Classification of finite group automorphisms with a large cycle II

Alexander Bors*

March 4, 2016

Abstract

In a previous paper, the author classified the pairs (G, α) where G is a finite group and α an automorphism of G having a cycle of length *greater than* $\frac{1}{2}|G|$. In this paper, we extend this classification to the case where α has a cycle of length *equal to* $\frac{1}{2}|G|$ and show some applications of the classification: We discuss an algorithm for listing the pairs (G, α) where the largest cycle length of α equals $\rho|G|$ on input any rational $\rho \in \left(\frac{1}{2}, 1\right]$, and we prove that the set of cycle length fractions of finite group automorphisms is not dense in $[0, 1]$.

1 Introduction

1.1 Motivation and main results

Finite groups satisfying certain "extreme" quantitative conditions have been studied for a long time. One aspect investigated by various authors is the impact on the group structure of the maximum fraction of group elements mapped to their e-th power by a single automorphism for some fixed exponent $e \in \mathbb{Z}$, particularly $e = -1, 2, 3$, see for instance [Miller, 1929; Liebeck, 1973; MacHale, 1975; Potter, 1988; Hegarty, 2003; Hegarty, 2009]. In [Bors, 2016+], we began to study the impact of another maximum fraction of group elements showing a certain behavior under an automorphism, namely the maximum fraction of elements lying on a single automorphism cycle. For the readers' convenience, we briefly recall some notation and terminology introduced there:

Notation 1.1.1. *1. Let X be a finite set, ψ a permutation on X.*

*University of Salzburg, Mathematics Department, Hellbrunner Straße 34, 5020 Salzburg, Austria.
E-mail: alexander.bors@sbg.ac.at
The author is supported by the Austrian Science Fund (FWF): Project F5504-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".
2010 *Mathematics Subject Classification*: 20B25, 20D45, 20G40, 20K01, 20K30.
Key words and phrases: Finite groups, Automorphisms, Cycle structure, Large cycles.

(a) $\Lambda(\psi)$ *denotes the largest length of one of the disjoint cycles into which* ψ *decomposes.*

(b) $\lambda(\psi) := \frac{1}{|X|}\Lambda(\psi)$*, the largest cycle length fraction of* ψ*.*

2. *Let* G *be a finite group.*

   (a) $\Lambda(G) := \max_{\alpha\in\mathrm{Aut}(G)} \Lambda(\alpha)$*, the maximum possible cycle length of an automorphism of* G*.*

   (b) $\lambda(G) := \frac{1}{|G|}\Lambda(G)$*, the maximum possible cycle length fraction of an automorphism of* G*.*

Since our problem is about studying finite groups together with the actions of automorphisms on them, we introduced the following terminology, motivated by the well-studied concept of a "finite dynamical system" (see, for instance, [Hernández-Toledo, 2005]):

Definition 1.1.2. *1. A* ***finite dynamical group (FDG)*** *is a finite group* G *together with an endomorphism* φ *of* G*.*

2. *An FDG* (G,φ) *is called* ***periodic*** *if and only if* φ *is an automorphism of* G*, and the* λ*- (resp.* Λ*-)value of a periodic FDG* (G,α) *is understood as the* λ*- (resp.* Λ*-)value of* α*.*

3. *A periodic FDG* (G,α) *is called* ***λ-maximal*** *if and only if* $\lambda(\alpha)=\lambda(G)$*.*

4. *An FDG* (G,φ) *is called* ***(elementary) abelian*** *if and only if* G *is (elementary) abelian,* ***nonabelian*** *if and only if it is not abelian, and for a prime* p*,* (G,φ) *is called a* ***p-FDG*** *if and only if* G *is a* p*-group.*

5. *For FDGs* $(G_1,\varphi_1),\ldots,(G_r,\varphi_r)$*, their* ***product*** $\prod_{i=1}^r (G_i,\varphi_i)$ *is defined as the FDG* $(\prod_{i=1}^r G_i, \prod_{i=1}^r \varphi_i)$*, where* $\prod_{i=1}^r \varphi_i$ *is the endomorphism of* $\prod_{i=1}^r G_i$ *sending* $(g_1,\ldots,g_r)\mapsto(\varphi_1(g_1),\ldots,\varphi_r(g_r))$*.*

If (G,φ) and (H,ψ) are FDGs, an *FDG isomorphism* between them is a group isomorphism $f: G\to H$ such that $f\circ\varphi=\psi\circ f$. The main result of the prequel to the present paper was a classification, up to isomorphism of FDGs, of those periodic FDGs (G,α) such that $\lambda(\alpha)>\frac{1}{2}$, see [Bors, 2016+, Corollary 1.1.8]. In other words, we completely understand those finite group automorphisms that have a cycle of length more than half the group order. It turned out that in such a case, the group always is abelian, whereas we observed that there exist periodic nonabelian FDGs (G,α) with $\lambda(\alpha)=\frac{1}{2}$.

