Chapter 2

# Preparations

In this chapter, we prove some auxiliary results that are used when discussing the details of our algorithm in Chapter 3.

## 2.1 Functional graphs of affine maps of finite groups

In this section, we derive some results on functional graphs of affine maps $A: x \mapsto ax + b$ of finite cyclic groups $\mathbb{Z}/m\mathbb{Z}$. We note that these graphs were studied earlier by Deng [21], and we use several of Deng's results and ideas here, as pointed out where appropriate. However, for the reader's convenience, we aim to keep our exposition self-contained. We also observe (at the end of the section) that these results can in fact be generalized to arbitrary finite groups. First, we consider the following concept.

**Definition 2.1.1.** Let $(\Gamma_j)_{j\in I}$ be a family of digraphs. Their *tensor product*, written $\bigotimes_{j\in I}\Gamma_j$, is the digraph with vertex set $\prod_{j\in I}\mathrm{V}(\Gamma_j)$ having an arc $(y_j)_{j\in I}\to(z_j)_{j\in I}$ if and only if for each $j\in I$, there is an arc $y_j\to z_j$ in $\Gamma_j$.

This concept corresponds to Deng's product graph from [21, formula (1) in Section 2].

**Remark 2.1.2.** If $(g_j)_{j\in I}$ is a family of functions $g_j: X_j\to X_j$, and if $\bigotimes_{j\in I} g_j$ denotes the function

$$\prod_{j\in I} X_j \to \prod_{j\in I} X_j, \quad (y_j)_{j\in I}\mapsto (g_j(y_j))_{j\in I},$$

then

$$\Gamma_{\bigotimes_{j\in I} g_j} = \bigotimes_{j\in I}\Gamma_{g_j}.$$

Due to Remark 2.1.2, the tensor product of digraphs is a useful tool when studying functional graphs of affine maps (in particular of endomorphisms) of finite cyclic groups $\mathbb{Z}/m\mathbb{Z}$. Indeed, if we factor $m = p_1^{v_1}\cdots p_K^{v_K}$, then for each given affine map $A: x\mapsto ax+b$ of $\mathbb{Z}/m\mathbb{Z}$ and each $j\in\{1,2,\ldots,K\}$, we may consider the reduction $A_j$ of $A$ modulo $p_j^{v_j}$, which is the affine map $A_j: x\mapsto ax+b$ of $\mathbb{Z}/p_j^{v_j}\mathbb{Z}$. By the Chinese remainder theorem, $\mathbb{Z}/m\mathbb{Z}$ is in a natural isomorphism with $\prod_{j=1}^K \mathbb{Z}/p_j^{v_j}\mathbb{Z}$, and under this isomorphism, $A$ corresponds to $\bigotimes_{j=1}^K A_j$. Hence we obtain the following, which is [21, Theorem 2].

**Lemma 2.1.3.** *Let $m = p_1^{v_1} \cdots p_K^{v_K}$ be a positive integer with displayed factorization into pairwise coprime prime powers. Let $A : x \mapsto ax + b$ be an affine map of $\mathbb{Z}/m\mathbb{Z}$, and denote by $A_j$ the reduction of $A$ modulo $p_j^{v_j}$ for $j = 1, 2, \ldots, K$. Then $\Gamma_A \cong \bigotimes_{j=1}^{K} \Gamma_{A_j}$.*

Lemma 2.1.3 allows us to reduce many arguments concerning functional graphs of affine maps of $\mathbb{Z}/m\mathbb{Z}$ to the case where $m = p^v$ is a prime power. We note the following interesting dichotomy (see also [21, Lemma 3]).

**Proposition 2.1.4.** *Let $m = p^v$ be a prime power, and let $A : x \mapsto ax + b$ be an affine map of $\mathbb{Z}/m\mathbb{Z}$.*

(1) *If $p \mid a$, then $A$ has exactly one periodic point $x$ (a fixed point necessarily), and $\Gamma_A$ is obtained from* $\mathrm{Tree}_{\Gamma_A}(x)$ *by adding a loop to the root $x$.*

(2) *If $p \nmid a$, then $A$ is a permutation of $\mathbb{Z}/m\mathbb{Z}$, whence $\Gamma_A$ is a disjoint union of directed cycles.*

We would like to use these reduction ideas to prove the following theorem.

**Theorem 2.1.5.** *Let $A : x \mapsto ax + b$ be an affine map of the finite cyclic group $\mathbb{Z}/m\mathbb{Z}$. Then all trees above periodic vertices in $\Gamma_A$ are isomorphic to each other. In fact, they are all isomorphic to any tree above a periodic vertex in $\Gamma_{\mu_a}$, where $\mu_a$ is the endomorphism $x \mapsto ax$ of $\mathbb{Z}/m\mathbb{Z}$.*

We note that it was proved by Sha [66, Corollary 3.4] that all trees above periodic vertices in $\Gamma_{\mu_a}$ are isomorphic to each other. The statement of Theorem 2.1.5 itself is implicit in Deng's proof of [21, Theorem 11].

Using Proposition 2.1.4, we can derive the following partial result swiftly, in the proof of which we use the notation

$$\nu_p^{(v)}(n) := \min\{v, \nu_p(n)\},$$

where $\nu_p(n)$ is the *$p$-adic valuation of $n$*, i.e., the exponent of $p$ in the prime power factorization of the integer $n$, defined to be $\infty$ if $n = 0$.

**Lemma 2.1.6.** *Theorem 2.1.5 holds when $m = p^v$ is a prime power.*

*Proof.* By [21, Lemma 4], if $\nu_p^{(v)}(a-1) \leq \nu_p^{(v)}(b)$, then $A$ has a fixed point, which leads to a digraph isomorphism between $\Gamma_A$ and $\Gamma_{\mu_a}$ (cf. also our Lemma 2.3.3). The result is thus clear by [66, Corollary 3.4].

On the other hand, if $\nu_p^{(v)}(b) < \nu_p^{(v)}(a-1)$, then $a \equiv 1 \pmod{p}$, which implies that $p \nmid a$. Therefore, by Proposition 2.1.4 (2), all rooted trees above periodic vertices in $\Gamma_A$ are trivial (i.e., they are isomorphic to a single vertex without arcs), and so are those trees in $\Gamma_{\mu_a}$, as required. ∎

Of course, we could now derive Theorem 2.1.5 in its full strength by observing that the property “all rooted trees above periodic vertices are isomorphic” is preserved under taking tensor products of functional graphs. We can, however, obtain an even more detailed result with some extra work, which we carry out. This requires some concepts and results from the first author’s paper [13], in which the structure of the trees above periodic vertices in functional graphs of finite group endomorphisms was characterized (thus extending Sha’s result [66, Corollary 3.4]).

**Definition 2.1.7.** Let $\Gamma = (V, E)$ be a finite digraph, and let $x \in V$.

(1) The *dual digraph* $\Gamma^*$ is obtained from $\Gamma$ by inverting each arc; formally, $\Gamma^* = (V, E^{-1})$, where $E^{-1} = \{(y,z) \in V^2 : (z,y) \in E\}$ is the inverse relation of $E$.

(2) A vertex $y \in V$ such that $\Gamma$ has an edge $x \to y$ is a *successor* or *child of* $x$.

(3) For each $k \in \mathbb{N}^+$, the *$k$-th procreation number of* $x$, written $\mathrm{proc}_k(x) = \mathrm{proc}_k^{(\Gamma)}(x)$, is the number of children $y$ of $x$ such that there is a length $k-1$ directed path $(w_1, w_2, \ldots, w_k)$ in $\Gamma$ with $w_1 = y$ (in this situation, we also say that $y$ *has (at least)* $k-1$ *successor generations*).

(4) We say that $\Gamma$ has *rigid procreation* if for all $y, z \in V$ and all positive integers $k$ with $\mathrm{proc}_k(y), \mathrm{proc}_k(z) > 0$, one has $\mathrm{proc}_k(y) = \mathrm{proc}_k(z)$.

Using the notation of Definition 2.1.7, we note that $\mathrm{proc}_1(x)$ is simply the number of all children of $x$ (i.e., the out-degree of $x$), that $\mathrm{proc}_2(x)$ is the number of children of $x$ that have children themselves, etc. Rigid procreation means that all vertices with children must have the same number of children (though it is fine for vertices without children to exist), that all vertices with at least one “grandchild” must have the same number of children that have a child (in particular the same number of grandchildren), etc. The following fact was noted but not proved in [13, Remark before Theorem 3], and we prove it here (after the proof of Lemma 2.1.10) for the reader’s convenience.

**Proposition 2.1.8.** *Let $\Gamma$ be a finite digraph that is a functional graph (i.e., all vertices of $\Gamma$ have out-degree* 1*), say $\Gamma = \Gamma_g$. If the dual digraph $\Gamma^*$ has rigid procreation, then for any two $g$-periodic vertices $x$ and $y$, we have* $\mathrm{Tree}_\Gamma(x) \cong \mathrm{Tree}_\Gamma(y)$. *Moreover, the common rooted tree isomorphism type above periodic vertices $x$ in $\Gamma$ is determined by the procreation number sequence* $(\mathrm{proc}_k(x))_{k\geq 1}$ *alone (i.e., it is the same in any finite functional graph with rigid procreation and the same procreation number sequence of periodic vertices).*

Readers interested in how the isomorphism type of $\mathrm{Tree}_\Gamma(x)$ can be derived from $(\mathrm{proc}_k(x))_{k\geq 1}$ for periodic vertices $x$ if $\Gamma^*$ has rigid procreation can find the details of this in Section 4.1. Before proving Proposition 2.1.8, we extend the notation $\mathrm{Tree}_\Gamma(x)$, which was already defined for finite functional graphs $\Gamma$ in Chapter 1, to the case where $\Gamma$ is a finite directed rooted tree $\Delta$ (with all arcs oriented toward the root) and prove a lemma.

**Definition 2.1.9.** Let $\Delta$ be a finite directed rooted tree, with root $\mathrm{rt}(\Delta)$. We observe that all vertices except $\mathrm{rt}(\Delta)$ have out-degree 1, and we let $g$ be the unique function $\mathrm{V}(\Delta) \setminus \{\mathrm{rt}(\Delta)\} \to \mathrm{V}(\Delta)$ such that $\Delta$ has an arc $x \to g(x)$ for each vertex $x \neq \mathrm{rt}(\Delta)$. For each $x \in \mathrm{V}(\Delta)$, we define $\mathrm{Tree}_\Delta(x)$, the so-called *tree above $x$ in $\Delta$*, as the induced subgraph of $\Delta$ on the set

$$\{x\} \cup \{y \in \mathrm{V}(\Delta) : y \neq x, \text{and } g^k(y) = x \text{ for some } k = k(y) \geq 1\}.$$

In the statement of the following lemma and beyond, we denote the height of a finite directed rooted tree $\Delta$ by $\mathrm{ht}(\Delta)$.

**Lemma 2.1.10.** *Let $\Delta_1$ and $\Delta_2$ be finite directed rooted trees. Moreover, we assume that $\Delta_1$ and $\Delta_2$ have the same height, that the dual digraphs $\Delta_1^*$ and $\Delta_2^*$ both have rigid procreation, and that* $\mathrm{proc}_h^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)) = \mathrm{proc}_h^{(\Delta_2^*)}(\mathrm{rt}(\Delta_2))$ *for* $1 \leq h \leq \mathrm{ht}(\Delta_1) = \mathrm{ht}(\Delta_2)$. *Then $\Delta_1$ and $\Delta_2$ are isomorphic.*

*Proof.* We proceed by induction on the common height of $\Delta_1$ and $\Delta_2$. If $\mathrm{ht}(\Delta_1)=0$, then both $\Delta_1$ and $\Delta_2$ consist of a single vertex without any arcs and thus are isomorphic. Now we assume that $\mathrm{ht}(\Delta_1) \geq 1$ and that the statement holds for all smaller heights. We note that $\Delta_1$ and $\Delta_2$ are isomorphic if and only if the following equality of multisets holds, where $[\Gamma]_\cong$ denotes the isomorphism type of the finite digraph $\Gamma$:

$$\begin{aligned} &\{[\mathrm{Tree}_{\Delta_1}(y_1)]_\cong : y_1 \text{ is a child of } \mathrm{rt}(\Delta_1) \text{ in } \Delta_1^*\} \\ &\quad = \{[\mathrm{Tree}_{\Delta_2}(y_2)]_\cong : y_2 \text{ is a child of } \mathrm{rt}(\Delta_2) \text{ in } \Delta_2^*\}. \end{aligned} \tag{2.1}$$

It is thus our goal to prove equality (2.1). Let us fix $h \in \{0, 1, 2, \ldots, \mathrm{ht}(\Delta_1) - 1\}$. The number of children $y_1$ of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$ such that $\mathrm{Tree}_{\Delta_1}(y_1)$ has height exactly $h$ is

$$\mathrm{proc}_{h+1}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)) - \mathrm{proc}_{h+2}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)).$$

As for children $y_2$ of $\mathrm{rt}(\Delta_2)$ in $\Delta_2^*$ such that $\mathrm{Tree}_{\Delta_2}(y_2)$ has height exactly $h$, one finds analogously that their number is

$$\mathrm{proc}_{h+1}^{(\Delta_2^*)}(\mathrm{rt}(\Delta_2)) - \mathrm{proc}_{h+2}^{(\Delta_2^*)}(\mathrm{rt}(\Delta_2)) = \mathrm{proc}_{h+1}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)) - \mathrm{proc}_{h+2}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)).$$

Moreover, for each child $y_1$ of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$ such that $\mathrm{Tree}_{\Delta_1}(y_1)$ has height exactly $h$, the first $h$ procreation numbers of $y_1$ in $(\mathrm{Tree}_{\Delta_1}(y_1))^*$ are the same as those of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$, since $\Delta_1^*$ has rigid procreation. In particular, by the induction hypothesis and for fixed $h$, all digraphs $\mathrm{Tree}_{\Delta_1}(y_1)$, where $y_1$ is a child of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$ with exactly $h$ successor generations in $\Delta_1^*$ are isomorphic, their isomorphism type $\mathfrak{T}_h^{(1)}$ being determined by the first $h$ procreation numbers of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$. An analogous statement holds with $\Delta_2$ and $\mathrm{rt}(\Delta_2)$ in place of $\Delta_1$ and $\mathrm{rt}(\Delta_1)$, say with isomorphism type $\mathfrak{I}_h^{(2)}$. But by assumption, the procreation numbers of $\mathrm{rt}(\Delta_1)$ in $\Delta_1^*$ and of $\mathrm{rt}(\Delta_2)$ in $\Delta_2^*$ are the same, whence $\mathfrak{I}_h^{(1)} = \mathfrak{I}_h^{(2)}$ for each $h$. This shows that the two multisets in formula (2.1) are the same, each consisting of exactly $\mathrm{proc}_{h+1}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1)) - \mathrm{proc}_{h+2}^{(\Delta_1^*)}(\mathrm{rt}(\Delta_1))$ copies of $\mathfrak{I}_h^{(1)}$ for each $h = 0, 1, \ldots, \mathrm{ht}(\Delta_1) - 1$. ■

*Proof of Proposition* 2.1.8. First of all, in order for the assertion to make sense, we observe that the sequence $(\mathrm{proc}_k^{(\Gamma^*)}(x))_{k\geq 1}$ does not depend on the choice of periodic vertex $x$. Indeed, if $y$ is another periodic vertex, then it is possible to form arbitrarily long directed paths in $\Gamma^*$ starting at either of $x$ or $y$ by going along the respective cycle. This implies that $\mathrm{proc}_k^{(\Gamma^*)}(x), \mathrm{proc}_k^{(\Gamma^*)}(y) > 0$ for each $k$, and thus $\mathrm{proc}_k^{(\Gamma^*)}(x) = \mathrm{proc}_k^{(\Gamma^*)}(y)$ since $\Gamma^*$ has rigid procreation.

