tag{10}$$

for any positive integer i.

Both claims clearly hold for $b = 1$ as $\tau(1+1) = \tau(1) + \tau^{e}(1)$ by formula (8), while the left side of (10) is identical to the right side for all $i \geq 1$. Now suppose that both claims hold for all $b < a$. Then by Lemma 5.3, $\tau(c + \overline{b}) \equiv \tau(c) + \tau^{e}(\overline{b})$ for all $c \in \mathbb{Z}_n$, $c \equiv 1 \pmod{k}$, and $\overline{b} \in \mathbb{Z}_n$, for which there exists a $b \in \{1, \ldots, a-1\}$ such that $\overline{b} \equiv b \mod k$. In particular,

$$\tau(\tau^{j_1}(1) + \tau^{j_2}(b)) \equiv \tau(\tau^{j_1}(1)) + \tau^{e}(\tau^{j_2}(b)) \equiv \tau^{1+j_1}(1) + \tau^{e+j_2}(b),$$

for any pair of positive integers j_1 and j_2 due to Lemma 5.2 (iii). Applying this observation allows us to compute $\tau^{i}(a)$ for an arbitrary integer i as follows:

$$\begin{aligned}\tau^{i}(a) &\equiv \tau^{i-1}\left(\tau(1 + (a-1))\right) \equiv \tau^{i-1}\left(\tau(1) + \tau^{e}(a-1)\right) \equiv \\ &\equiv \tau^{i-2}\left(\tau(\tau(1) + \tau^{e}(a-1))\right) \equiv \tau^{i-2}\left(\tau^{2}(1) + \tau^{2e}(a-1)\right) \equiv \\ &\qquad\vdots \\ &\equiv \tau\left(\tau^{i-1}(1) + \tau^{(i-1)e}(a-1)\right) \equiv \tau^{i}(1) + \tau^{ie}(a-1) \equiv \\ &\equiv \tau^{i}(1) + \tau^{ie}(1) + \cdots + \tau^{ie^{a-1}}(1).\end{aligned}$$

The last congruence holds as $a - 1 < a$, and thus,

$$\tau^{ie}(a-1) \equiv \tau^{ie}(1) + \cdots + \tau^{ie^{a-1}}(1)$$

by the induction assumption. Thus, (10) holds for a as well. To prove that $\tau(1+a) \equiv \tau(1) + \tau^e(a)$, we calculate the right side using (10) with a substituted for b and e substituted for i:

$$\tau(1) + \tau^e(a) \equiv \tau(1) + \tau^e(1) + \tau^{e^2}(1) + \cdots + \tau^{e^a}(1) \equiv \tau(1+a).$$

This concludes our proof by induction of the identities $\tau(1+b) = \tau(1) + \tau^e(b)$ and (10), for all b and $i \geq 1$. We proceed to show that the equation

$$\tau(a+b) \equiv \tau(a) + \tau^{e^a}(b)$$

holds for each $a, b \in \{0, 1, \ldots, k-1\}$. It clearly holds when $a = 0$ or $b = 0$. Thus, suppose that neither a nor b are equal to zero. Then, substituting $i = e^a$ into formula (10), we obtain

$$\tau(a) + \tau^{e^a}(b) \equiv \Big(\tau(1) + \cdots + \tau^{e^{a-1}}(1)\Big) + \Big(\tau^{e^a}(1) + \cdots + \tau^{e^{a+b-1}}(1)\Big) \equiv \tau(a+b),$$

which proves our claim.

Combining this result with Lemma 5.3, we have proved that τ is a skew-morphism of $\mathbb{Z}_n$ with $i_a = e^a$ for each $a \in \mathbb{Z}_n$. As τ is a skew-morphism of an abelian group and the orbit of element 1 is generating, we have $|\tau| = |\mathcal{O}_1| = r$. Let π denote the power function of the skew-morphism τ. Then $\pi(a)$ equals $e^a \pmod r$ for each $a \in \mathbb{Z}_n$ (note that $e^{a \pmod k} \equiv e^a \pmod r$ by Condition (iv)). Summing up all these, we obtain the first claim of the following lemma.