In this paper, we will classify all periodic FDGs with λ-value equal to $\frac{1}{2}$ (including the abelian ones), the classification being given in Theorem 1.1.4 below. The following notation and terminology will be used in the formulation of the theorem:

Definition 1.1.3. *1. For a positive integer* n*, set* $\mathrm{Z}_n := \{0,\ldots,n-1\}$*, the canonical set of representatives of integer residue classes modulo* n*.*

2. *Say that an integer* m *is* ***n-Knuthian*** *if and only if* $m\equiv 1 \pmod{p}$ *for every prime divisor* p *of* n*, and additionally* $m\equiv 1 \pmod 4$ *if* $4\mid n$*.*

The terminology in Definition 1.1.3(2) is motivated by Knuth's characterization of affine maps of $\mathbb{Z}/n\mathbb{Z}$ that are permutations consisting of one n-cycle, see [Knuth, 1998, Section 3.2.1.2, Theorem A].

Theorem 1.1.4. *The following is the complete (up to isomorphism) list of periodic FDGs whose λ-value equals $\frac{1}{2}$. Except for the FDGs in points 4 and 5, they are all λ-maximal.*

1. *$\mathbb{Z}/2\mathbb{Z}$ with the identity.*
2. *$\mathbb{Z}/4\mathbb{Z}$ with multiplication by 3.*
3. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \langle v_1, v_2 \mid v_1^2 = v_2^4 = 1, [v_1, v_2] = 1\rangle$ with the automorphism sending $v_1 \mapsto v_1 v_2^2$ and $v_2 \mapsto v_1 v_2$.*
4. *$(\mathbb{Z}/2\mathbb{Z})^2$ with the automorphism given by the (Frobenius) companion matrix of $(X-1)^2 \in \mathbb{F}_2[X]$ (see also Subsection 1.3).*
5. *$(\mathbb{Z}/2\mathbb{Z})^3$ with the automorphism given by the companion matrix of $(X-1)^3 \in \mathbb{F}_2[X]$.*
6. *$(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ with the product of the automorphism of $(\mathbb{Z}/2\mathbb{Z})^2$ given by the companion matrix of the polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$ with multiplication by 2 on $\mathbb{Z}/3\mathbb{Z}$.*
7. *$\mathrm{D}_{2n} = \langle r, x \mid r^n = x^2 = 1, xrx^{-1} = r^{-1}\rangle$ with the automorphism sending $r \mapsto r^m, x \mapsto xr$ for $n \geq 3$ and $m \in \mathrm{Z}_n$ being n-Knuthian. For each n, any two such FDGs arising from different choices of m are nonisomorphic.*
8. *$\mathrm{Dic}_{2n} = \langle r, x \mid r^n = 1, x^2 = r^{\frac{n}{2}}, xrx^{-1} = r^{-1}\rangle$ with the automorphism sending $r \mapsto r^m, x \mapsto xr$ for even $n \geq 4$ and $m \in \mathrm{Z}_n$ being n-Knuthian. For each n, any two such FDGs arising from different choices of m are nonisomorphic.*
9. *$\mathrm{D}((\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/o\mathbb{Z}) = \langle r_1, r_2, r, x \mid r_1^2 = r_2^2 = r^o = [r_1, r_2] = [r_1, r] = [r_2, r] = 1, x^2 = 1, [r_1, x] = [r_2, x] = 1, xrx^{-1} = r^{-1}\rangle$ with the automorphism sending $r_1 \mapsto r_2, r_2 \mapsto r_1, r \mapsto r^m, x \mapsto xr_1 r$ for odd $o \geq 3$ and $m \in \mathrm{Z}_o$ being o-Knuthian. For each o, any two such FDGs arising from different choices of m are nonisomorphic.*
10. *$\mathrm{Dic}((\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/o\mathbb{Z}) = \langle r_1, r_2, r, x \mid r_1^2 = r_2^2 = r^o = [r_1, r_2] = [r_1, r] = [r_2, r] = 1, x^2 = r_1 r_2, [r_1, x] = [r_2, x] = 1, xrx^{-1} = r^{-1}\rangle$ with the automorphism sending $r_1 \mapsto r_2, r_2 \mapsto r_1, r \mapsto r^m, x \mapsto xr_1 r$ for odd $o \geq 3$ and $m \in \mathrm{Z}_o$ being o-Knuthian. For each o, any two such FDGs arising from different choices of m are nonisomorphic.*