Let us write $\Gamma = \Gamma_g$ for a suitably chosen function $g : \mathrm{V}(\Gamma) \to \mathrm{V}(\Gamma)$, and fix a $g$-periodic vertex $x$. We note that $\mathrm{Tree}_\Gamma(y) = \mathrm{Tree}_{\mathrm{Tree}_\Gamma(x)}(y)$ for each $y \in \mathrm{V}(\mathrm{Tree}_\Gamma(x))$. We observe that

$$\mathrm{proc}_k^{(\mathrm{Tree}_\Gamma(x)^*)}(x) = \mathrm{proc}_k^{(\Gamma^*)}(x) - 1$$

for each $k \geq 1$; this is because exactly one of the children of $x$ counted by $\mathrm{proc}_k^{(\Gamma^*)}(x)$ is periodic and hence must be ignored in the procreation number in $\mathrm{Tree}_\Gamma(x)^*$. In particular, for each $h \geq 0$, the number of children $y$ of $x$ in $\mathrm{Tree}_\Gamma(x)^*$ such that $\mathrm{Tree}_\Gamma(y)$ has height exactly $h$ is

$$\mathrm{proc}_{h+1}^{(\mathrm{Tree}_\Gamma(x)^*)}(x) - \mathrm{proc}_{h+2}^{(\mathrm{Tree}_\Gamma(x)^*)}(x) = \mathrm{proc}_{h+1}^{(\Gamma^*)}(x) - \mathrm{proc}_{h+2}^{(\Gamma^*)}(x).$$

Moreover, for each child $y$ of $x$ in $\mathrm{Tree}_\Gamma(x)^*$, the fact that $\Gamma^*$ has rigid procreation implies that $\mathrm{Tree}_\Gamma(y)^*$ has rigid procreation, and, more specifically, whenever $\mathrm{proc}_k^{(\mathrm{Tree}_\Gamma(y)^*)}(z) > 0$ for some $z \in \mathrm{V}(\mathrm{Tree}_\Gamma(y))$, one has $\mathrm{proc}_k^{(\mathrm{Tree}_\Gamma(y)^*)}(z) = \mathrm{proc}_k^{\Gamma^*}(z) = \mathrm{proc}_k^{\Gamma^*}(x)$. Lemma 2.1.10 thus implies that the multiset of isomorphism types

$$\{[\mathrm{Tree}_\Gamma(y)]_{\cong} : g(y) = x, y \text{ is } g\text{-transient}\},$$

which determines the isomorphism type of $\mathrm{Tree}_\Gamma(x)$, is in turn entirely determined by the procreation number sequence $(\mathrm{proc}_k^{(\Gamma^*)}(x))_{k\geq 1}$, which is what we needed to prove. ■

In view of Proposition 2.1.8, the following result, which is [13, Theorem 2], both implies that the rooted trees above periodic vertices in $\Gamma_{\mu_a}$, the functional graph of the endomorphism $x \mapsto ax$ of $\mathbb{Z}/m\mathbb{Z}$, are pairwise isomorphic, and characterizes the corresponding rooted tree isomorphism type.

**Theorem 2.1.11.** *Let $m$ be a positive integer, and let $\mu_a : x \mapsto ax$, be an endomorphism of the cyclic group $\mathbb{Z}/m\mathbb{Z}$. The dual functional graph $(\Gamma_{\mu_a})^*$ has rigid procreation, and for each $k \in \mathbb{N}^+$ and each periodic vertex $x$ of $\Gamma_{\mu_a}$, one has* $\mathrm{proc}_k(x) = |\ker^{(k)}(\mu_a) : \ker^{(k-1)}(\mu_a)|$, *where* $\ker^{(j)}(\mu_a) := \{y \in \mathbb{Z}/m\mathbb{Z} : (\mu_a)^j(y) = a^j y = 0\}$.

Recall that our goal is to understand the functional graphs of affine maps $A : x \mapsto ax + b$ of finite cyclic groups in general. Understanding that for $b = 0$, the graph has rigid procreation with known procreation numbers may only seem like a small special case. However, as we will see, both the rigid procreation behavior and the procreation numbers are preserved when passing to a general $b$ (see Theorem 2.1.13). In fact, this is not even just a special property of finite cyclic groups but holds true for all finite groups (with a suitable definition of "affine map" – see Theorem 2.1.21 at the end of this section).

In view of Theorem 2.1.11, Theorem 2.1.5 is clear once we have proved the following result, which allows us more generally to derive the isomorphism type of $\Gamma_A$ from the isomorphism types of the functional graphs $\Gamma_{A_j}$ of the reductions of $A$ modulo the prime power factors $p_j^{v_j}$ of $m$.

**Proposition 2.1.12.** *Let $g_j : X_j \to X_j$ for $j = 1, 2$ be functions on finite sets.*

(1) *We have* $\mathrm{per}(g_1 \otimes g_2) = \mathrm{per}(g_1) \times \mathrm{per}(g_2)$. *In particular, if $g_1$ and $g_2$ each have precisely one periodic point, then so does $g_1 \otimes g_2$.*

(2) *We assume that the dual functional graphs $\Gamma^*_{g_1}$ and $\Gamma^*_{g_2}$ have rigid procreation. Then the dual functional graph*

$$\Gamma^*_{g_1 \otimes g_2} \cong (\Gamma_{g_1} \otimes \Gamma_{g_2})^* = (\Gamma_{g_1})^* \otimes (\Gamma_{g_2})^*$$

*has rigid procreation, and if $y_j$ is a periodic point of $g_j$ for $j = 1, 2$, then $\vec{y} = (y_1, y_2)$ is a periodic point of $g_1 \otimes g_2$ and* $\mathrm{proc}_k(\vec{y}) = \mathrm{proc}_k(y_1) \cdot \mathrm{proc}_k(y_2)$.

(3) *Let us denote by $\circledast$ the unique $\mathbb{Q}$-bilinear product of polynomials in $\mathbb{Q}[x_n : n \in \mathbb{N}^+]$ such that*

$$(x_1^{e_1} \cdots x_N^{e_N}) \circledast (x_1^{e'_1} \cdots x_{N'}^{e'_{N'}}) = \prod_{1 \leq n \leq N, 1 \leq n' \leq N'} x_n^{e_n} \circledast x_{n'}^{e_{n'}}$$

*and*

$$x_n^e \circledast x_{n'}^{e'} = x_{\mathrm{lcm}(n,n')}^{ee' \gcd(n,n')}.$$

*We assume that each $g_j$ is a permutation of the respective set $X_j$. Then $g_1 \otimes g_2$ is a permutation of $X_1 \times X_2$, and its cycle type can be computed as the $\circledast$-product of the cycle types of $g_1$ and $g_2$.*

(4) *We assume that $g_1$ has precisely one periodic point $y_1$ (a fixed point, necessarily) and that $g_2$ is a permutation of $X_2$. Then the induced subgraph of $g_1 \otimes g_2$ on* $\mathrm{per}(g_1 \otimes g_2)$ *is isomorphic to $\Gamma_{g_2}$, and for each $\vec{y} \in$* $\mathrm{per}(g_1 \otimes g_2)$, *one has* $\mathrm{Tree}_{\Gamma_{g_1 \otimes g_2}}(\vec{y}) \cong \mathrm{Tree}_{\Gamma_{g_1}}(y_1)$.

*Proof.* Since $g_1 \otimes g_2$ is the component-wise application of $g_1$ and $g_2$ on $X_1 \times X_2$, it is clear that a point $(y_1, y_2) \in X_1 \times X_2$ is periodic under $g_1 \otimes g_2$ if and only if $y_j$ is periodic under $g_j$ for $j = 1, 2$, which settles statement (1) as well as the first assertion on $\vec{y}$ in statement (2).

For the rest of statement (2), we proceed as follows. In order to see that $(\Gamma_{g_1})^* \otimes (\Gamma_{g_2})^*$ has rigid procreation, let $k$ be a positive integer, and let $\vec{y} = (y_1, y_2)$ and $\vec{z} = (z_1, z_2)$ be points in $X_1 \times X_2$ which have at least $k$ successor generations each in that graph. This is equivalent to each of $y_1, y_2, z_1, z_2$ having at least $k$ successor generations in the respective graph $\Gamma_{g_1}^*$ or $\Gamma_{g_2}^*$. It follows that $\mathrm{proc}_k(y_1) = \mathrm{proc}_k(z_1)$ and $\mathrm{proc}_k(y_2) = \mathrm{proc}_k(z_2)$. Now, for $\vec{w} = (w_1, w_2) \in X_1 \times X_2$, the procreation number $\mathrm{proc}_k(\vec{w})$ counts the number of children $\vec{w'} = (w_1', w_2')$ of $\vec{w}$ in $(\Gamma_{g_1})^* \otimes (\Gamma_{g_2})^*$ that have at least $k - 1$ successor generations. But $\vec{w'}$ has at least $k - 1$ successor generations if and only if each $w_j'$ is a child of $w_j$ in $\Gamma_{g_j}^*$ that has at least $k - 1$ successor generations. Therefore, $\mathrm{proc}_k(\vec{w}) = \mathrm{proc}_k(w_1) \cdot \mathrm{proc}_k(w_2)$. In particular,

$$\mathrm{proc}_k(\vec{y}) = \mathrm{proc}_k(y_1)\,\mathrm{proc}_k(y_2) = \mathrm{proc}_k(z_1)\,\mathrm{proc}_k(z_2) = \mathrm{proc}_k(\vec{z}),$$

as required.

For statement (3), see [86, Theorem 2.4 and its proof].

For statement (4), we observe that this is implicit in [13, Theorem 1 (4)], but since it is not proved in detail there, let us do so here. By statement (1), we know that $\vec{z} = (z_1, z_2) \in X_1 \times X_2$ is a periodic point of $g_1 \otimes g_2$ if and only if $z_j \in \mathrm{per}(g_j)$ for $j = 1, 2$. Hence, the periodic points of $g_1 \otimes g_2$ are in bijection with those of $g_2$ via $y_2 \mapsto (y_1, y_2)$, and this bijection preserves cycle lengths. Therefore, the asserted isomorphism $\Gamma_{g_2} \cong \Gamma_{(g_1 \otimes g_2)_{|\mathrm{per}(g_1 \otimes g_2)}}$ is clear. Finally, it is not hard to check that for each $y_2 \in \mathrm{per}(g_2)$, the function $X_1 \to X_1 \times X_2$, $z_1 \mapsto (z_1, ((g_2)_{|\mathrm{per}(g_2)})^{-\mathrm{pperl}_{g_1}(z_1)}(y_2))$, is a digraph isomorphism between $\mathrm{Tree}_{\Gamma_{g_1}}(y_1)$ and $\mathrm{Tree}_{\Gamma_{g_1 \otimes g_2}}((y_1, y_2))$. ∎

We are now ready to prove Theorem 2.1.5. In fact, we prove the following stronger version of it.

**Theorem 2.1.13.** *Let $m$ be a positive integer, and let $A : x \mapsto ax + b$ be an affine map of the cyclic group $\mathbb{Z}/m\mathbb{Z}$. The dual functional graph $(\Gamma_A)^*$ has rigid procreation, and for each $k \in \mathbb{N}^+$ and each periodic vertex $x$ of $\Gamma_A$, one has* $\mathrm{proc}_k(x) = |\ker^{(k)}(\mu_a) : \ker^{(k-1)}(\mu_a)|$. *In particular, each rooted tree above a periodic vertex in $\Gamma_A$ is isomorphic to each rooted tree above a periodic vertex in $\Gamma_{\mu_a}$.*

We note that in the situation of Theorem 2.1.13, one has $|\ker^{(j)}(\mu_a)| = \gcd(a^j, m)$ for all $j \in \mathbb{N}_0$, making the computation of the procreation numbers (and thus the understanding of the isomorphism types of rooted trees above periodic vertices) easy.

*Proof of Theorem* 2.1.13. The "In particular" statement is clear by Proposition 2.1.8 and Theorem 2.1.11, so we focus on the proof of the main statement.