Lemma 5.4 *Let $(n;\, k,\, h,\, s,\, e)$ be a set of admissible parameters, let r be the integer defined in the previous subsection, and let τ be the permutation of Z_n defined by $\tau(0) = 0$ and formulas (7) and (8). Then the following hold:*

(i) *The permutation τ is a skew-morphism of $\mathbb{Z}_n$ with the power function $\pi(a) = e^a \pmod r$, $a \in \mathbb{Z}_n$;*

(ii) *τ is a coset-preserving skew-morphism;*

(iii) *$\operatorname{Par}\tau = (n;\, k,\, h,\, s,\, e)$.*

Proof: The skew-morphism τ satisfies $\tau(a) \equiv a \pmod k$ for each $a \in \mathbb{Z}_n$ by Lemma 5.2 (iii). Thus, the values e^a and $e^{\tau(a)}$ are equal modulo r because $e^k \equiv 1 \pmod r$ by Condition (v). It follows that τ is a coset-preserving skew-morphism of $\mathbb{Z}_n$. It remains to show that $\operatorname{Par}\tau = (n;\, k,\, h,\, s,\, e)$.

As τ is defined on $\mathbb{Z}_n$, its first parameter obviously equals n. It is also straightforward to see that $\tau(1) - 1 = 1 + h - 1 = h$, and hence the third parameter of τ equals h.

To verify that the fourth parameter equals s, we must prove that s is the smallest positive integer such that $\tau(k) \equiv sk$. Number s satisfies the equation due to Lemma 5.2 (v). Suppose that $\tau(k) \equiv \overline{s}k$ for some positive integer $\overline{s} \leq s$. We obtain

$$sk \equiv \overline{s}k \implies s \equiv \overline{s} \pmod d,$$

and hence $s = \overline{s}$ as $s < d$ by Condition (iii).

The fifth parameter $\pi(1)$ equals $e \pmod{r}$. As $e < r$ by Condition (v), we obtain $\pi(1) = e$.

Finally, recall that the order of $\pi(1) = e$ modulo $|\tau| = r$ equals k by Condition (v). Hence $\pi(a) = (e^a \pmod{r}) \neq 1$ for all non-zero elements $a \in \mathbb{Z}_n$ smaller than k and $\pi(k) = (e^k \pmod{r}) = 1$. Thus k is the smallest non-zero element of $\ker \pi$, i.e., the second parameter of τ. □

The following classification theorem is the main result of our paper.

Theorem 5.5 (1) *Let* $(n;\, k,\, h,\, s,\, e)$ *be a set of admissible parameters. Then there exists a unique non-trivial coset-preserving skew-morphism* τ *of the cyclic group* $\mathbb{Z}_n$ *such that* $\operatorname{Par}\tau = (n;\, k,\, h,\, s,\, e)$.

(2) *Let* φ *be a non-trivial coset-preserving skew-morphism of a cyclic group* $\mathbb{Z}_n$. *Then* $\operatorname{Par}\varphi$ *is a set of admissible parameters.*

Let us point out that by restricting the above theorem to five-tuples consisting of an even n and $k = 2$, we have also obtained a classification of t-balanced skew-morphisms of cyclic groups. A different version of a classification of the t-balanced skew-morphisms of cyclic groups that give rise to a regular Cayley map (i.e., admit a generating orbit closed under inverses) was obtained in [15].

In view of Theorem 5.5, for any positive integer n, there is a one-to-one correspondence between the set of admissible parameter five-tuples $(n;\, k,\, h,\, s,\, e)$ and the set of coset-preserving skew-morphisms of $\mathbb{Z}_n$. It follows obviously from their definition that the three parameters k, h, s are smaller than n. In addition, as shown, in Lemma 4.1, $|\ker \pi| > \sqrt{n}$, and thus $k < \sqrt{n}$, since k is a generator for $\ker \pi$. In [6], it was shown that the order of any skew-morphism φ of a finite group G is smaller than the order of G. Hence, any skew-morphism of $\mathbb{Z}_n$ satisfies $|\varphi| < n$, and since e belongs to $\mathbb{Z}_{|\varphi|}$, $e < n$ as well. It follows that any admissible five-tuple $(n;\, k,\, h,\, s,\, e)$ satisfies the inequalities $k < \sqrt{n}$ and $h, s, e < n$, and finding all admissible five-tuples for a given parameter n requires checking the easy arithmetic Conditions (i) - (vii) for at most $n^{3.5}$ four-tuples $(k,\, h,\, s,\, e)$. Having all admissible parameter sets for a given n, it is also not hard (specifically, polynomial in n) to use formulas (7) and (8) to construct all skew-morphism for $\mathbb{Z}_n$.