So the list consists of six particular abelian FDGs and four infinite classes of nonabelian FDGs, over dihedral groups, dicyclic groups and a kind of generalized dihedral and generalized dicyclic groups (as the three generalized dicyclic groups over $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/o\mathbb{Z}$ associated with each of its order 2 elements are isomorphic, we suppress the element in our notation). Apart from Theorem 1.1.4, we will also discuss two applications of our previous classification result, [Bors, 2016+, Corollary 1.1.8]:

1. Firstly, we will discuss an algorithm which, on input a rational number $\rho \in \left[\frac{1}{2}, 1\right]$, outputs an explicit list of the (isomorphism types of) *abelian* FDGs (G, α) such that $\lambda(\alpha) = \rho$ (note that for $\rho > \frac{1}{2}$, these are *all* FDGs (G, α) with $\lambda(\alpha) = \rho$).
2. Secondly, we will prove the following theorem about some topological properties of the set of possible largest automorphism cycle length fractions:

   Theorem 1.1.5. *Consider the image* $\mathrm{im}(\lambda) \subseteq (0, 1]$ *of the function* λ *defined on the class of periodic FDGs, and set*

   $$\rho_0 := \frac{4}{5} \cdot \prod_p (1 - \frac{1}{2^p}) = 0.504307524\ldots,$$

   where the index p *runs over all primes. Then the following hold:*

   (a) $\mathrm{im}(\lambda)$ *has no isolated points. More precisely, for all* $\rho \in \mathrm{im}(\lambda)$*, there exists a sequence* $((G_n, \alpha_n))_{n\geq 0}$ *of periodic FDGs such that* $\lambda(\alpha_n) < \rho$ *for all* $n \in \mathbb{N}$ *and* $\lim_{n\to\infty} \lambda(\alpha_n) = \rho$.

   (b) $\mathrm{im}(\lambda)$ *is not dense in* $(0, 1]$*. More precisely,* $\mathrm{im}(\lambda) \cap \left(\frac{1}{2}, \rho_0\right] = \emptyset$.

   (c) $\mathrm{im}(\lambda)$ *is not closed in* $(0, 1]$*. More precisely,* $\inf(\mathrm{im}(\lambda) \cap (\rho_0, 1)) = \rho_0$*, while* ρ_0 *itself is not an element of* $\mathrm{im}(\lambda)$*, by point (b) of this theorem.*

1.2 Outline of the paper

Section 2 "prepares the ground" for the proof of Theorems 1.1.4 and 1.1.5. In Subsection 2.1, for the readers' convenience, we give an overview on results from [Bors, 2016+] which we will need. The aim of Subsection 2.2 is to classify the affine maps (see the beginning of Subsubsection 2.1.2 for the definition of this concept) on finite abelian groups moving all elements in one large cycle, an auxiliary result for Theorem 1.1.4. Finally, Subsection 2.3 consists of the discussion of the aforementioned algorithm for explicit classification of periodic FDGs (G, α) with $\lambda(\alpha) = \rho$.

Section 3 consists of the proofs of Theorems 1.1.4 (Subsection 3.1) and 1.1.5 (Subsection 3.2). We give some concluding remarks in Section 4.

As in [Bors, 2016+], we remark that at some points, we have used GAP [The GAP group, 2014] to check a few statements. The source code is available from the author upon request.

1.3 Notation

By $\mathbb{N}$, we denote the set of natural numbers (including 0), and by $\mathbb{N}^+$ the set of positive integers. $\mathbb{P}$ denotes the set of prime numbers. The image of a set M under a function f is denoted by $f[M]$, the restriction of f to M by $f_{|M}$, and the domain of f by $\mathrm{dom}(f)$.