As above, we factor $m = p_1^{v_1} \cdots p_K^{v_K}$ and denote by $A_j$ the reduction of $A$ modulo $p_j^{v_j}$. We claim that for each $j = 1, 2, \ldots, K$, the dual functional graph $(\Gamma_{A_j})^*$ has rigid procreation, and that for each $A_j$-periodic vertex $x \in \mathbb{Z}/p_j^{v_j}\mathbb{Z}$, the procreation number sequence of $x$ in $(\Gamma_{A_j})^*$ agrees with that of a periodic vertex in the dual functional graph of the reduction $(\mu_a)_j$ of $\mu_a$ modulo $p_j^{v_j}$. Indeed, following the proof of Lemma 2.1.6, this is clear both if $\nu_{p_j}^{(v_j)}(a-1) \leq \nu_{p_j}^{(v_j)}(b)$ (where the digraphs $(\Gamma_{A_j})^*$ and $(\Gamma_{(\mu_a)_j})^*$ are actually isomorphic as a whole) and if $\nu_{p_j}^{(v_j)}(a-1) > \nu_{p_j}^{(v_j)}(b)$ (where both $(\Gamma_{A_j})^*$ and $(\Gamma_{(\mu_a)_j})^*$ are disjoint unions of directed cycles).

Now, we recall that $\Gamma_A = \bigotimes_{j=1}^K \Gamma_{A_j}$ and $\Gamma_{\mu_a} = \bigotimes_{j=1}^K \Gamma_{(\mu_a)_j}$. In both tensor products, the duals of the factors indexed by $j$ have rigid procreation with the same procreation number sequences of periodic vertices. Therefore, by Proposition 2.1.12 (2), the same applies to $(\Gamma_A)^*$ versus $(\Gamma_{\mu_a})^*$, and this settles the main statement by virtue of the formula for procreation numbers in Theorem 2.1.11. ∎

We also note the following consequence of Proposition 2.1.12 (1), which will become important later.

**Lemma 2.1.14.** *Let $m$ be a positive integer, let $a, b \in \mathbb{Z}/m\mathbb{Z}$, and let $L$ be a positive integer that is so large that $\gcd(a^L, m) = \prod_{p \mid \gcd(a,m)} p^{\nu_p(m)}$ (for example, $\operatorname{mpe}(m) := \max_p \nu_p(m) \leq \lfloor \log_2 m \rfloor$ is a valid choice for $L$). Then $y \in \mathbb{Z}/m\mathbb{Z}$ is a periodic point of the affine map $A : z \mapsto az + b$ of $\mathbb{Z}/m\mathbb{Z}$ if and only if*

$$y \equiv \sum_{t=0}^{L-1} a^t \cdot b \pmod{\gcd(a^L, m)}.$$

We take note of a notation used especially in group-theoretic literature that can be used to denote the product $\prod_{p \mid \gcd(a,m)} p^{\nu_p(m)}$ from Lemma 2.1.14 in a compact form. Namely, for a set $P$ of primes and a positive integer $n$, the *$P$-part of $n$*, written $n_P$, is defined as $\prod_{p \in P} p^{\nu_p(n)}$. Accordingly, the product $\prod_{p \mid \gcd(a,m)} p^{\nu_p(m)}$ may be written as $m_{\pi(a)}$, where $\pi(a)$ denotes the set of prime divisors of $a$.

*Proof of Lemma 2.1.14.* By Proposition 2.1.12 (1) and the Chinese remainder theorem, a point $y \in \mathbb{Z}/m\mathbb{Z}$ is periodic under $A$ if and only if the reduction $y_p$ of $y$ modulo $p^{\nu_p(m)}$ is periodic under the reduction $A_p$ of $A$ modulo $p^{\nu_p(m)}$ for each prime $p \mid m$. But if $p \nmid a$, then by Proposition 2.1.4 (2), $A_p$ is a permutation of $\mathbb{Z}/p^{\nu_p(m)}\mathbb{Z}$, so $y_p$ is periodic under $A_p$. Therefore, only the primes $p \mid \gcd(a, m)$ actually give a restriction on $y$. For those primes $p$, we know by Proposition 2.1.4 (1) that $A_p$ has precisely one periodic point. It follows that if $y_0 \in \mathbb{Z}/m\mathbb{Z}$ is a periodic point of $A$, then the periodic points $y$ of $A$ are characterized by the congruence $y \equiv y_0 \pmod{\gcd(a^L, m)}$. Therefore, it only remains to prove that $\sum_{t=0}^{L-1} a^t \cdot b$ is a periodic point of $A$.

Now, using the same argument with $b = 0$ so that it applies to $\mu_a : z \mapsto az$, we see that periodic points $y$ of $\mu_a$ are characterized by the congruence

$$y \equiv 0 \pmod{\gcd(a^L, m)}.$$

In particular, $(\mu_a)^L(z) = a^L z$ is periodic under $\mu_a$ for each $z \in \mathbb{Z}/m\mathbb{Z}$. Since the trees above periodic vertices in the functional graphs of $\mu_a$ and $A$ are isomorphic (by Theorem 2.1.5) and thus have the same height, it follows that $A^L(z)$ is periodic under $A$ for each $z \in \mathbb{Z}/m\mathbb{Z}$. In particular, $A^L(0) = \sum_{t=0}^{L-1} a^t \cdot b$ is periodic under $A$, as we needed to show. ∎

This concludes our results for cyclic groups. To round this section off, we put in some extra work to generalize Theorem 2.1.13 to arbitrary finite groups. First, we need to clarify what we mean by “affine map” in general. In what follows, for a fixed group $G$ we denote by $\rho_{\mathrm{r}} : G \to \mathrm{Sym}(G)$, $x \mapsto (y \mapsto yx)$, the so-called *right-regular representation of* $G$ *on itself* (for each $x \in G$, the function value $\rho_{\mathrm{r}}(x) \in \mathrm{Sym}(G)$ is the right-multiplication by $x$ on $G$). Analogously, $\rho_{\mathfrak{l}}$ denotes the *left-regular representation of* $G$ *on itself*, whose function values are the left-multiplications on $G$ by fixed elements of $G$. As is common in group theory, we write the composition of a function $g : X \to Y$ with a function $g' : Y \to Z$ as the product $gg' : X \to Z$ (a synonymous notation is $g' \circ g$). When using this notation for composition, applications of functions to arguments are commonly written using exponents: $x^g$ instead of $g(x)$, so that $x^{gg'} = (x^g)^{g'}$.

**Definition 2.1.15.** Let $G$ be a group. An *affine map of* $G$ is a function $G \to G$ of the form $\varphi\rho_{\mathrm{r}}(b) : x \mapsto x^{\varphi}b$ for some fixed element $b \in G$ and group endomorphism $\varphi$ of $G$.

**Remark 2.1.16.** We note the following concerning the concept of an affine map.

(1) Since $\varphi\rho_{\mathrm{r}}(1_G) = \varphi$, affine maps are generalizations of group endomorphisms.

(2) The affine maps of a given group $G$ form a monoid of functions on $G$, as they are composed via the formula

$$\varphi\rho_{\mathrm{r}}(b) \cdot \varphi'\rho_{\mathrm{r}}(b') = \varphi\varphi'\rho_{\mathrm{r}}(b^{\varphi'}b').$$

(3) Alternatively, one could define affine maps through left-multiplication by a constant after application of a group endomorphism $\varphi$, i.e., as compositions $\varphi\rho_{\mathfrak{l}}(b) = \rho_{\mathfrak{l}}(b) \circ \varphi$. This leads to the same class of functions, as

$$(\rho_{\mathfrak{l}}(b) \circ \varphi)(x) = b\varphi(x) = bx^{\varphi} = bx^{\varphi}b^{-1}b = x^{\varphi\,\mathrm{conj}(b^{-1})}b = x^{\varphi\,\mathrm{conj}(b^{-1})\cdot\rho_{\mathrm{r}}(b)},$$

where $\mathrm{conj}(g)$ is the inner automorphism (conjugation) $x \mapsto g^{-1}xg$ of $G$.

We briefly review some more concepts and results from [13].

**Definition 2.1.17.** Let $G$ be a finite group and $\varphi$ an endomorphism of $G$. The *hyperkernel of* $\varphi$, written $\mathrm{nil}(\varphi)$, consists of those $x \in G$ such that $\varphi^n(x) = 1_G$ for some $n = n(x) \in \mathbb{N}_0$.

**Remark 2.1.18.** The notation $\mathrm{nil}(\varphi)$ stems from the fact that this is the largest $\varphi$-invariant subgroup of $G$ of which the corresponding restriction of $\varphi$ is a nilpotent endomorphism (i.e., an endomorphism that becomes trivial if composed with itself sufficiently often). This subgroup was called the *nilpotent part of $G$ with respect to $\varphi$* in [13], and the authors are not aware of any other names used for it earlier. In particular, in Caranti's paper [16], to which Theorem 2.1.19 below can be traced back, no name was given to this subgroup. The authors decided to switch to the terminology "hyperkernel" in this memoir instead because calling $\mathrm{nil}(\varphi)$ "nilpotent part" may give the wrong impression that it is always a nilpotent group.

In the following theorem, we use the notation $G = H \ltimes N$ to express that the group $G$ is the *(internal) semidirect product of $H$ and $N$*, which means that $H$ is a subgroup of $G$, that $N$ is a normal subgroup of $G$, and that one has $H \cap N = \{1_G\}$ and $HN = \{hn : h \in H, n \in N\} = G$. In this situation, each element of $G$ can be written as a product $hn$ for $h \in H$ and $n \in N$ *in a unique way*, and one may multiply elements of $G$ via the formula $(hn) \cdot (h'n') = hh'n^{h'}n'$, where $n^{h'} = n^{\mathrm{conj}(h')} = (h')^{-1}nh'$.

**Theorem 2.1.19.** *Let $G$ be a finite group, and $\varphi$ an endomorphism of $G$. Then $G = \mathrm{per}(\varphi) \ltimes \mathrm{nil}(\varphi)$.*

*Proof.* See [13, proof of Theorem 1 (1–3)]. We note that after observing that $\mathrm{per}(\varphi)$ is a subgroup and $\mathrm{nil}(\varphi)$ is a normal subgroup of $G$, the rest of the statement follows easily from a group-theoretic version of Fitting's lemma that was proved by Caranti, see [16, Theorem 4.2]. ∎

Theorem 2.1.19 has an interesting consequence concerning the functional graph $\Gamma_\varphi$, which was originally stated as [13, Theorem 1 (4)] and is easy to prove using Proposition 2.1.12 with $X_1 = \mathrm{per}(\varphi)$ and $X_2 = \mathrm{nil}(\varphi)$.

**Corollary 2.1.20.** *Let $G$ be a finite group, and $\varphi$ an endomorphism of $G$. Then*

$$\Gamma_\varphi = \Gamma_{\varphi_{|\mathrm{per}(\varphi)}} \otimes \Gamma_{\varphi_{|\mathrm{nil}(\varphi)}},$$

*and, consequently, for each $x \in \mathrm{per}(\varphi)$, one has $\mathrm{Tree}_{\Gamma_\varphi}(x) \cong \mathrm{Tree}_{\Gamma_{\varphi_{|\mathrm{nil}(\varphi)}}}(1_G)$, a rooted tree that can be obtained from $\Gamma_{\varphi_{|\mathrm{nil}(\varphi)}}$ by deleting the unique loop of the latter at $1_G$.*

The following result extends Theorem 2.1.13 to arbitrary finite groups.

**Theorem 2.1.21.** *Let $G$ be a finite group, $b \in G$, and $\varphi$ an endomorphism of $G$. Then $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ has rigid procreation. Moreover, the sequence of procreation numbers $(\mathrm{proc}_k(x))_{k\geq 1}$ of any periodic vertex $x$ in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ is the same as that of a periodic vertex in $\Gamma^*_\varphi$.*

*Proof.* We prove by induction on $k \geq 1$ that if $x, y \in G$ each have at least $k$ successor generations in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$, then $\mathrm{proc}_k(x) = \mathrm{proc}_k(y)$ in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$. For the induction base, $k = 1$, we observe that for $z \in \{x, y\}$, one has

$$\begin{aligned}\mathrm{proc}_1(z) &= \#\text{ children of } z \text{ in } \Gamma^*_{\varphi\rho_{\mathrm{r}}(b)} \\ &= |\{w \in G : w^{\varphi\rho_{\mathrm{r}}(b)} = z\}| = |\{w \in G : w^{\varphi} = zb^{-1}\}|.\end{aligned}$$

Since $\{w \in G : w^{\varphi} = zb^{-1}\}$ is either empty or a coset of $\ker\varphi$, it follows that $\mathrm{proc}_1(x) = \mathrm{proc}_1(y) = |\ker\varphi|$ whenever $\mathrm{proc}_1(x), \mathrm{proc}_1(y) > 0$, as required.