Based on these ideas, the first author and M. Hagara created a *C++* program to search the admissible parameter sets up to $n = 2000$, and to create complete lists of coset-preserving skew-morphisms of cyclic groups of order up to 500 (with the lists becoming too big for $n > 500$). The complete list up to the order 500 contains 177753 coset-preserving skew-morphisms out of which 76115 are automorphisms. The cyclic group with the largest number of coset-preserving skew-morphisms up to the order 500 is the group $\mathbb{Z}_{480}$ which admits 2144 coset-preserving skew-morphisms.

We conclude our paper with two examples of the use of the above techniques for constructing coset-preserving skew-morphisms. In the first example, we demonstrate the construction of a coset-preserving skew-morphism for the given admissible parameter set. In the second example, we present a classification of coset-preserving skew-morphisms for the cyclic group $\mathbb{Z}_{18}$.

Example 5.6 Consider the parameter set $(n;\, k,\, h,\, s,\, e) = (20;\, 4,\, 8,\, 1,\, 3)$. It is easy to verify that this parameter set satisfies all the conditions of Theorem 4.3, and thus, (20; 4, 8, 1, 3) is an admissible parameter set. As the first parameter equals 20, we will be building a coset-preserving skew-morphisms φ of $\mathbb{Z}_{20}$ (and thus all the congruences without a specified modulus will be meant $\pmod{20}$).

1. Let $\varphi(0) \equiv 0$.
2. Using (7), define

   $$\varphi^i(1) \equiv 1 + 1^0 \cdot 8 + 1^1 \cdot 8 + \cdots + 1^{i-1} \cdot 8 \equiv (1 + 8i),$$

   for each positive integer i. Since the smallest positive integer r such that $1 + 8r \equiv 1$ equals 5, we obtain the orbit of 1 under φ of length 5:

   $$\varphi(1) \equiv 9,\ \ \varphi^2(1) \equiv 17,\ \ \varphi^3(1) \equiv 5,\ \ \varphi^4(1) \equiv 13,\ \ \varphi^5(1) \equiv 1.$$

3. The remaining values $\varphi(a)$, for $a \in \mathbb{Z}_{20}$, $a \neq 0, 1, 9, 17, 5, 13$, can be computed using formula (8), i.e.,

   $$\varphi(a) \equiv \varphi(1) + \varphi^3(1) + \varphi^{3^2}(1) + \cdots + \varphi^{3^{a-1}}(1).$$

   An even simpler method follows from Lemma 5.2 (ix), which asserts that $\varphi(a + lk) \equiv \varphi(a) + slk$ for all non-negative integers a and positive integers l. Since, in our case, $k = 4$ and $s = 1$, Lemma 5.2 (ix) yields $\varphi(a + 4l) \equiv \varphi(a) + 4l$. Thus, to determine the rest of φ, it suffices to find the values $\varphi(0)$, $\varphi(1)$, $\varphi(2)$ and $\varphi(3)$. We already know that $\varphi(0) \equiv 0$ and $\varphi(1) \equiv 1$. Using the above formula based on (8), we obtain the values $\varphi(2)$ and $\varphi(3)$:

   $$\varphi(2) \equiv \varphi(1) + \varphi^3(1) \equiv 9 + 5 \equiv 14,$$
   $$\varphi(3) \equiv \varphi(1) + \varphi^3(1) + \varphi^9(1) \equiv \varphi(1) + \varphi^3(1) + \varphi^4(1) \equiv 9 + 5 + 13 \equiv 7,$$

   (where the powers in the exponents of φ are calculated modulo 5, which is the length of the orbit $\mathcal{O}_1$, while the 'base' calculations are performed modulo $n = 20$, the order of the group).

   Using $\varphi(a + 4l) \equiv \varphi(a) + 4l$ for $a = 1, 2, 3$ and $l = 1, 2, 3, 4$, we obtain $(1, 9, 17, 5, 13)(2, 14, 6, 18, 10)(3, 7, 11, 15, 19)$. Finally, by the definition of the parameters k and s, $\varphi(lk) \equiv slk$, and we obtain

   $$\varphi = (0)(4)(8)(12)(16)(1, 9, 17, 5, 13)(2, 14, 6, 18, 10)(3, 7, 11, 15, 19).$$

The resulting coset-preserving skew-morphism φ of $\mathbb{Z}_{20}$ has the desired parameters $\operatorname{Par}\varphi = (20;\ 4,\ 8,\ 1,\ 3)$. Note that φ is neither an automorphism nor a t-balanced skew-morphism of $\mathbb{Z}_{20}$ as $\ker\pi = \langle 4\rangle$ is of index 4 in $\mathbb{Z}_{20}$, and thus, the power function π assumes 4 distinct values. The group $\mathbb{Z}_{20}$ is the smallest cyclic group which admits a coset-preserving skew-morphism which is neither an automorphism nor t-balanced (see Table 1).