For a group G and an element $g \in G$, the centralizer of g in G is denoted by $\mathrm{C}_G(g)$. The order of a group element g is denoted by $\mathrm{ord}(g)$; the group itself is suppressed in this notation, but is usually clear from the context. In the proof of

Theorem 2.2.2 below, we also use ord to denote the order of a polynomial in the sense of [Lidl, Niederreiter, 1997, Definition 3.2]

Euler's totient function is denoted by ϕ, which is to be distinguished from the symbol φ used for group endomorphisms. For a prime p and $a \in \mathbb{N}^+$, we denote by $\nu_p(a)$ the p-adic valuation of a. For a prime power q, the finite field with q elements is denoted by $\mathbb{F}_q$. For a commutative ring R and $n \in \mathbb{N}^+$, we denote by R^* the multiplicative group of units in R, and by $\mathrm{Mat}_n(R)$ the ring of $(n \times n)$-matrices over R. For a monic polynomial $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ over a field K, we denote the Frobenius companion matrix of $P(X)$, i.e., the $(n \times n)$-matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_n(K),$$

by $\mathrm{M}(P(X))$. The algebraic closure of a field K is denoted by $\overline{K}$, and the (natural) exponential function $\mathbb{R} \to \mathbb{R}$ by exp.

2 Preparation for the proofs of Theorems 1.1.4 and 1.1.5

2.1 Overview on results from "Classification of finite group automorphisms with a large cycle"

2.1.1 Classification

According to our classification result [Bors, 2016+, Corollary 1.1.8], there are three types of "basic building blocks" for periodic FDGs (G, α) with $\lambda(\alpha) > \frac{1}{2}$ (meaning that every such FDG is a product of them):

1. Primary cyclic groups $\mathbb{Z}/p^k\mathbb{Z}$ for $p > 2$ prime and $k \in \mathbb{N}$, together with the multiplication by some primitive root modulo p^k. They have Λ-value $\phi(p^k) = p^{k-1}(p-1)$ and λ-value $1 - \frac{1}{p}$.
2. Elementary abelian groups $(\mathbb{Z}/p\mathbb{Z})^d$, p prime and $d \in \mathbb{N}^+$ such that $(p, d) \neq (2, 1)$, together with an automorphism moving all nontrivial elements in one cycle (which are just the automorphisms represented, with respect to some $\mathbb{F}_p$-basis, by $\mathrm{M}(P(X))$ for some monic primitive irreducible polynomial $P(X) \in \mathbb{F}_p[X]$ of degree d). They have Λ-value $p^d - 1$ and λ-value $1 - \frac{1}{p^d}$, and they will hitherto be referred to as the "standard" elementary abelian FDGs.
3. "Exceptional" elementary abelian FDGs of dimension 2. These consist of the group $(\mathbb{Z}/p\mathbb{Z})^2$ for some prime $p > 2$, together with an automorphism, given, with respect to some basis, by $\mathrm{M}((X - g)^2)$, where g is a generator of $\mathbb{F}_p^*$. The Λ-value of such an FDG equals $p(p-1)$, and the λ-value $1 - \frac{1}{p}$.

The only other two possibilities for such FDGs, apart from the building blocks, are the following:

4. Products of building blocks of type 2, all with $p = 2$, where the Λ-values $2^{d_i} - 1$ are pairwise coprime (which is equivalent to the pairwise coprimality of the d_i), and $\prod_{i=1}^{r}(1 - \frac{1}{2^{d_i}}) > \frac{1}{2}$. The λ-value of such an FDG then equals $\prod_{i=1}^{r}(1 - \frac{1}{2^{d_i}})$.
5. A product of one FDG as in the previous point with one building block of odd order such that the Λ-values of the two factors are coprime and their product is greater than half the product order. The λ-value of such an FDG is the product of the λ-values of the two factors.