Now we assume that $k \geq 2$ and that the statement holds up to $k-1$. Each of the two vertices $x$ and $y$ has at least $n$ successor generations in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ for each $n \in \{1, 2, \dots, k-1\}$, whence by the induction hypothesis, one has $\mathrm{proc}_n(x) = \mathrm{proc}_n(y)$ for $n = 1, 2, \dots, k-1$. Now, for each $z \in G$, the number of endpoints of directed paths of length $k$ in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ starting at $z$ is

$$\begin{aligned}|\{w \in G : w^{((\varphi\rho_{\mathrm{r}}(b))^k)} = z\}| &= |\{w \in G : \varphi^k(w) \cdot \varphi^{k-1}(b)\varphi^{k-2}(b) \cdots \varphi(b)b = z\}| \\ &= |\{w \in G : \varphi^k(w) = zb^{-1}\varphi(b)^{-1} \cdots (\varphi^{k-1}(b))^{-1}\}|,\end{aligned}$$

and the set $\{w \in G : \varphi^k(w) = zb^{-1}\varphi(b)^{-1} \cdots (\varphi^{k-1}(b))^{-1}\}$ is either empty or a coset of

$$\ker^{(k)}(\varphi) := \{w \in G : \varphi^k(w) = 1_G\}.$$

Hence, $x$ and $y$ have the same number of endpoints of length $k$ directed paths in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ starting at them, namely $|\ker^{(k)}(\varphi)|$. Using the induction hypothesis in its general form (which basically states that $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ has rigid procreation "for $k-1$ generations"), an easy induction on $n = 1, 2, \dots, k-1$ shows that for each vertex $w \in G$ with at least $n$ successor generations in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$, the number of endpoints of directed paths in $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ of length $n$ starting at $w$ is $\prod_{j=1}^{n} \mathrm{proc}_j(w)$. In particular, if $w$ is a child of $z \in \{x, y\}$ that has at least $k-1$ successor generations, then the number of endpoints of length $k-1$ paths starting at $w$ is $\prod_{j=1}^{k-1} \mathrm{proc}_j(w)$, which is equal to $\prod_{j=1}^{k-1} \mathrm{proc}_j(z)$ by the induction hypothesis. Since the number of such children $w$ of $z$ is $\mathrm{proc}_k(z)$, we conclude that

$$\begin{aligned}\prod_{j=1}^{k} \mathrm{proc}_j(z) &= \mathrm{proc}_k(z) \cdot \prod_{j=1}^{k-1} \mathrm{proc}_j(z) \\ &= \#\text{ endpoints of length } k \text{ paths starting at } z = |\ker^{(k)}(\varphi)|.\end{aligned}$$

Because $z \in \{x, y\}$ is arbitrary, it follows that

$$\prod_{j=1}^{k} \mathrm{proc}_j(x) = \prod_{j=1}^{k} \mathrm{proc}_j(y),$$

and since $\mathrm{proc}_j(x) = \mathrm{proc}_j(y) > 0$ for $j = 1, 2, \ldots, k-1$, this allows us to conclude that $\mathrm{proc}_k(x) = \mathrm{proc}_k(y)$, as required.

Concerning the claim that the procreation numbers of $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ and $\Gamma^*_{\varphi}$ are the same, the above argument shows that for any positive integer $k$ and any periodic vertex $x$ of $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$, we have

$$\prod_{j=1}^{k} \mathrm{proc}_j(x) = |\ker^{(k)}(\varphi)|.$$

It follows that

$$\mathrm{proc}_k(x) = |\ker^{(k)}(\varphi) : \ker^{(k-1)}(\varphi)|$$

for each $k \in \mathbb{N}^+$ (we note that $\ker^{(0)}(\varphi) = \{1_G\}$). Therefore, the procreation number sequence of a periodic vertex of $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)}$ only depends on $\varphi$, not on $b$, and for $b := 1_G$, one has $\Gamma^*_{\varphi\rho_{\mathrm{r}}(b)} = \Gamma^*_{\varphi}$. ■

## 2.2 The master lemma

From the introduction, we recall the notion of an $m$-CC (short for "$m$-congruential condition"), which we defined as a condition of the form $\nu(x \equiv \mathfrak{b} \pmod{\mathfrak{a}})$ with $\mathfrak{a} \mid m$ and $\nu \in \{\emptyset, \neg\}$. In this section, we consider systems formed from $m$-CCs in one common variable. Such a system is *consistent* if it has an integer solution, and two such systems are *equivalent* if they have the same solution set in $\mathbb{Z}$ (or, equivalently, in $\mathbb{Z}/m\mathbb{Z}$). The solution set in $\mathbb{Z}/m\mathbb{Z}$ of a consistent system of $m$-CCs is a block of the associated arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$ (see Definition 1.5). We note the following fundamental result on systems of $m$-congruences, which is a well-known generalization of the Chinese remainder theorem.

**Proposition 2.2.1.** *Let $m$ be a positive integer. We consider a system of $m$-congruences, of the form*

$$\begin{aligned} x &\equiv \mathfrak{b}_1 \pmod{\mathfrak{a}_1}, \\ x &\equiv \mathfrak{b}_2 \pmod{\mathfrak{a}_2}, \\ &\vdots \\ x &\equiv \mathfrak{b}_K \pmod{\mathfrak{a}_K}. \end{aligned} \tag{2.2}$$

*The following statements are equivalent.*

(1) *System (2.2) is consistent.*

(2) *For all $1 \leq j < k \leq K$, one has* $\gcd(\mathfrak{a}_j, \mathfrak{a}_k) \mid \mathfrak{b}_j - \mathfrak{b}_k$.

(3) *Any pair of $m$-congruences in system (2.2) form a consistent system.*

(4) *System* (2.2) *is equivalent to a single $m$-congruence, of the form*

$$x \equiv \mathfrak{b} \pmod{\operatorname{lcm}(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_K)}.$$

*In particular, if system* (2.2) *is consistent, then its number of solutions modulo $m$ is equal to $m/\operatorname{lcm}(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_K)$ and is, therefore, independent of the $\mathfrak{b}_j$.*

*Proof.* For the equivalence "(1)⇔(2)" and the implication "(1)⇒(4)", see [41, Theorem 3.3.4 on p. 78], for example. Moreover, the implication "(4)⇒(1)" is trivial. As for the equivalence "(1)⇔(3)", we note that by the already established equivalence "(1)⇔(2)", applied to the system

$$\begin{aligned} x &\equiv \mathfrak{b}_j \pmod{\mathfrak{a}_j}, \\ x &\equiv \mathfrak{b}_k \pmod{\mathfrak{a}_k}, \end{aligned} \tag{2.3}$$

that system is consistent if and only if the single divisibility $\gcd(\mathfrak{a}_j, \mathfrak{a}_k) \mid \mathfrak{b}_j - \mathfrak{b}_k$ holds. But statement (3) just demands that system (2.3) be consistent for all $1 \le j < k \le K$, which is therefore equivalent to statement (2), and thus to statement (1). ■

Proposition 2.2.1 is the basis for proving the following lemma, which is crucial for our recursive approach for understanding the rooted trees in Section 3.3.

**Lemma 2.2.2.** *[Master lemma] Let $m$ be a positive integer, and let $\mathcal{P}$ be an arithmetic partition of $\mathbb{Z}/m\mathbb{Z}$. Moreover, let $a, b \in \mathbb{Z}/m\mathbb{Z}$, and consider the affine map $A : x \mapsto ax + b$ of $\mathbb{Z}/m\mathbb{Z}$. There is an arithmetic partition $\mathcal{P}'$ of $\mathbb{Z}/m\mathbb{Z}$ with $\operatorname{AC}(\mathcal{P}') \le \operatorname{AC}(\mathcal{P}) + 1$ such that if $x, y \in \mathbb{Z}/m\mathbb{Z}$ are from a common block of $\mathcal{P}'$, and if $B$ is a block of $\mathcal{P}$, then $|A^{-1}(\{x\}) \cap B| = |A^{-1}(\{y\}) \cap B|$.*

*More specifically, if $\mathcal{P} = \mathfrak{P}(x \equiv \mathfrak{b}_j \pmod{\mathfrak{a}_j} : j = 1, 2, \dots, K)$, then*

$$\mathfrak{P}'(\mathcal{P}, A) := \mathfrak{P}\begin{pmatrix} x \equiv a\mathfrak{b}_1 + b \pmod{\gcd(a\mathfrak{a}_1, m)} \\ x \equiv a\mathfrak{b}_2 + b \pmod{\gcd(a\mathfrak{a}_2, m)} \\ \vdots \\ x \equiv a\mathfrak{b}_K + b \pmod{\gcd(a\mathfrak{a}_K, m)} \\ x \equiv b \pmod{\gcd(a, m)} \end{pmatrix}$$

*is a valid choice for $\mathcal{P}'$, and a formula for $|A^{-1}(\{x\}) \cap B|$ in terms of the $\mathcal{P}$-block $B$ and the unique $\mathfrak{P}'(\mathcal{P}, A)$-block $B'$ containing $x$ can be obtained as follows: write $B = \mathcal{B}(\mathcal{P}, \vec{\nu})$ and $B' = \mathcal{B}(\mathfrak{P}'(\mathcal{P}, A), \vec{\nu'})$ with $\vec{\nu} = (\nu_1, \dots, \nu_K) \in \{\emptyset, \neg\}^K$ and $\vec{\nu'} = (\nu'_1, \dots, \nu'_{K+1}) \in \{\emptyset, \neg\}^{K+1}$. We introduce the following notations.*

- *$J_-(\vec{\nu}) := \{j \in \{1, 2, \dots, K\} : \nu_j = \neg\}$ and (analogously)*

$$J_-(\vec{\nu'}) := \{j' \in \{1, 2, \dots, K+1\} : \nu'_{j'} = \neg\};$$

- *$J_+(\vec{\nu}) := \{1, 2, \dots, K\} \setminus J_-(\vec{\nu})$;*

- *For $J \subseteq J_-(\vec{\mathfrak{v}})$, we denote by $E(\vec{\mathfrak{v}}, J)$ the condition*

$$\gcd(\mathfrak{a}_{j_1}, \mathfrak{a}_{j_2}) \mid \mathfrak{b}_{j_1} - \mathfrak{b}_{j_2} \quad \textit{for all } j_1, j_2 \in J_+(\vec{\mathfrak{v}}) \cup J.$$

*Then for each $x \in \mathcal{B}(\mathfrak{P}'(\mathcal{P}, A), \vec{\nu'})$, the intersection size $|A^{-1}(\{x\}) \cap \mathcal{B}(\mathcal{P}, \vec{\mathfrak{v}})|$ is equal to*

$$\sum_{J \subseteq J_-(\vec{\mathfrak{v}})} (-1)^{|J|} \kappa_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'}, J) =: \sigma_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'}),$$

*where*

$$\begin{aligned}&\kappa_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'}, J) \\ &\quad := \delta_{\nu'_{K+1}=\emptyset} \cdot \delta_{E(\vec{\mathfrak{v}},J)} \cdot \delta_{(J_+(\vec{\mathfrak{v}}) \cup J) \cap J_-(\vec{\nu'})=\emptyset} \cdot \frac{m}{\operatorname{lcm}(\frac{m}{\gcd(a,m)}, \mathfrak{a}_j : j \in J_+(\vec{\mathfrak{v}}) \cup J)},\end{aligned}$$

*the three deltas being Kronecker deltas.*

We call a number of the form $\sigma_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'})$ a *distribution number of $\mathcal{P}$ (under $A$).*

*Proof of Lemma 2.2.2.* To verify that

$$\mathcal{P}' := \mathfrak{P}'(\mathcal{P}, A)$$

has the desired property, we set

- $M_j := \{x \in \mathbb{Z}/m\mathbb{Z} : x \equiv \mathfrak{b}_j \pmod{\mathfrak{a}_j}\}$ for $j = 1, 2, \ldots, K$;
- $M_+(\vec{\mathfrak{v}}) := \bigcap_{j \in J_+(\vec{\mathfrak{v}})} M_j$;

and note that $B = M_+(\vec{\mathfrak{v}}) \cap \bigcap_{j \in J_-(\vec{\mathfrak{v}})} M_j^c$ (the superscript $c$ denoting set complementation in $\mathbb{Z}/m\mathbb{Z}$). Therefore, by the inclusion-exclusion principle, the intersection size $|A^{-1}(\{x\}) \cap B|$ we are looking for is equal to

$$\sum_{J \subseteq J_-(\vec{\mathfrak{v}})} (-1)^{|J|} \Big|(M_+(\vec{\mathfrak{v}}) \cap A^{-1}(\{x\})) \cap \bigcap_{j \in J} M_j\Big|.$$

It is thus our goal to argue that the value of this sum is equal to $\sigma_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'})$ (in particular, it is independent of the choice of $x \in B' = \mathcal{B}(\mathcal{P}', \vec{\nu'})$). We do so by arguing that, in fact, the intersection size

$$\Big|(M_+(\vec{\mathfrak{v}}) \cap A^{-1}(\{x\})) \cap \bigcap_{j \in J} M_j\Big|$$

is equal to $\kappa_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu'}, J)$, for each $J \subseteq J_-(\vec{\mathfrak{v}})$. Now, writing

$$J_+(\vec{\mathfrak{v}}) \cup J = \{j_1, j_2, \ldots, j_N\},$$

the intersection $(M_+(\vec{\mathfrak{v}}) \cap A^{-1}(\{x\})) \cap \bigcap_{j\in J} M_j$ is the solution set in $\mathbb{Z}/m\mathbb{Z}$ of the following system in the variable $y$:

$$\begin{aligned} y &\equiv \mathfrak{b}_{j_1} \pmod{\mathfrak{a}_{j_1}}, \\ y &\equiv \mathfrak{b}_{j_2} \pmod{\mathfrak{a}_{j_2}}, \\ &\vdots \\ y &\equiv \mathfrak{b}_{j_N} \pmod{\mathfrak{a}_{j_N}}, \\ ay + b &\equiv x \pmod{m}. \end{aligned} \tag{2.4}$$

Now, the single congruence $ay + b \equiv x \pmod{m}$ is solvable in $y$ if and only if $\gcd(a, m) \mid x - b$, i.e., if and only if $x \equiv b \pmod{\gcd(a, m)}$. This is one of the spanning congruences for $\mathcal{P}'$, whence its truth value is constant for all $x \in B'$. If that congruence is false for all $x \in B'$ (equivalently, if $\nu'_{K+1} = \neg$), then system (2.4) is always false, whence $|(M_+(\vec{\mathfrak{v}}) \cap A^{-1}(\{x\})) \cap \bigcap_{j\in J} M_j| = 0$ for all $J \subseteq J_-(\vec{\mathfrak{v}})$, independently of $x$. This explains the first Kronecker delta in the definition of $\kappa_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu}', J)$.