Example 5.7 In our last example, we present the complete list of all coset-preserving skew-morphisms of $\mathbb{Z}_{18}$. All of these have been obtained using the method illustrated in Example 5.6. To simplify the list, we only present power functions for those skew-morphisms which are not automorphisms, and, for those, we only list the value of π for one element of each orbit.

For $n = 18$, there exist 13 admissible parameter sets, which give rise to 13 nontrivial coset-preserving skew-morphisms of $\mathbb{Z}_{18}$. By extending the list by the identity permutation of $\mathbb{Z}_{18}$, we obtain the complete list of coset-preserving skew-morphisms of $\mathbb{Z}_{18}$:

$\varphi_1 = \operatorname{Id}(\mathbb{Z}_{18})$, automorphism of $\mathbb{Z}_{18}$;

$\varphi_2 = (1,5,7,17,13,11)\,(2,10,14,16,8,4)\,(3,15)\,(6,12)$,
automorphism of $\mathbb{Z}_{18}$, $\operatorname{Par}\varphi_2 = (18;\ 1,\ 4,\ 5,\ 1)$;

$\varphi_3 = (1,7,13)\,(2,14,8)\,(4,10,16)\,(5,17,11)$,
automorphism of $\mathbb{Z}_{18}$, $\operatorname{Par}\varphi_3 = (18;\ 1,\ 6,\ 7,\ 1)$;

$\varphi_4 = (1,17)\,(2,16)\,(3,15)\,(4,14)\,(5,13)\,(6,12)\,(7,11)\,(8,10)$,
automorphism of $\mathbb{Z}_{18}$, $\operatorname{Par}\varphi_6 = (18;\ 1,\ 16,\ 17,\ 1)$;

$\varphi_5 = (1,13,7)\,(2,8,14)\,(4,16,10)\,(5,11,17)$,
automorphism of $\mathbb{Z}_{18}$, $\operatorname{Par}\varphi_5 = (18;\ 1,\ 12,\ 13,\ 1)$;

$\varphi_6 = (1,11,13,17,7,5)\,(2,4,8,16,14,10)\,(3,15)\,(6,12)$,
automorphism of $\mathbb{Z}_{18}$, $\operatorname{Par}\varphi_4 = (18;\ 1,\ 10,\ 11,\ 1)$;

$\varphi_7 = (1,3,5,7,9,11,13,15,17)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_7 = (18;\ 2,\ 2,\ 1,\ 8)$;

$\varphi_8 = (1,5,9,13,17,3,7,11,15)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_8 = (18;\ 2,\ 4,\ 1,\ 8)$;

$\varphi_9 = (1, 7, 13)\,(3, 9, 15)\,(5, 11, 17)$,
2-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = \pi(3) = \pi(5) = 2$,
$\operatorname{Par}\varphi_9 = (18;\ 2,\ 6,\ 1,\ 2)$;

$\varphi_{10} = (1, 9, 17, 7, 15, 5, 13, 3, 11)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_{10} = (18;\ 2,\ 8,\ 1,\ 8)$;

$\varphi_{11} = (1, 11, 3, 13, 5, 15, 7, 17, 9)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_{11} = (18;\ 2,\ 10,\ 1,\ 8)$;

$\varphi_{12} = (1, 13, 7)\,(3, 15, 9)\,(5, 17, 11)$,
2-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = \pi(3) = \pi(5) = 2$,
$\operatorname{Par}\varphi_{12} = (18;\ 2,\ 12,\ 1,\ 2)$;

$\varphi_{13} = (1, 15, 11, 7, 3, 17, 13, 9, 5)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_{13} = (18;\ 2,\ 14,\ 1,\ 8)$;

$\varphi_{14} = (1, 17, 15, 13, 11, 9, 7, 5, 3)$,
8-balanced skew-morphism of $\mathbb{Z}_{18}$, $\pi(1) = 8$, $\operatorname{Par}\varphi_{14} = (18;\ 2,\ 16,\ 1,\ 8)$.