2.1.2 Affine maps and transfer ideas

For some results, it turned out to be useful to generalize the notion of a group endomorphism in the following way: For a group G, an element $g_0 \in G$ and an endomorphism φ of G, the map $G \to G, g \mapsto g_0\varphi(g)$, is the *(left-)affine map of G with respect to g_0 and φ*, denoted by $\mathrm{A}_{g_0,\varphi}$. It is bijective if and only if φ is an automorphism of G. We denoted the group of bijective affine maps of G, which is canonically isomorphic with the holomorph of G, $\mathrm{Hol}(G)$, by $\mathrm{Aff}(G)$, and set $\Lambda_{\mathrm{aff}}(G) := \max_{A\in\mathrm{Aff}(G)} \Lambda(A)$ and $\lambda_{\mathrm{aff}}(G) := \frac{1}{|G|}\Lambda_{\mathrm{aff}}(G)$. Furthermore, we defined a *generalized FDG (gFDG)* as a pair (G, A) where G is a finite group and A an affine map of G. Just like for FDGs, we call a gFDG (G, A) *periodic* (resp. *abelian*) if and only if A is bijective (resp. G is abelian).

Point 1 of the following lemma relates actions of bijective affine maps on cosets xH of a subgroup H to actions of other affine maps on H. This was used to prove points 2 and 3 in [Bors, 2016+]. Note that point 3 relates λ-values of characteristic subgroups of a finite group G, and of quotients of G by them, to the λ-value of G.

Lemma 2.1.1. *(see "Transfer Lemma", [Bors, 2016+, Lemma 2.1.3]) Let G be a finite group, $g_0 \in G$, α an automorphism of G, and set $A := \mathrm{A}_{g_0,\alpha}$.*

1. *Let H be an α-invariant subgroup of G, and xH a left coset of H in G such that $A[xH] = xH$, say $A(x) = xh_0$. Then the map $\tau : H \to xH, h \mapsto xh$, is an isomorphism between the finite dynamical systems $(H, \mathrm{A}_{h_0,\alpha_{|H}})$ and $(xH, A_{|xH})$ (i.e., $\tau \circ \mathrm{A}_{h_0,\alpha_{|H}} = A_{|xH} \circ \tau$).*
2. *If N is a characteristic subgroup of G and $\tilde{A}$ denotes the bijective affine map of G/N induced by A (uniquely determined by the relation $\pi \circ A = \tilde{A} \circ \pi$, where $\pi : G \to G/N$ is the canonical projection), then $\lambda(\tilde{A}) \geq \lambda(A)$.*
3. *For any characteristic subgroup N of G, we have $\min\{\lambda(G/N), \lambda_{\mathrm{aff}}(N)\} \geq \lambda(G)$ and $\min\{\lambda_{\mathrm{aff}}(G/N), \lambda_{\mathrm{aff}}(N)\} \geq \lambda_{\mathrm{aff}}(G)$.* □

In studying the applicability of these transfer ideas to finite abelian p-groups, one is naturally led to the following concept: Let $E = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $F = \prod_{i=1}^{n} \mathbb{Z}/p^{f_i}\mathbb{Z}$ be finite abelian p-groups, associated with nondecreasing tuples $e = (e_1, \ldots, e_n)$ and $f = (f_1, \ldots, f_n)$ of nonnegative integers, and assume that $e_i \geq f_i$ for $i = 1, \ldots, n$

(so that F can be viewed as the image of E under the product π of the canonical projections $\pi_i : \mathbb{Z}/p^{e_i}\mathbb{Z} \to \mathbb{Z}/p^{f_i}\mathbb{Z}$). We say that e and f (or E and F) are *downward compatible* if and only if $e_j - f_j \leq e_i - f_i$ for all $1 \leq j \leq i \leq n$, and *upward compatible* if and only if $e_j - f_j \geq e_i - f_i$ for all $1 \leq j \leq i \leq n$.

The motivation for this is the following (see "Compatibility Lemma", [Bors, 2016+, Lemma 2.4.3]): If E and F are downward compatible, then for every matrix $A \in \mathrm{Mat}_n(\mathbb{Z})$ representing an automorphism of E (in the sense of [Hillar, Rhea, 2007, Theorem 3.3]), A also represents an automorphism of F (namely the induced automorphism under $\pi : E \to F$). In particular (and this is what we will be using in the proof of Theorem 2.2.2 below), if E and F are downward compatible, then each bijective affine map of E, say $\mathrm{A}_{v_0,\alpha}$, induces a bijective affine map on F, namely $\mathrm{A}_{\pi(v_0),\tilde{\alpha}}$, with $\tilde{\alpha}$ the automorphism of F induced by α. Similarly, if E and F are upward compatible, then for every $A \in \mathrm{Mat}_n(\mathbb{Z})$ representing an automorphism of F, A also represents an automorphism of E, and this automorphism induces the automorphism on F under π.