We may thus henceforth assume that $\nu'_{K+1} = \emptyset$, i.e., that $x \equiv b \pmod{\gcd(a, m)}$ for all $x \in B'$. Then the congruence $ay + b \equiv x \pmod{m}$ can be equivalently rewritten into

$$y \equiv \mathrm{inv}_{m/\gcd(a,m)}\left(\frac{a}{\gcd(a, m)}\right) \cdot \frac{x - b}{\gcd(a, m)} \left(\mathrm{mod}\ \frac{m}{\gcd(a, m)}\right), \tag{2.5}$$

where $\mathrm{inv}_n(x)$ denotes the multiplicative inverse of the unit $x$ modulo $n$. If we replace the congruence $ay + b \equiv x \pmod{m}$ in the system (2.4) by the equivalent congruence (2.5), then the resulting system consists entirely of $m$-congruences. By Proposition 2.2.1, there are only two possibilities for the number of solutions modulo $m$ of this system: either the system is inconsistent and, thus, has 0 solutions, or it has $m/L$ solutions, where $L$ is the least common multiple of the moduli that occur. Neither of these two expressions for the number of solutions depends on $x$, so we aim to show that it does not depend on the choice of $x \in B'$ which of the two cases occurs.

Now, Proposition 2.2.1 also implies that system (2.4) is consistent if and only if any pair of conditions in it is consistent. It thus suffices to argue that for no pair of conditions in system (2.4) does the consistency of the system formed from those two conditions depend on the choice of $x \in B'$. If both of those conditions are distinct from the congruence $ay + b \equiv x \pmod{m}$, then they are of the forms $y \equiv \mathfrak{b}_j \pmod{\mathfrak{a}_j}$ and $y \equiv \mathfrak{b}_k \pmod{\mathfrak{a}_k}$, for suitable $j, k \in J_+(\vec{\mathfrak{v}}) \cup J$, and by Proposition 2.2.1, those two conditions form a consistent system if and only if $\gcd(\mathfrak{a}_j, \mathfrak{a}_k) \mid \mathfrak{b}_j - \mathfrak{b}_k$. Equivalently, the system obtained from (2.4) by deleting the single congruence $ay + b \equiv x \pmod{m}$ is consistent if and only if the condition $E(\vec{\mathfrak{v}}, J)$ holds, which explains the second Kronecker delta in the definition of $\kappa_{\mathcal{P},A}(\vec{\mathfrak{v}}, \vec{\nu}', J)$.

It remains to consider two-condition subsystems of (2.4) of the form

$$\begin{aligned} ay + b &\equiv x \pmod{m}, \\ y &\equiv \mathfrak{b}_j \pmod{\mathfrak{a}_j} \end{aligned} \tag{2.6}$$

for some $j \in J_+(\vec{\nu}) \cup J$. We claim that system (2.6) is consistent if and only if $x \equiv a\mathfrak{b}_j + b \pmod{\gcd(a\mathfrak{a}_j, m)}$. Indeed, if system (2.6) is consistent, then there is a $k \in \mathbb{Z}$ such that some $y = \mathfrak{b}_j + k\mathfrak{a}_j$ satisfies the first condition of the system. That is, one then has

$$x \equiv ay + b = a\mathfrak{b}_j + ka\mathfrak{a}_j + b \pmod{m}.$$

In particular,

$$x \equiv a\mathfrak{b}_j + ka\mathfrak{a}_j + b \equiv a\mathfrak{b}_j + b \pmod{\gcd(a\mathfrak{a}_j, m)},$$

as required. On the other hand, let us assume that

$$x \equiv a\mathfrak{b}_j + b \pmod{\gcd(a\mathfrak{a}_j, m)}.$$

Then we can write $x = a\mathfrak{b}_j + b + k' \gcd(a\mathfrak{a}_j, m)$ for some $k' \in \mathbb{Z}$. We need to verify that there is an integer $k$ such that for $y = \mathfrak{b}_j + k\mathfrak{a}_j$, one has

$$ay + b = a\mathfrak{b}_j + ka\mathfrak{a}_j + b \equiv x = a\mathfrak{b}_j + b + k' \gcd(a\mathfrak{a}_j, m) \pmod{m},$$

which is equivalent to $ka\mathfrak{a}_j \equiv k' \gcd(a\mathfrak{a}_j, m) \pmod{m}$. And indeed, this is solvable in $k$, because $\gcd(a\mathfrak{a}_j, m) \mid k' \gcd(a\mathfrak{a}_j, m)$.

Now, because $x \equiv a\mathfrak{b}_j + b \pmod{\gcd(a\mathfrak{a}_j, m)}$ is the $j$-th spanning congruence of $\mathcal{P}'$, it follows that if $\nu'_j = \neg$ (equivalently, if $j \in J_-(\vec{\nu'})$), then the intersection $(M_+(\vec{\nu}) \cap A^{-1}(\{x\})) \cap \bigcap_{j \in J} M_j$ is empty whenever $j \in J_+(\vec{\nu}) \cup J$ as well, which explains the third Kronecker delta in the definition of $\kappa_{\mathcal{P},A}(\vec{\nu}, \vec{\nu'}, J)$.

If all three Kronecker deltas in the definition of $\kappa_{\mathcal{P},A}(\vec{\nu}, \vec{\nu'}, J)$ are 1, then our argumentation shows that system (2.4) is consistent and is thus equivalent to a single $m$-congruence by an application of Proposition 2.2.1 (we recall that the last congruence in system (2.4) may be replaced by the equivalent $m$-congruence (2.5)), the modulus of which is the least common multiple $L$ of the moduli involved in the $m$-congruence forms of the conditions in system (2.4). It follows that the size of the solution set of system (2.4) then is

$$\frac{m}{L} = \frac{m}{\operatorname{lcm}\left(\frac{m}{\gcd(a,m)}, \mathfrak{a}_j : j \in J_+(\vec{\nu}) \cup J\right)}.$$

Therefore, our technical parameter $\kappa_{\mathcal{P},A}(\vec{\nu}, \vec{\nu'}, J)$ indeed always agrees with the intersection size $|(M_+(\vec{\nu}) \cap A^{-1}(\{x\})) \cap \bigcap_{j \in J} M_j|$, and this concludes the proof. ∎

## 2.3 CRL-lists of affine maps of finite cyclic groups

We view $\mathbb{Z}/m\mathbb{Z}$, where $m \in \mathbb{N}^+$, as a ring with underlying set $\{0, 1, \dots, m-1\}$ and modular addition and modular multiplication as the ring operations. In particular, if $m_1 \leq m_2$ are positive integers, then we have an inclusion of sets $\mathbb{Z}/m_1\mathbb{Z} \subseteq \mathbb{Z}/m_2\mathbb{Z}$. We may also view integers outside of the range $\{0, 1, \dots, m-1\}$ as elements of $\mathbb{Z}/m\mathbb{Z}$, via reduction modulo $m$ (identifying $x \in \mathbb{Z}$ with $x \bmod m$). We remind the reader of the notation $\nu_p^{(v)}(x) := \min\{v, \nu_p(x)\}$ for $p$ prime, $v \in \mathbb{N}_0$ and $x \in \mathbb{Z}$, originally introduced after Theorem 2.1.5.

As was mentioned in the introduction, the construction of a CRL-list (in the sense of Definition 1.2) for a generalized cyclotomic mapping of $\mathbb{F}_q$ can be reduced to the corresponding problem for affine maps of finite cyclic groups, which we solve in this section; see Section 3.1 for the application of this to constructing CRL-lists of generalized cyclotomic mappings. We also observed in the introduction that determining a CRL-list for a function $g : X \to X$ with $X$ finite is generally a harder problem than the determination of the cycle type of $g_{|\mathrm{per}(g)}$, and we would like to give an overview of the history of the latter problem for the case where $g$ is an affine permutation of a finite cyclic group.

Ahmad [5] determined the cycle structure of *automorphisms* of finite cyclic groups. The cycle index of the group of affine permutations of a finite cyclic group $\mathbb{Z}/m\mathbb{Z}$ (which is a polynomial that encodes how many affine permutations of each given cycle type there are) was described by Wei and Xu [86]. In their paper, they gave the formulas for the case where $m$ is a prime power without proof, referring to the two-page research announcement [85] by Wei, Gao and Yang. Unfortunately, while Bors and Wang were working on [15], they were unable to find [85] through an online search, which led them to derive those formulas independently as [15, Theorem 4.8], based on a precise description of the cycle type of a given affine permutation $A : x \mapsto ax + b$ of $\mathbb{Z}/p^v\mathbb{Z}$ in terms of $a$ and $b$, stated as [15, Proposition 4.7]. This latter result is as of now, to the authors' knowledge, the only accessible reference that lists those cycle types explicitly, in a tabular form. While working on the current memoir, the authors realized that [15, Proposition 4.7] could also have been easily derived from Deng's results [21, Lemmas 4 and 7] and Ahmad's result [5, Theorem 1].

Let us now turn to the determination of CRL-lists. Let $m$ be a positive integer, and let $a, b \in \mathbb{Z}$. We consider the affine map $A : x \mapsto ax + b$ of $\mathbb{Z}/m\mathbb{Z}$. From Proposition 2.1.4, we know the following.

- The reduction of $A$ modulo $m' := \prod_{p \mid m, p \nmid a} p^{\nu_p(m)}$ is an affine permutation of $\mathbb{Z}/m'\mathbb{Z}$.
- The reduction of $A$ modulo $m'' := \prod_{p \mid \gcd(a,m)} p^{\nu_p(m)}$ has exactly one periodic point $\mathfrak{f}''$ in $\mathbb{Z}/m''\mathbb{Z}$, which we know explicitly thanks to Lemma 2.1.14.

Now, the restriction of the projection

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m''\mathbb{Z} \to \mathbb{Z}/m'\mathbb{Z}$$

to $\mathbb{Z}/m'\mathbb{Z} \times \{\mathfrak{f}''\}$ is bijective; we denote by $\Lambda$ its inverse function $\mathbb{Z}/m'\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Then, if $\mathcal{L}'$ is a CRL-list of the reduction of $A$ modulo $m'$, the set $\{(\Lambda(r), l) : (r, l) \in \mathcal{L}'\}$ is a CRL-list of $A$. This reduces the problem to the special case where $A$ is an affine *permutation* of a finite cyclic group, which we henceforth assume.

In order to understand CRL-lists of affine permutations of finite cyclic groups, it is helpful to proceed in several steps.

(1) First, we determine a CRL-list for each *group automorphism* of each finite *primary* cyclic group (i.e., $\mathbb{Z}/p^v\mathbb{Z}$).

(2) Next, we extend this to arbitrary affine permutations of finite *primary* cyclic groups.

(3) Finally, we use the Chinese remainder theorem and some extra ideas to construct a CRL-list of any affine permutation $A$ of each finite cyclic group from CRL-lists of the reductions of $A$ modulo the various prime powers $p^{v_p(m)}$.

Before tackling step (1) properly, we prove the following useful lemma.

**Lemma 2.3.1.** *Let $X$ be a finite set, $\psi \in \mathrm{Sym}(X)$, $\mathcal{L}$ a CRL-list of $\psi$, and $n \in \mathbb{Z}$. Then the following is a CRL-list of $\psi^n$:*

$$\left\{\left(\psi^j(r), \frac{l}{\gcd(n,l)}\right) : (r, l) \in \mathcal{L}, j = 0, 1, \ldots, \gcd(n,l) - 1\right\}.$$

*In particular, if* $\gcd(n, \mathrm{ord}(\psi)) = 1$*, then $\mathcal{L}$ is also a CRL-list of $\psi^n$.*

*Proof.* Each cycle of $\psi^n$ is contained in a cycle of $\psi$, and for any given cycle $\zeta$ of $\psi$ of length $l$, the $\psi^n$-cycles into which $\zeta$ decomposes correspond to the cosets of the subgroup of $\mathbb{Z}/l\mathbb{Z}$ generated by $n + l\mathbb{Z}$. Since the additive order of $n$ modulo $l$ is $l/\gcd(n,l)$, it follows that $\zeta$ decomposes into $\gcd(n,l)$ cycles of $\psi^n$, each of length $l/\gcd(n,l)$. If $r$ is the representative of $\zeta$ from $\mathcal{L}$, then for each $\psi^n$-cycle $\zeta'$ contained in $\zeta$, the elements on $\zeta'$ are just those of the form $\psi^t(r)$ for $t \in k + \gcd(n,l)\mathbb{Z}$, for some $k = k(\zeta') \in \mathbb{Z}$. It follows that the $\gcd(n,l)$ elements $\psi^j(r)$ of (the support set of) $\zeta$ for $j = 0, 1, \ldots, \gcd(n,l) - 1$ lie on pairwise distinct $\psi^n$-cycles and thus form a system of representatives for the $\psi^n$-cycles contained in $\zeta$. This proves the main statement of the lemma. The "In particular" statement follows because the equality $\gcd(n, \mathrm{ord}(\psi)) = 1$ is equivalent to "$\gcd(n,l) = 1$ for each cycle length $l$ of $\psi$". ■

We are now ready to specify a CRL-list for each automorphism of each finite primary cyclic group. In the proof of the following lemma and beyond, we use the notation $H \leq G$ for "$H$ is a subgroup of $G$", and $\langle g_1, g_2, \ldots, g_n\rangle$ to denote the subgroup of the group $G$ generated by the elements $g_1, g_2, \ldots, g_n \in G$.

| Case for $p$ and $a$ | elements of $\mathcal{L}(p^v, a)$ |
|---|---|
| $p > 2$ | $\left(\mathrm{r}^j p^t, \frac{\phi(p^{v-t})}{\gcd\left(\frac{\phi(p^v)}{\mathrm{ord}(a)}, \phi(p^{v-t})\right)}\right)$ for<br>$t = 0, 1, \ldots, v$ and $j = 0, 1, \ldots, \gcd\left(\frac{\phi(p^v)}{\mathrm{ord}(a)}, \phi(p^{v-t})\right) - 1$. |
| $p = 2, a \equiv 1 \pmod 4$ | $(0, 1)$, $(2^{v-1}, 1)$;<br>$\left(5^j 2^t, \frac{2^{v-t-2}}{\gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right)}\right)$, $\left(-5^j 2^t, \frac{2^{v-t-2}}{\gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right)}\right)$ for<br>$t = 0, 1, \ldots, v-2$ and $j = 0, 1, \ldots, \gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right) - 1$. |
| $p = 2, a \equiv 3 \pmod 4$ | $(0, 1)$, $(2^{v-1}, 1)$;<br>$(j \cdot \mathrm{ord}(-a), 2)$ for $j = 1, 2, \ldots, \frac{2^{v-1}}{\mathrm{ord}(-a)} - 1$;<br>$\left(5^j 2^t, \frac{\mathrm{ord}(-a)}{2^t}\right)$, $\left(-5^j 2^t, \frac{\mathrm{ord}(-a)}{2^t}\right)$ for<br>$t = 0, 1, \ldots, \log_2(\mathrm{ord}(-a)) - 1$ and<br>$j = 0, 1, \ldots, \frac{2^{v-2}}{\mathrm{ord}(-a)} - 1$. |