Note that the skew-morphisms $\varphi_3, \ldots, \varphi_6$ are successive powers of φ_2, and $\varphi_8, \ldots, \varphi_{14}$ are powers of φ_7. Also observe that the only types of coset-preserving skew-morphisms for $\mathbb{Z}_{18}$ are either automorphisms of $\mathbb{Z}_{18}$ (the powers of φ_2) or t-balanced skew-morphisms with kernel of order 9. Thus, even though Lemma 4.1 appears to allow for coset-preserving skew-morphisms of $\mathbb{Z}_{18}$ with kernel of order $6 > \sqrt{18}$, no such skew-morphisms actually exist. This is due to another important property of coset-preserving skew-morphisms. Namely, if φ were a coset-preserving skew-morphism with kernel of order 6, the size of the coset of 1 would also be equal to 6, and hence the length of the orbit of 1 under φ would be at most 6. Recall also that the order m of φ would have to match the size of the orbit of 1 (a generator for $\mathbb{Z}_{18}$), and that the power function π of φ would be a homomorphism from $\mathbb{Z}_{18}$ into $\mathbb{Z}_m^*$. However, $|\mathbb{Z}_m^*| \leq 2$, for $2 \leq m \leq 6$, $m \neq 5$, and hence the order of φ cannot be $2, 3, 4$ or 6 as we would not have three distinct power function values for the three distinct cosets of the kernel. It cannot be equal to 5 either, as that would require the existence of a homomorphism from $\mathbb{Z}_{18}$ *onto* $\mathbb{Z}_5^*$, but 4 does not divide 18.

All the above skew-morphisms also appear on the list of the skew-morphisms of $\mathbb{Z}_{18}$ maintained by Conder [3]. Next, we list the non-coset-preserving skew-morphisms (equivalently, skew-morphisms with periodicity at least 2) for the sake of completeness, although they are simply lifted from [3]. We also list their periodicities and their corresponding powers that belong to the above list of coset-preserving skew-morphisms. Such powers always exist due to Theorem 3.2.

$\varphi_{15} = (1, 11, 7, 5, 13, 17)\,(2, 16, 14, 4, 8, 10)\,(3, 15)\,(6, 12),\quad p_{\varphi_{15}} = 2,\quad \varphi_{15}^2 = \varphi_3,$

$\varphi_{16} = (1, 17, 7, 11, 13, 5)\,(2, 4, 14, 10, 8, 16)\,(3, 15)\,(6, 12),\quad p_{\varphi_{16}} = 2,\quad \varphi_{16}^2 = \varphi_3,$

$\varphi_{17} = (1, 5, 13, 11, 7, 17)\,(2, 16, 8, 10, 14, 4)\,(3, 15)\,(6, 12),\quad p_{\varphi_{17}} = 2,\quad \varphi_{17}^2 = \varphi_5,$

$\varphi_{18} = (1, 17, 13, 5, 7, 11)\,(2, 10, 8, 4, 14, 16)\,(3, 15)\,(6, 12),\quad p_{\varphi_{18}} = 2,\quad \varphi_{18}^2 = \varphi_5,$

$\varphi_{19} = (1, 9, 5, 7, 15, 11, 13, 3, 17)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{19}} = 3,\quad \varphi_{19}^3 = \varphi_9,$

$\varphi_{20} = (1, 15, 5, 7, 3, 11, 13, 9, 17)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{20}} = 3,\quad \varphi_{20}^3 = \varphi_9,$

$\varphi_{21} = (1, 15, 17, 7, 3, 5, 13, 9, 11)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{21}} = 3,\quad \varphi_{21}^3 = \varphi_9,$

$\varphi_{22} = (1, 3, 17, 7, 9, 5, 13, 15, 11)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{22}} = 3,\quad \varphi_{22}^3 = \varphi_9,$

$\varphi_{23} = (1, 3, 11, 7, 9, 17, 13, 15, 5)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{23}} = 3,\quad \varphi_{23}^3 = \varphi_9$

$\varphi_{24} = (1, 9, 11, 7, 15, 17, 13, 3, 5)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{24}} = 3,\quad \varphi_{24}^3 = \varphi_9,$

$\varphi_{25} = (1, 11, 15, 13, 5, 9, 7, 17, 3)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{25}} = 3,\quad \varphi_{25}^3 = \varphi_{12},$

$\varphi_{26} = (1, 17, 3, 13, 11, 15, 7, 5, 9)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{26}} = 3,\quad \varphi_{26}^3 = \varphi_{12},$

$\varphi_{27} = (1, 17, 9, 13, 11, 3, 7, 5, 15)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{27}} = 3,\quad \varphi_{27}^3 = \varphi_{12},$