2.1.3 Primary Frobenius blocks and lower bounds on λ-values of automorphisms of finite elementary abelian 2-groups

We recall that, as mentioned in [Bors, 2016+, Section 2.3], by the theory of rational canonical forms (or Frobenius normal forms), each $(n \times n)$-matrix A over a field K is similar to a block diagonal matrix whose blocks are companion matrices of powers of irreducible polynomials over K. This block diagonal matrix is unique up to reordering of the blocks, to which we referred as the "primary Frobenius blocks of A" (or of any vector space endomorphism represented by A with respect to an appropriate basis).

The investigation of automorphisms with a "large" cycle of finite elementary abelian groups led to the following corollary:

Corollary 2.1.2. *([Bors, 2016+, Corollary 2.3.4]) Let (G, α) be a periodic elementary abelian 2-FDG such that one of the following holds:*

- $|G| \geq 2^4$ *and* $\lambda(\alpha) \geq \frac{1}{2}$,
- $\lambda(\alpha) > \frac{1}{2}$.

Then $\lambda(\alpha) > \prod_{p\in\mathbb{P}} (1 - \frac{1}{2^p}) > 0.63038$. □

Note that similarly to Theorem 1.1.5(b), this says that the set of λ-values of automorphisms of finite *elementary abelian 2-groups* does not assume any values in the interval $\left(\frac{1}{2}, \rho_1\right]$, with $\rho_1 := \prod_{p\in\mathbb{P}} (1 - \frac{1}{2^p})$. This will be used multiple times in the proof of Theorem 1.1.5(b). We will also need the similar result Corollary 2.1.3 below, which is new.

Corollary 2.1.3. *Let (G, α) be a periodic elementary abelian 2-FDG such that $\lambda(\alpha) > \frac{1}{2}$ and the primary Frobenius blocks of α are all of dimension greater than 2. Then $\lambda(\alpha) > (1 - \frac{1}{2^4}) \cdot \prod_{p\geq 3} (1 - \frac{1}{2^p}) = 0.78798\ldots$.*

Proof. We know by our classification that $\lambda(\alpha) = \prod_{i=1}^{r}(1 - \frac{1}{2^{d_i}})$, where the numbers $d_1, \ldots, d_r$ are pairwise coprime and are just the dimensions of the primary Frobenius blocks of α. To obtain a lower bound, replace d_i divisible by at least one odd prime by their largest prime divisor p_i, and should one d_i happen to be a power of 2, then it is at least 4 by assumption and we may replace it by 4. The lower bound which we get then is a finite subproduct of the infinite product which is the asserted lower bound, whence we are done. ☐

2.2 Classification of periodic abelian gFDGs (G, A) with $\lambda(A) = 1$

For proving Theorem 1.1.4, we will need this classification result at one point. We start with a lemma:

Lemma 2.2.1. *Let G be a finite abelian group, $g \in G$ and α an automorphism of G. Then the order of $\mathrm{A}_{g,\alpha}$ equals the product of the order of α with the order of some fixed point of α in G.*

Proof. Since the map $\mathrm{Hol}(G) \to \mathrm{Aff}(G), (g, \alpha) \mapsto \mathrm{A}_{g,\alpha}$ is an isomorphism, we show the respective statement for elements of the holomorph instead. Clearly, $\mathrm{ord}(\alpha) \mid \mathrm{ord}((g, \alpha))$, and $(g, \alpha)^{\mathrm{ord}(\alpha)} = (g\alpha(g) \cdots \alpha^{\mathrm{ord}(\alpha)-1}(g), \mathrm{id})$. But $g\alpha(g) \cdots \alpha^{\mathrm{ord}(\alpha)-1}(g)$ is a fixed point of α since G is abelian, and the assertion follows. ☐

The main effort in establishing the classification result of this subsection lies in analyzing the p-group case, which is achieved by Theorem 2.2.2:

Theorem 2.2.2. *Let G be a finite abelian p-group for some prime p. The following are equivalent:*

1. $\lambda_{\mathrm{aff}}(G) = 1$.
2. $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ *or* $G \cong \mathbb{Z}/p^n\mathbb{Z}$ *for some* $n \in \mathbb{N}$.