**Table 2.1.** CRL-lists of automorphisms of finite primary cyclic groups.

**Lemma 2.3.2.** *Let $p$ be a prime, $v \in \mathbb{N}^+$, and $a \in \mathbb{Z}$ with $p \nmid a$. If $p$ is odd, let $\mathrm{r}$ be a fixed primitive root modulo $p^v$, and let $\phi$ denote Euler's totient function. Table 2.1 provides a CRL-list $\mathcal{L}(p^v, a)$ of the automorphism $\mu_a : x \mapsto ax$ of $\mathbb{Z}/p^v\mathbb{Z}$. We write* $\mathrm{ord}(a) = \mathrm{ord}(\mu_a)$ *for the* multiplicative *order of $a$ modulo $p^v$.*

*Proof of Lemma 2.3.2.* First, we assume that $p > 2$. If $a$ is a primitive root modulo $p^v$, then the cyclic group $\langle a \rangle = (\mathbb{Z}/p^v\mathbb{Z})^* \cong \mathrm{Aut}(\mathbb{Z}/p^v\mathbb{Z})$ acts transitively on each subset of $\mathbb{Z}/p^v\mathbb{Z}$ consisting of all elements of a given additive order. Indeed, on the one hand, automorphisms of $\mathbb{Z}/p^v\mathbb{Z}$ must preserve the additive order of elements, and conversely, if $x, y \in \mathbb{Z}/p^v\mathbb{Z}$ are of the same order, then they are multiples of each other. Hence $y = z \cdot x$ for some $z \in (\mathbb{Z}/p^v\mathbb{Z})^*$. Since $z$ is a power of $a$, the transitivity assertion follows. We conclude that if $a$ is a primitive root modulo $p^v$, then $\mathcal{L}(p^v, a)$ may be chosen as $\{(p^t, \phi(p^{v-t})) : t = 0, 1, \ldots, v\}$, which matches with Table 2.1.

For general $a$, we note that $a$ and $\mathrm{r}^{\phi(p^v)/\mathrm{ord}(a)}$ are powers of each other, whence by the "In particular" of Lemma 2.3.1 we may assume without loss of generality that $a = \mathrm{r}^{\phi(p^v)/\mathrm{ord}(a)}$. The claim now follows by applying the main statement of Lemma 2.3.1 with $n := \phi(p^v)/\mathrm{ord}(a)$ and $\mathcal{L} := \{(p^t, \phi(p^{v-t})) : t = 0, 1, \ldots, v\}$.

Now we assume that $p = 2$. First, let us discuss the case $a = 5$. The automorphism $\mu_5 : x \mapsto 5x$, like any automorphism of $\mathbb{Z}/2^v\mathbb{Z}$, fixes the unique elements $0$ and $2^{v-1}$ of additive orders $1$ and $2$, respectively. It also fixes the order $4$ elements $2^{v-2}$ and $3 \cdot 2^{v-2} = -2^{v-2}$. Moreover, we claim that for each $t' \in \{3, 4, \ldots, v\}$, the automorphism $\mu_5$ has exactly two cycles on the elements of $\mathbb{Z}/2^v\mathbb{Z}$ of additive order $2^{t'}$, both of length $2^{t'-2}$ and spanned by $2^{v-t'}$ and $-2^{v-t'}$, respectively. Indeed, this is clear for $t' = 3$ and $t' = v$; for the latter, we use that the multiplicative order of $5 = 1 + 2^2$ modulo $2^v$ is $2^{v-2}$, that $\langle 5\rangle \leq (\mathbb{Z}/2^v\mathbb{Z})^*$ acts semiregularly (i.e., such that no element of that group except the neutral element 1 admits fixed points in that action) on the set of generators (i.e., elements of additive order $2^v$) of $\mathbb{Z}/2^v\mathbb{Z}$, and that $1 \not\equiv -1 \pmod 4$. For each other value of $t'$, denoting by $\mathrm{aord}(x)$ the additive order of $x$ modulo $2^v$, it follows from the commutativity of the diagram

$$\begin{tikzcd}
\{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^v\} \arrow[r, "x \mapsto 5x"] \arrow[d, "x \mapsto 2^{v-t'}x"'] & \{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^v\} \arrow[d, "x \mapsto 2^{v-t'}x"] \\
\{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^{t'}\} \arrow[r, "x \mapsto 5x"'] & \{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^{t'}\}
\end{tikzcd}$$

that $x \mapsto 5x$ has *at most* two cycles on the set of order $2^{t'}$ elements, namely the ones spanned by $2^{v-t'} \cdot 1 = 2^{v-t'}$ and $2^{v-t'} \cdot (-1) = -2^{v-t'}$. Likewise, the commutativity of the diagram

$$\begin{tikzcd}
\{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^{t'}\} \arrow[r, "x \mapsto 5x"] \arrow[d, "x \mapsto 2^{t'-3}x"'] & \{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 2^{t'}\} \arrow[d, "x \mapsto 2^{t'-3}x"] \\
\{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 8\} \arrow[r, "x \mapsto 5x"'] & \{x \in \mathbb{Z}/2^v\mathbb{Z} : \mathrm{aord}(x) = 8\}
\end{tikzcd}$$

implies that $2^{v-t'}$ and $-2^{v-t'}$ lie on *distinct* cycles of $x \mapsto 5x$. This shows that $\mathcal{L}(2^v, 5)$ can be chosen as indicated in Table 2.1.

As for other values of $a$, if $a \equiv 1 \pmod 4$, then $a$ is congruent to a power of 5 modulo $2^v$, and the choice for $\mathcal{L}(2^v, a)$ specified in Table 2.1 can be derived from the one for $\mathcal{L}(2^v, 5)$ using Lemma 2.3.1 (analogously to the end of the argument for $p > 2$ above).

It remains to deal with the case $a \equiv 3 \pmod 4$. Then $-a \equiv 1 \pmod 4$. We view the automorphism $\mu_a$ of $\mathbb{Z}/2^v\mathbb{Z}$ as the composition of the automorphisms $\mu_{-a}$ and $\mu_{-1}$. For each $t' \in \{0, 1, \ldots, v\}$, we want to understand the cycles of $\mu_a$ on the set of elements $x$ of additive order $2^{t'}$, and we do so by distinguishing some cases for $t'$.

- If $t' \in \{0, 1\}$ (i.e., $x \in \{0, 2^{v-1}\}$), then $x$, being the only element in $\mathbb{Z}/2^v\mathbb{Z}$ of its additive order, is fixed by $\mu_a$.
- If $t' \in \{2, 3, \ldots, v - \log_2(\mathrm{ord}(-a))\}$, then $\mu_{-a}$ fixes each element of order $2^{t'}$; this can be seen by using the formula for "$a \equiv 1 \pmod 4$" in Table 2.1 and noting

that if $x \in \{a^j 2^t, -a^j 2^t\}$, then $2^{t'} = \operatorname{aord}(x) = 2^{v-t}$. It follows that the restriction of $\mu_a$ to set of order $2^{t'}$ elements is the same as that of $\mu_{-1}$. Therefore,

$$\left\{(j \cdot \operatorname{ord}(-a), 2) : j = 1, 2, \ldots, \frac{2^{v-1}}{\operatorname{ord}(-a)} - 1\right\},$$

which is a CRL-list of the restriction of $\mu_{-1}$ to the set of elements of $\mathbb{Z}/2^v\mathbb{Z}$ with order in $\{2^2, 2^3, \ldots, 2^{v-\log_2(\operatorname{ord}(-a))}\}$, is also a CRL-list of the corresponding restriction of $\mu_a$.

- Finally, if $t' > v - \log_2(\operatorname{ord}(-a))$, then all cycles of $\mu_{-a}$ on the set of order $2^{t'}$ elements in $\mathbb{Z}/2^v\mathbb{Z}$ are of even length (in fact, their length is a nontrivial power of 2). For a fixed $j \in \{0, 1, \ldots, \gcd(\frac{2^{v-2}}{\operatorname{ord}(-a)}, 2^{t'-2}) - 1\} = \{0, 1, \ldots, \frac{2^{v-2}}{\operatorname{ord}(-a)} - 1\}$, we consider the two cycles of $\mu_{-a}$ spanned by $5^j 2^{v-t'}$ and $-5^j 2^{v-t'}$, respectively. These cycles are distinct (according to the case "$a \equiv 1 \pmod 4$" in Table 2.1, applied to $-a$), both have length

$$\frac{2^{t'-2}}{\gcd\left(\frac{2^{v-2}}{\operatorname{ord}(-a)}, 2^{t'-2}\right)} = \frac{2^{t'-2}}{2^{v-2-\log_2(\operatorname{ord}(-a))}} = 2^{t'-v+\log_2(\operatorname{ord}(-a))}$$

and are images of each other under $\mu_{-1}$. In fact, since $\mu_{-a}$ and $\mu_{-1}$ commute, we have $\mu_{-1}(\mu_{-a}^n(\pm 5^j 2^{v-t'})) = \mu_{-a}^n(\mu_{-1}(\pm 5^j 2^{v-t'}))$ for each $n \in \mathbb{Z}$, which leads to the following diagrammatic picture of how the cycles are matched under $\mu_{-1}$, setting $k := 2^{t'-v+\log_2(\operatorname{ord}(-a))-1}$, so that $k$ is half of the common cycle length of $\pm 5^j 2^{v-t'}$ under $\mu_{-a}$:

$$\begin{tikzcd}
5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] \arrow[d, "\mu_{-1}"'] & (-a)5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] \arrow[d, "\mu_{-1}"'] & \cdots \arrow[r, "\mu_{-a}"] \arrow[d, "\mu_{-1}"'] & (-a)^{2k-1}5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] & 5^j 2^{v-t'} \arrow[d, "\mu_{-1}"'] \\
-5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] & -(-a)5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] & \cdots \arrow[r, "\mu_{-a}"] & -(-a)^{2k-1}5^j 2^{v-t'} \arrow[r, "\mu_{-a}"] & -5^j 2^{v-t'}
\end{tikzcd}$$

It follows that $\mu_a = \mu_{-1} \circ \mu_{-a}$ decomposes into two cycles on the union of the support sets of the above two cycles of $\mu_{-a}$: one is spanned by $5^j 2^{v-t'}$ and consists of the "even elements" $5^j 2^{v-t'}, (-a)^2 5^j 2^{v-t'}, (-a)^4 5^j 2^{v-t'}, \ldots$ of the upper cycle as well as the "odd elements" of the lower cycle, whereas the other is spanned by $-5^j 2^{v-t'}$ and consists of the "odd elements" of the upper and "even elements" of the lower cycle. If we let $t'$ and $j$ run through their respective range, the corresponding cycle pairs partition the set of all elements of additive order larger than $2^v/\operatorname{ord}(-a)$. Together with the observations for smaller values of $t'$ from above, we obtain a CRL-list for $\mu_a$, which can be easily checked to coincide with the one specified in Table 2.1 (we note that $t' = v - t$ in the notation of that table). ■

Now we tackle step (2) in our plan for this section, i.e., working out a CRL-list for every affine permutation $A$ of every finite primary cyclic group. A useful observation, which we explain in more detail, is that the case where $A$ has a fixed point can be reduced to the automorphism case (i.e., to Lemma 2.3.2). This idea appears in [21, proof of Lemma 4], which was concerned with cyclic groups, but it can easily be extended to general groups. We remind the reader that we write $\rho_{\mathrm{r}}$ for the right-regular representation of a group (that must be clear from context) on itself.

**Lemma 2.3.3.** *Let $G$ be a group, $b \in G$, $\alpha$ an automorphism of $G$, $A$ the affine permutation $x \mapsto x^{\alpha}b$ of $G$, and $\mathfrak{f} \in G$ a fixed point of $A$. Then*

$$A = \rho_{\mathrm{r}}(\mathfrak{f})^{-1}\alpha\rho_{\mathrm{r}}(\mathfrak{f}).$$

*In particular, $\rho_{\mathrm{r}}(\mathfrak{f})$ is a digraph isomorphism from $\Gamma_{\alpha}$ to $\Gamma_{A}$.*

*Proof.* The equality $\mathfrak{f}^{A} = \mathfrak{f}$ is equivalent to $b = (\mathfrak{f}^{-1})^{\alpha}\mathfrak{f}$. For each $x \in G$, we have

$$x^{\rho_{\mathrm{r}}(\mathfrak{f})^{-1}\alpha\rho_{\mathrm{r}}(\mathfrak{f})} = (x\mathfrak{f}^{-1})^{\alpha\rho_{\mathrm{r}}(\mathfrak{f})} = x^{\alpha}(\mathfrak{f}^{-1})^{\alpha}\mathfrak{f} = x^{\alpha}b = x^{A},$$

as required. The “In particular” statement follows because of the well-known (and easy to verify) fact that for each set $X$ and all $\psi, \psi' \in \mathrm{Sym}(X)$, the permutation $\psi$ maps $x \in X$ to $y \in X$ if and only if its $\psi'$-conjugate $(\psi')^{-1}\psi\psi'$ maps $x^{\psi'}$ to $y^{\psi'}$. ■

Lemma 2.3.3 is interesting for us because of the following elementary observation.