$\varphi_{28} = (1, 5, 15, 13, 17, 9, 7, 11, 3)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{28}} = 3,\quad \varphi_{28}^3 = \varphi_{12},$

$\varphi_{29} = (1, 5, 3, 13, 17, 15, 7, 11, 9)\,(2, 14, 8)\,(4, 10, 16),\quad p_{\varphi_{29}} = 3,\quad \varphi_{29}^3 = \varphi_{12},$

$\varphi_{30} = (1, 11, 9, 13, 5, 3, 7, 17, 15)\,(2, 8, 14)\,(4, 16, 10),\quad p_{\varphi_{30}} = 3,\quad \varphi_{30}^3 = \varphi_{12}.$

Acknowledgments

The first author acknowledges support from the project VEGA 1/0007/14, and the second author acknowledges support from VEGA 1/0577/14, VEGA 1/0474/15, NSFC 11371307, and by the Slovenian Research Agency research project J1-6720.

References

[1] M. Bachratý, *Powers of skew-morphisms*, Bachelor thesis, Comenius University, 2013.

[2] M. Bachratý and R. Jajcay, Powers of skew-morphisms, in: *Symmetries in Graphs, Maps, and Polytopes*, 5th SIGMAP Workshop, West Malvern, UK,

July 2014 (J. Širáň and R. Jajcay, eds.), Springer Proceedings in Mathematics & Statistics 159 (2016), 1–26.

[3] M. Conder, List of skew-morphisms for small cyclic groups, University of Auckland, `https://www.math.auckland.ac.nz/∼conder/SkewMorphisms-SmallCyclicGroups-60.txt`

[4] M. Conder, R. Jajcay and T. Tucker, Regular t-balanced Cayley maps, *J. Combin. Theory Ser. B* 97 (3) (2007), 453–473.

[5] M. Conder, R. Jajcay and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebr. Combin.* 25 No. 3 (2007), 259–283.

[6] M. Conder, R. Jajcay and T. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* 453 (2016), 68–100.

[7] R. Feng, R. Jajcay and Y. Wang, Regular t-balanced Cayley maps for abelian groups, *Discrete Math.* 311 (21) (2011), 2309–2316.

[8] R. Jajcay, Automorphism groups of Cayley maps, *J. Combin. Theory Ser. B* 59 (1993), 297–310.

[9] R. Jajcay and R. Nedela, Half-regular Cayley maps, *Graphs Combin.* 31 (2015), 1003–1018.

[10] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* 244 (1-3) (2002), 167–179.

[11] I. Kovács, D. Marušič and M. Muzychuk, On G-arc-regular dihedrants and regular dihedral maps, *J Algebr. Combin.* 38 (2013), 437–455.

[12] I. Kovács, D. Marušič and M. Muzychuk, On dihedrants admitting arc-regular group actions, *J. Algebr. Combin.* 33 (2011), 409–426.

[13] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars. Math. Contemp.* (4) (2011), 329–349.

[14] I. Kovács and R. Nedela, Skew-morphisms of cyclic p-groups, (submitted).

[15] Y.S. Kwon, A classification of regular t-balanced Cayley maps for cyclic groups, *Discrete Math.* 313 (2013), 656–664.

[16] Ľ. Lišková, M. Mačaj and M. Škoviera, Regular maps from Cayley graphs, *Discrete Math.* 307 no. 3-5 (2007), 517–533.

[17] R.B. Richter, J. Širáň, R. Jajcay, T.W. Tucker and M.E. Watkins, Cayley maps, *J. Combin. Theory Ser. B* 95 (2) (2005), 189–245.

[18] J. Širáň and M. Škoviera, Groups with sign structure and their antiautomorphisms, *Discrete Math.* 108 (1992), 189–202.

[19] M. Škoviera and J. Širáň, Regular maps from Cayley graphs I: balanced Cayley maps, *Discrete Math.* 109 (1992), 265–276.

[20] J. Širáň and M. Škoviera, Regular maps from Cayley graphs II: antibalanced Cayley maps, *Discrete Math.* 124 (1994), 179–191.

[21] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for dihedral groups, *Discrete Math.* 338 (2015), 1163–1172.

[22] J.-Y. Zhang, A classification of regular Cayley maps with trivial Cayley-core for dihedral groups, *Discrete Math.* 338 (2015), 1216–1225.

[23] J.-Y. Zhang and S.-F. Du, On the skew-morphisms of dihedral groups, (submitted).

(Received 22 Jan 2016; revised 7 Aug 2016)