Proof. For "2 ⇒ 1": It is easy to check that if α is an automorphism of order 2 of $(\mathbb{Z}/2\mathbb{Z})^2$ and $v \in (\mathbb{Z}/2\mathbb{Z})^2$ is not a fixed point of α, then $\lambda(\mathrm{A}_{v,\alpha}) = 1$. For the cyclic groups G, just consider the map $G \to G$, $g \mapsto g_0 g$, for any generator g_0 of G.

For "1 ⇒ 2": The idea is to use a downward compatibility argument to reduce to the study of a few special cases. More precisely, write $G = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$ with $(e_1, \ldots, e_n)$ nondecreasing. G is downward compatible with the elementary abelian group $(\mathbb{Z}/p\mathbb{Z})^n$, and if $n = 2$ and $e_2 > 1$, then G is either downward compatible with $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ (if $e_1 < e_2$) or with $(\mathbb{Z}/p^2\mathbb{Z})^2$ (if $e_1 = e_2$). Hence by the compatiblity and transfer ideas from Subsubsection 2.1.2, it is sufficient to show the following three assertions:

(A) For odd p and $n \geq 2$, $\lambda_{\mathrm{aff}}((\mathbb{Z}/p\mathbb{Z})^n) < 1$.

(B) For $n \geq 3$, $\lambda_{\mathrm{aff}}((\mathbb{Z}/2\mathbb{Z})^n) < 1$.

(C) $\max(\lambda_{\mathrm{aff}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}), \lambda_{\mathrm{aff}}((\mathbb{Z}/4\mathbb{Z})^2)) < 1$.

Assertion (C) (more precisely, $\lambda_{\mathrm{aff}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = \lambda_{\mathrm{aff}}((\mathbb{Z}/4\mathbb{Z})^2) = \frac{1}{2}$) is readily verified using GAP [The GAP group, 2014].

As for assertions (A) and (B), let p be any prime and assume that $n \geq 2$. Note that by Lemma 2.2.1 and the fact that the orders of automorphisms of nontrivial finite groups are always smaller than the group order (see [Horoševskiĭ, 1974, Theorem 2]), if $A = \mathrm{A}_{v,\alpha}$ is a bijective affine map of $(\mathbb{Z}/p\mathbb{Z})^n$ of λ-value 1, then α must have a nontrivial fixed point and $\mathrm{ord}(\alpha) = p^{n-1}$. In particular, the order of one of the primary Frobenius blocks of α equals p^{n-1}; fix one such block, say of the form $\mathrm{M}(P(X)^k)$, with $1 \leq k \leq n$ and $P(X) \in \mathbb{F}_p[X]$ irreducible with $P(0) \neq 0$. Let ξ be any of the roots of $P(X)$ in $\overline{\mathbb{F}_p}$. By [Lidl, Niederreiter, 1997, Theorems 3.8 and 9.96], we have

$$p^{n-1} = \mathrm{ord}(\mathrm{M}(P(X)^k)) = \mathrm{ord}(P(X)^k) = \mathrm{ord}(\xi) \cdot p^{\lceil \log_p(k) \rceil},$$

where $\mathrm{ord}(P(X)^k)$ denotes the order of the polynomial $P(X)^k$ (the smallest positive integer e such that $P(X)^k \mid X^e - 1$ in $\mathbb{F}_p[X]$), and $\mathrm{ord}(\xi)$ is the order of ξ in the multiplicative group $\overline{\mathbb{F}_p}^*$. It follows that $\xi = 1$, whence $P(X) = X - 1$, and $\lceil \log_p(k) \rceil = n - 1$. Since $\lceil \log_p(n-1) \rceil < n - 1$ for all $n \geq 2$, we must have $k = n$ (in particular, α has precisely one primary Frobenius block), and because $\lceil \log_p(n) \rceil < n - 1$ holds for all p for $n \geq 4$ and for odd p for $n \geq 3$, we can refute the case $n \geq 3$ for all p except possibly for the subcase $p = 2, n = 3$. However, that subcase is readily refuted with GAP [The GAP group, 2014]: $\lambda_{\mathrm{aff}}((\mathbb{Z}/2\mathbb{Z})^3) = \frac{7}{8}$.