**Lemma 2.3.4.** *Let $X$ be a finite set, and let $\psi_1, \psi_2 \in \mathrm{Sym}(X)$ be conjugate permutations, say*

$$\psi_2 = (\psi')^{-1}\psi_1\psi'.$$

*If $\mathcal{L}$ is a CRL-list for $\psi_1$, then $\{(r^{\psi'}, l) : (r, l) \in \mathcal{L}\}$ is a CRL-list for $\psi_2$.*

*Proof.* This is clear because $(y_0, y_1, \ldots, y_{l-1})$ is a cycle of $\psi_1$ if and only if

$$(y_0^{\psi'}, y_1^{\psi'}, \ldots, y_{l-1}^{\psi'})$$

is a cycle of $\psi_2$ (see the last sentence in the proof of Lemma 2.3.3). ■

Through combining Lemmas 2.3.3 and 2.3.4, we get the next result.

**Lemma 2.3.5.** *Let $G$ be a finite group, $b \in G$, $\alpha$ an automorphism of $G$, $A$ the affine permutation $x \mapsto x^{\alpha}b$ of $G$, and $\mathfrak{f} \in G$ a fixed point of $A$. If $\mathcal{L}$ is a CRL-list of $\alpha$, then $\{(r\mathfrak{f}, l) : (r, l) \in \mathcal{L}\}$ is a CRL-list of $A$.*

We are now ready to construct a CRL-list for each affine permutation of each finite primary cyclic group.

| No. | Case for $p^v, a, b$ | elements of $\mathcal{L}(p^v, a, b)$ |
|---|---|---|
| 1 | $p > 2$,<br>$\nu_p^{(v)}(b) \geq \nu_p^{(v)}(a-1)$ | $\left(\mathfrak{r}^j p^t + \mathfrak{f}, \frac{\phi(p^{v-t})}{\gcd\left(\frac{\phi(p^v)}{\mathrm{ord}(a)}, \phi(p^{v-t})\right)}\right)$<br>for $t = 0, 1, \ldots, v$ and<br>$j = 0, 1, \ldots, \gcd\left(\frac{\phi(p^v)}{\mathrm{ord}(a)}, \phi(p^{v-t})\right) - 1$. |
| 2 | $p > 2$,<br>$\nu_p^{(v)}(b) < \nu_p^{(v)}(a-1)$ | $(j, p^{v-\nu_p^{(v)}(b)})$ for $j = 0, 1, \ldots, p^{\nu_p^{(v)}(b)} - 1$. |
| 3 | $p = 2, v \leq 2, a = 1$ | $(j, \mathrm{aord}(b))$ for $j = 0, 1, \ldots, \frac{2^v}{\mathrm{aord}(b)} - 1$. |
| 4 | $p^v = 4, a = 3, b = 0$ | $(0, 1), (1, 2), (2, 1)$. |
| 5 | $p^v = 4, a = 3, b = 2$ | $(0, 2), (1, 1), (3, 1)$. |
| 6 | $p^v = 4, a = 3, 2 \nmid b$ | $(0, 2), (2, 2)$. |
| 7 | $p = 2, v \geq 3$,<br>$\nu_2^{(v)}(b) \geq \nu_2^{(v)}(a-1)$,<br>$a \equiv 1 \pmod 4$ | $(\mathfrak{f}, 1), (2^{v-1} + \mathfrak{f}, 1)$;<br>$\left(5^j 2^t + \mathfrak{f}, \frac{2^{v-t-2}}{\gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right)}\right)$,<br>$\left(-5^j 2^t + \mathfrak{f}, \frac{2^{v-t-2}}{\gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right)}\right)$<br>for $t = 0, 1, \ldots, v-2$ and<br>$j = 0, 1, \ldots, \gcd\left(\frac{2^{v-2}}{\mathrm{ord}(a)}, 2^{v-t-2}\right) - 1$. |
| 8 | $p = 2, v \geq 3$,<br>$\nu_2^{(v)}(b) \geq \nu_2^{(v)}(a-1)$,<br>$a \equiv 3 \pmod 4$ | $(\mathfrak{f}, 1), (2^{v-1} + \mathfrak{f}, 1)$;<br>$(j \cdot \mathrm{ord}(-a) + \mathfrak{f}, 2)$ for $j = 1, 2, \ldots, \frac{2^{v-1}}{\mathrm{ord}(-a)} - 1$;<br>$\left(5^j 2^t + \mathfrak{f}, \frac{\mathrm{ord}(-a)}{2^t}\right), \left(-5^j 2^t + \mathfrak{f}, \frac{\mathrm{ord}(-a)}{2^t}\right)$<br>for $t = 0, 1, \ldots, \log_2(\mathrm{ord}(-a)) - 1$<br>and $j = 0, 1, \ldots, \frac{2^{v-2}}{\mathrm{ord}(-a)} - 1$. |
| 9 | $p = 2, v \geq 3$,<br>$\nu_2^{(v)}(b) < \nu_2^{(v)}(a-1)$,<br>$a \equiv 1 \pmod 4$ | $(j, 2^{v-\nu_2^{(v)}(b)})$ for $j = 0, 1, \ldots, 2^{\nu_2^{(v)}(b)} - 1$. |
| 10 | $p = 2, v \geq 3$,<br>$\nu_2^{(v)}(b) < \nu_2^{(v)}(a-1)$,<br>$a \equiv 3 \pmod 4$ | $(b \cdot j, 2\,\mathrm{ord}(-a))$ for $j = 1, 2, 3, 4, \ldots, \frac{2^{v-1}}{\mathrm{ord}(-a)}$. |

**Table 2.2.** CRL-lists of affine permutations of finite primary cyclic groups.

**Proposition 2.3.6.** *Let $p$ be a prime, $v \in \mathbb{N}^+$, and $a, b \in \mathbb{Z}$ with $p \nmid a$. Table 2.2 provides a CRL-list $\mathcal{L}(p^v, a, b)$ for the affine permutation $A : x \mapsto ax + b$ of $\mathbb{Z}/p^v\mathbb{Z}$, using the following conditional notations.*

- *If $p$ is odd, we denote by $\mathfrak{r}$ a fixed primitive root modulo $p^v$.*
- *If $\nu_p^{(v)}(b) \geq \nu_p^{(v)}(a-1)$, we set*

$$\mathfrak{f} := -\frac{b}{p^{\nu_p^{(v)}(a-1)}} \cdot \mathrm{inv}_{p^{v-\nu_p^{(v)}(a-1)}}\left(\frac{a-1}{p^{\nu_p^{(v)}(a-1)}}\right).$$

*Proof.* First, we observe that if $\nu_p^{(v)}(b) \geq \nu_p^{(v)}(a-1)$, then $\mathfrak{f}$ is a fixed point of $A$. Indeed, $x \in \mathbb{Z}/p^v\mathbb{Z}$ is a fixed point of $A$ if and only if

$$\begin{aligned}
&ax + b \equiv x \pmod{p^v} \Leftrightarrow (a-1)x \equiv -b \pmod{p^v} \\
&\Leftrightarrow \frac{a-1}{p^{\nu_p^{(v)}(a-1)}}x \equiv -\frac{b}{p^{\nu_p^{(v)}(a-1)}} \pmod{p^{v-\nu_p^{(v)}(a-1)}} \\
&\Leftrightarrow x \equiv -\frac{b}{p^{\nu_p^{(v)}(a-1)}} \cdot \mathrm{inv}_{p^{v-\nu_p^{(v)}(a-1)}}\left(\frac{a-1}{p^{\nu_p^{(v)}(a-1)}}\right) = \mathfrak{f} \pmod{p^{v-\nu_p^{(v)}(a-1)}}.
\end{aligned}$$

The form of the CRL-list for $A$ specified in cases 1, 7 and 8 in Table 2.2 thus follows from Lemma 2.3.5 and the corresponding CRL-list for $\mu_a$, read off from Table 2.1. Moreover, cases 3–6 in Table 2.2 are easy to check separately. It remains to justify the specified CRL-list in cases 2, 9 and 10 in Table 2.2, which we do now.

- Case 2: We note that in this case, $a \equiv 1 \pmod{p}$ necessarily. The units modulo $p^v$ that are congruent to 1 modulo $p$ form the unique, cyclic Sylow $p$-subgroup of $(\mathbb{Z}/p^v\mathbb{Z})^*$, of order $p^{v-1}$. For each $t \in \{0, 1, \ldots, v-1\}$, the unit $1 + p^{v-t}$ has order $p^t$, and thus all order $p^t$ units modulo $p^v$ are powers of $1 + p^{v-t}$ with exponent coprime to $p$ and vice versa. Therefore, using the "In particular" statement of Lemma 2.3.1 and that $\mathrm{ord}(A)$ is a power of $p$, we may assume without loss of generality that $a = 1 + p^{v-t}$ for some $t \in \{0, 1 \ldots, v-1\}$. We observe that $v - t = \nu_p^{(v)}(a-1)$, and thus $v - t > \nu_p^{(v)}(b)$ by the case assumptions. For each $x \in \mathbb{Z}/p^v\mathbb{Z}$, we have $A(x) = ax + b = (1 + p^{v-t})x + b \equiv x \pmod{p^{\nu_p^{(v)}(b)}}$. Hence, the elements $0, 1, \ldots, p^{\nu_p^{(v)}(b)} - 1$ lie on pairwise distinct cycles of $A$. On the other hand, by [15, Table 3], $A$ has exactly $p^v/\,\mathrm{aord}(b) = p^{\nu_p^{(v)}(b)}$ cycles, each of length $\mathrm{aord}(b) = p^{v-\nu_p^{(v)}(b)}$, so the said elements are representatives for all cycles of $A$ and $\{(j, p^{v-\nu_p^{(v)}(b)}) : j = 0, 1, \ldots, p^{\nu_p^{(v)}(b)} - 1\}$ is a CRL-list of $A$, as required.
- Case 9: This can be dealt with similarly to case 2. We observe that the unit $5 = 1 + 2^2$ has multiplicative order $2^{v-2}$ and generates an index 2 cyclic subgroup of $(\mathbb{Z}/2^v\mathbb{Z})^*$, which consists precisely of those units that are congruent to 1 modulo 4. For each $t \in \{0, 1, \ldots, v-2\}$, the unit $1 + 2^{v-t}$ lies in this subgroup and has order $2^t$, so any unit of order $2^t$ that is congruent to 1 modulo 4 is a power of $1 + 2^{v-t}$ with odd exponent and vice versa. Using the "In particular" statement of Lemma 2.3.1 and that $\mathrm{ord}(A)$ is a power of 2, we may assume without loss of generality that $a = 1 + 2^{v-t}$ for some $t \in \{0, 1, \ldots, v-2\}$, and the remainder of this argument is analogous to the one for case 2, resulting in $\{(j, 2^{v-\nu_2^{(v)}(b)}) : j = 0, 1, \ldots, 2^{\nu_2^{(v)}(b)} - 1\}$ being a CRL-list of $A$.
- Case 10: Due to $-a \equiv 1 \pmod{4}$, we may assume without loss of generality that $-a = 1 + 2^{v-t}$ for some $t \in \{0, 1, \ldots, v-2\}$ (see the argument for case 9). Let $A'$

be the affine function $x \mapsto -x+b$ of $\mathbb{Z}/2^{v-t}\mathbb{Z}$. For each $x \in \mathbb{Z}/2^v\mathbb{Z}$, we have $A(x) = -(1+2^{v-t})x+b \equiv -x+b \pmod{2^{v-t}}$. This means that elements of $\mathbb{Z}/2^{v-t}\mathbb{Z}$ that lie on different cycles of $A'$ also lie on different cycles of $A$ (we remind the reader that $\mathbb{Z}/2^{v-t}\mathbb{Z} \subseteq \mathbb{Z}/2^v\mathbb{Z}$ by our convention on the underlying set of $\mathbb{Z}/m\mathbb{Z}$ stated at the beginning of this section). Now, $A'$ is an involution without fixed points (because $2 \nmid b$) and thus consists of $2^{v-t-1}$ transpositions. But by [15, Table 4], $A$ has exactly $2^{v-t-1}$ cycles. Indeed, if $a = -5^n$, then $2^t = \mathrm{ord}(-a) = 2^{v-2-\nu_2^{(v-2)}(n)}$, and therefore $t = v-2-\nu_2^{(v-2)}(n)$, whence the cycle number $2^{1+\nu_2^{(v-2)}(n)}$ specified in [15, Table 4] equals $2^{v-t-1}$. Therefore, any set of representatives for the cycles of $A'$ on $\mathbb{Z}/2^{v-t}\mathbb{Z}$ is also a set of representatives for the cycles of $A$ on $\mathbb{Z}/2^v\mathbb{Z}$, all of which are of length $2^{t+1}$ by [15, Table 4]. Thus, in order to find a CRL-list for $A$, it suffices to find cycle representatives for $A'$. To that end, we first assume that $b=1$. Then every cycle (i.e., transposition) of $A'$ on $\mathbb{Z}/2^{v-t}\mathbb{Z}$ contains exactly one element from the "left half" $\{1,2,\ldots,2^{v-t-1}\}$ and one from the "right half" $\{2^{v-t-1}+1, 2^{v-t-1}+2, \ldots, 2^{v-t}-1, 2^{v-t} \equiv 0\}$, and the elements 0 and 1 lie on the same cycle. It follows that $\{1,2,3,4,\ldots,2^{v-t-1}\}$ is a set of representatives for the cycles of $A'$, and this matches with the CRL-list for $A$ specified in Table 2.2. For general $b$, we observe that

$$A' = (x \mapsto -x+b) = (x \mapsto b^{-1}x) \cdot (x \mapsto -x+1) \cdot (x \mapsto bx),$$

whence Lemma 2.3.4 allows us to conclude that

$$b \cdot \{1,2,3,4,\ldots,2^{v-t-1}\} = \{b, 2b, 3b, 4b, \ldots, 2^{v-t-1}b\}$$

is a set of representatives for the cycles of $A'$, as required. ■

Now that we know a CRL-list for each affine permutation of each finite *primary* cyclic group, let us discuss how to deal with general finite cyclic groups. Through identifying the group $\mathbb{Z}/m\mathbb{Z}$ with the direct product $\prod_{p|m} \mathbb{Z}/p^{\nu_p(m)}\mathbb{Z}$ via the Chinese remainder theorem, we can view any affine permutation $A: x \mapsto ax+b$ of $\mathbb{Z}/m\mathbb{Z}$ as the "function tensor product" $\bigotimes_{p|m} A_p$, where $A_p$ is the *reduction of* $A$ *modulo* $p^{\nu_p(m)}$, i.e., the affine permutation $x \mapsto ax+b$ of $\mathbb{Z}/p^{\nu_p(m)}\mathbb{Z}$, as introduced in Remark 2.1.2. That is, $A$ becomes the component-wise application of its reductions $A_p$ under this identification. This leads to the following, more general problem, which we solve next.

**Problem 2.3.7.** *Given finite sets* $X_1, X_2, \ldots, X_n$, *permutations* $\psi_j \in \mathrm{Sym}(X_j)$ *for* $j = 1,2,\ldots,n$, *and a CRL-list* $\mathcal{L}_j$ *of* $\psi_j$ *for* $j = 1,2,\ldots,n$, *construct a CRL-list* $\mathcal{L}$ *of* $\psi := \bigotimes_{j=1}^n \psi_j \in \mathrm{Sym}(\prod_{j=1}^n X_j)$.

For the rest of this section, we use the notation fixed in Problem 2.3.7. We denote by $\mathcal{L}_j^{(1)} \subseteq X_j$ the set of first entries of the pairs in $\mathcal{L}_j$ (i.e., the set of cycle representatives of $\psi_j$ exhibited by $\mathcal{L}_j$), and for $r \in \mathcal{L}_j^{(1)}$, we denote by $r^{\langle \psi_j \rangle}$ the orbit of $r$

under the action of the permutation group $\langle\psi_j\rangle$ (i.e., the set of points on the $\psi_j$-cycle of $r$).

For each $\vec{r} = (r_1, r_2, \dots, r_n) \in \prod_{j=1}^{n} \mathcal{L}_j^{(1)}$, we set $B_{\vec{r}} := \prod_{j=1}^{n} r_j^{\langle\psi_j\rangle}$. These sets $B_{\vec{r}}$ form a partition of $\prod_{j=1}^{n} X_j$, and each set $B_{\vec{r}}$ is a union of cycles of $\psi$. Therefore, it suffices to find a CRL-list $\mathcal{L}_{\vec{r}}$ of the restriction $\psi_{|B_{\vec{r}}}$ for each $\vec{r}$, then set $\mathcal{L} := \bigcup_{\vec{r}} \mathcal{L}_{\vec{r}}$.

Let us thus assume that $\vec{r}$ is fixed. For $j = 1, 2, \dots, n$, we denote by $l_j = l_j(\vec{r})$ the $\psi_j$-cycle length of $r_j$. Every cycle of $\psi$ on $B_{\vec{r}}$ has length $l_{\vec{r}} := \operatorname{lcm}(l_1, l_2, \dots, l_n)$, and there are exactly $(\prod_{j=1}^{n} l_j)/l_{\vec{r}}$ such cycles (see also [86, Lemma 2.1]). It remains to find representatives for them.

We consider the bijection

$$\iota_{\vec{r}} : \prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z} \to B_{\vec{r}}, \quad (k_1, k_2, \dots, k_n) \mapsto (\psi_1^{k_1}(r_1), \psi_2^{k_2}(r_2), \dots, \psi_n^{k_n}(r_n)).$$

If we identify $B_{\vec{r}}$ with $\prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}$ via this bijection, then the action of $\psi$ on $B_{\vec{r}}$ turns into that of the function

$$\mathfrak{s}_{\vec{r}} : \prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z} \to \prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}, \quad (k_1, k_2, \dots, k_n) \mapsto (k_1 + 1, k_2 + 1, \dots, k_n + 1),$$

each displayed addition being modulo the corresponding $l_j$, of course. So it suffices to find a set of representatives for the cycles of $\mathfrak{s}_{\vec{r}}$ on $\prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}$, then map that set under $\iota_{\vec{r}}$. In order to describe a particular set of cycle representatives for $\mathfrak{s}_{\vec{r}}$ neatly, we introduce the following auxiliary concepts.

**Definition 2.3.8.** We denote by $\pi(l_{\vec{r}})$ the set of all prime divisors of $l_{\vec{r}}$.

(1) A function $\mathcal{I} : \pi(l_{\vec{r}}) \to \{1, 2, \dots, n\}$ is an *$\vec{r}$-admissible indexing function* if for each $p \in \pi(l_{\vec{r}})$ we have $\nu_p(l_{\mathcal{I}(p)}) = \max\{\nu_p(l_j) : j = 1, 2, \dots, n\}$.

(2) If $\mathcal{I}$ is an $\vec{r}$-admissible indexing function, then a tuple

$$(k_1, k_2, \dots, k_n) \in \prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}$$

is *$\mathcal{I}$-good* if $k_{\mathcal{I}(p)} \equiv 0 \pmod{p^{\nu_p(l_{\mathcal{I}(p)})}}$ for each $p \in \pi(l_{\vec{r}})$.

(3) For each $\vec{r}$-admissible indexing function $\mathcal{I}$, we denote by $\operatorname{Good}_{\vec{r}}(\mathcal{I})$ the set of all $\mathcal{I}$-good tuples in $\prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}$.

The following result solves Problem 2.3.7.

**Proposition 2.3.9.** *Let $\mathcal{I}$ be an $\vec{r}$-admissible indexing function. Then* $\operatorname{Good}_{\vec{r}}(\mathcal{I})$ *is a set of representatives for the cycles of $\mathfrak{s}_{\vec{r}}$ on $\prod_{j=1}^{n} \mathbb{Z}/l_j\mathbb{Z}$. Equivalently,*

$$\iota_{\vec{r}}(\operatorname{Good}_{\vec{r}}(\mathcal{I})) \times \{l_{\vec{r}}\}$$

*is a CRL-list for $\psi_{|B_{\vec{r}}}$, and so*

$$\bigcup_{\vec{r}\in\prod_{j=1}^{n}\mathcal{L}_j^{(1)}} (\iota_{\vec{r}}(\mathrm{Good}_{\vec{r}}(\mathcal{I}))\times\{l_{\vec{r}}\})$$

*is a CRL-list for $\psi$.*

*Proof.* By definition and the Chinese remainder theorem, the number of $\mathcal{I}$-good tuples in $\prod_{j=1}^{n}\mathbb{Z}/l_j\mathbb{Z}$ is

$$\frac{\prod_{j=1}^{n} l_j}{\prod_{p\in\pi(l_{\vec{r}})} p^{\nu_p(l_{\mathcal{I}(p)})}} = \frac{|\prod_{j=1}^{n}\mathbb{Z}/l_j\mathbb{Z}|}{l_{\vec{r}}},$$

which is also the number of cycles of $\mathfrak{s}_{\vec{r}}$ on $\prod_{j=1}^{n}\mathbb{Z}/l_j\mathbb{Z}$. Hence, it suffices to show that different $\mathcal{I}$-good tuples lie on distinct cycles of $\mathfrak{s}_{\vec{r}}$. Let $\vec{k}=(k_1,k_2,\ldots,k_n)$ and $\vec{k'}=(k'_1,k'_2,\ldots,k'_n)$ be $\mathcal{I}$-good tuples that lie on the same cycle of $\mathfrak{s}_{\vec{r}}$. This means that there is a $t\in\mathbb{Z}$ such that $k_j+t\equiv k'_j \pmod{l_j}$ for each $j=1,2,\ldots,n$. Now, let $p\in\pi(l_{\vec{r}})$. Since $t\equiv k'_{\mathcal{I}(p)}-k_{\mathcal{I}(p)} \pmod{l_{\mathcal{I}(p)}}$ and $\vec{k},\vec{k'}$ are $\mathcal{I}$-good, it follows that $t\equiv 0 \pmod{p^{\nu_p(l_{\mathcal{I}(p)})}}$. Because this holds for every $p\in\pi(l_{\vec{r}})$, we conclude that

$$\mathrm{lcm}(l_1,l_2,\ldots,l_n)=l_{\vec{r}}=\prod_{p\in\pi(l_{\vec{r}})} p^{\nu_p(l_{\mathcal{I}(p)})}$$

divides $t$, whence $k_j\equiv k'_j \pmod{l_j}$ for each $j=1,2,\ldots,n$. This means that $\vec{k}=\vec{k'}$, as required. ■

## 2.4 Affine discrete logarithms and cycle lengths

Let $m\geq 1$ be an integer, and let $a,b\in\mathbb{Z}/m\mathbb{Z}$ with $\gcd(a,m)=1$. We consider the affine permutation $A: x\mapsto ax+b$ of $\mathbb{Z}/m\mathbb{Z}$. Given $x,y\in\mathbb{Z}/m\mathbb{Z}$, we set

$$\log_A^{(m)}(x,y):=\begin{cases}\infty, & \text{if there is no } k\in\mathbb{Z} \text{ with } A^k(x)=y,\\ \min\{k\in\mathbb{N}_0 : A^k(x)=y\}, & \text{otherwise.}\end{cases}$$

In this short section, we discuss how to compute $\log_A^{(m)}(x,y)$ and the cycle length of $x$ under $A$, which is closely related, as it is the minimal *positive* integer $k$ such that $A^k(x)=x$ (while $\log_A^{(m)}(x,x)=0$). It is not surprising that modular discrete logarithms play an important role in this, because they are a special case of the notion $\log_A^{(m)}(x,y)$. Namely, the discrete logarithm of $x\in(\mathbb{Z}/m\mathbb{Z})^*$ modulo $m$ with base $a\in(\mathbb{Z}/m\mathbb{Z})^*$, written $\log_a^{(m)}(x)$, is equal to $\log_{\mu_a}^{(m)}(1,x)$.

In order to discuss the computational details, we make a case distinction.

- First, we assume that $a \equiv 1 \pmod{m}$, a simple case for which no discrete logarithms need to be computed. Indeed, one then has $A^k(x) = x + kb \equiv y \pmod{m}$ if and only if $kb \equiv y - x \pmod{m}$. That last congruence is solvable in $k$ if and only if $\gcd(b, m) \mid y - x$, in which case the congruence is equivalent to

$$\frac{b}{\gcd(b,m)} k \equiv \frac{y-x}{\gcd(b,m)} \left(\mathrm{mod}\ \frac{m}{\gcd(b,m)}\right) \tag{2.7}$$

and has the minimal solution

$$\left(\frac{y-x}{\gcd(b,m)} \cdot \mathrm{inv}_{m/\gcd(b,m)}\left(\frac{b}{\gcd(b,m)}\right)\right) \bmod \frac{m}{\gcd(b,m)} = \log_A^{(m)}(x,y).$$

We note that in case $x = y$, the minimal *positive* solution of congruence (2.7), and thus the cycle length of $x$ under $A$ modulo $m$, is $m/\gcd(b,m)$.

- Now we assume that $a \not\equiv 1 \pmod{m}$. Then $m > 1$, and $a \not\equiv 0 \pmod{m}$ due to $\gcd(a,m) = 1$, so we may assume that as an integer, $a > 1$. We have $A^k(x) = y$ if and only if

$$\begin{aligned} a^k x + \frac{a^k - 1}{a-1} b &\equiv y \pmod{m} \\ \Leftrightarrow a^k(a-1)x + (a^k - 1)b &\equiv (a-1)y \pmod{(a-1)m} \\ \Leftrightarrow a^k((a-1)x + b) &\equiv (a-1)y + b \pmod{(a-1)m}. \end{aligned} \tag{2.8}$$

In order for congruence (2.8) to be solvable in $k$, it is necessary that $(a-1)x + b$ and $(a-1)y + b$ have the same additive order modulo $(a-1)m$, i.e., that

$$\gcd((a-1)x + b, (a-1)m) = \gcd((a-1)y + b, (a-1)m) =: \mathfrak{d}. \tag{2.9}$$

If condition (2.9) is satisfied, then congruence (2.8) is equivalent to

$$a^k \cdot \frac{(a-1)x+b}{\mathfrak{d}} \equiv \frac{(a-1)y+b}{\mathfrak{d}} \left(\mathrm{mod}\ \frac{(a-1)m}{\mathfrak{d}}\right),$$

i.e., to

$$a^k \equiv \frac{(a-1)y+b}{\mathfrak{d}} \cdot \mathrm{inv}_{(a-1)m/\mathfrak{d}}\left(\frac{(a-1)x+b}{\mathfrak{d}}\right) \left(\mathrm{mod}\ \frac{(a-1)m}{\mathfrak{d}}\right), \tag{2.10}$$

which shows that

$$\log_A^{(m)}(x,y) = \log_a^{((a-1)m/\mathfrak{d})}\left(\frac{(a-1)y+b}{\mathfrak{d}} \cdot \mathrm{inv}_{(a-1)m/\mathfrak{d}}\left(\frac{(a-1)x+b}{\mathfrak{d}}\right)\right),$$

with the convention that $\log_a^{(m)}(x) = \infty$ if $x$ is not a power of $a$ modulo $m$. If $x = y$, then the right-hand side in congruence (2.10) simplifies to 1, whence the cycle length of $x$ under $A$ equals the multiplicative order of $a$ modulo $(a-1)m/\mathfrak{d}$.

The upshot of this discussion is that $\log_A^{(m)}(x, y)$ and the cycle length of $x$ under $A$ modulo $m$ can be computed efficiently if one has efficient algorithms for computing discrete logarithms and multiplicative orders of units in $(\mathbb{Z}/m\mathbb{Z})^*$. Hence, $\log_A^{(m)}(x,y)$ can be computed efficiently on a quantum computer. Indeed, Shor showed that such computers admit efficient algorithms both for computing discrete logarithms and for integer factorization [68], the latter of which is sufficient to compute element orders in $(\mathbb{Z}/m\mathbb{Z})^*$ efficiently; in fact, all one needs for that is an explicit factorization of the Euler totient function value $\phi(m)$, see also the proof of Lemma 5.1.6 (2).