In particular, this proves assertion (B), and for proving assertion (A), it remains to refute the case $n = 2$ for odd p, which can be done as follows: We already know by [Bors, 2016+, Corollary 1.1.8] that, with respect to an appropriate $\mathbb{F}_p$-basis of $(\mathbb{Z}/p\mathbb{Z})^2$, α is represented by $\mathrm{M}((X-1)^2)$, which has characteristic polynomial $(X-1)^2$, so α can be represented, with respect to some other basis $\mathcal{B}$, by a matrix of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ for an element $a \in \mathbb{F}_p^*$ (we must have $a \neq 0$ since otherwise, the order of A could only be at most p). Replacing A by an appropriate power, we may even assume w.l.o.g. that $a = 1$. From now on, all elements of $(\mathbb{Z}/p\mathbb{Z})^2$ are represented by their coordinate vectors with respect to $\mathcal{B}$. If $v = (x, y)^t$, we find, by an easy induction on $n \geq 0$, that the image of $(0,0)^t$ under A^n equals $(nx + \Delta_{n-1}y, ny)^t$, where $\Delta_k = \frac{1}{2}k(k+1)$ is the k-th triangle number. In particular, the cycle returns to the zero element after p iterations of A, although it should only return after p^2 iterations, a contradiction. □

It is now not difficult to even classify the periodic abelian gFDGs (G, A) such that $\lambda(A) = 1$:

Corollary 2.2.3. *Let G be a finite abelian group, $A = \mathrm{A}_{g_0,\alpha}$ a bijective affine map of G. The following are equivalent:*

1. *$\lambda(A) = 1$.*
2. *Up to isomorphism of gFDGs, one of the following holds:*
   (a) *$G = \prod_{p \| G|} \mathbb{Z}/p^{k_p}\mathbb{Z}$ is cyclic, g_0 is a generator of G, and, splitting $\alpha = \prod_{p \| G|} \alpha_p$ over the Sylow subgroups $\mathbb{Z}/p^{k_p}\mathbb{Z}$ of G, α_p is the multiplication by a factor a_p such that $a_p \equiv 1 \pmod p$ for all prime divisors p of $|G|$, and*

such that, if $k_2 \geq 2$*, then* $a_2 \equiv 1 \pmod 4$ *(in other words,* α *corresponds to multiplication by an* $|G|$*-Knuthian number on* G*).*

(b) $G = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/o\mathbb{Z}$ *for some odd* $o \geq 1$*, and, splitting* $g_0 = (g_2, g_o)$ *and* $\alpha = \alpha_2 \times \alpha_o$ *over that product,* $\mathrm{A}_{g_o,\alpha_o}$ *is an affine map of* $\mathbb{Z}/o\mathbb{Z}$ *as described in point (a), and* α_2 *is an automorphism of* $(\mathbb{Z}/2\mathbb{Z})^2$ *of order* 2 *such that* g_2 *is not a fixed point of* α_2*.*

Proof. Write G as the product of its Sylow subgroups: $G = \prod_{p\in\mathbb{P}} G_p$. Note that every automorphism of G is a product of automorphisms of the G_p. If $A = \mathrm{A}_{(g_p)_{p\in\mathbb{P}},(\alpha_p)_{p\in\mathbb{P}}}$ is a bijective affine map of G, then A can be written as $A = \prod_{p\in\mathbb{P}} \mathrm{A}_{g_p,\alpha_p}$, i.e., as a product of bijective affine maps of the single G_p. Using this, it is not difficult to see that $\lambda(A) = 1$ if and only if $\lambda(\mathrm{A}_{g_p,\alpha_p}) = 1$ for all $p \in \mathbb{P}$.

By Theorem 2.2.2, this reduces the problem to classifying the periodic gFDGs (G, A) where $\lambda(A) = 1$ and G is of one of the two forms $\mathbb{Z}/p^k\mathbb{Z}$, for p prime and $k \geq 0$, or $(\mathbb{Z}/2\mathbb{Z})^2$ respectively. For $(\mathbb{Z}/2\mathbb{Z})^2$, this is an easy exercise, and for the $\mathbb{Z}/p^k\mathbb{Z}$, a classification as desired is given by Knuth's aforementioned theorem, see [Knuth, 1998, Section 3.2.1.2, Theorem A]. □

2.3 A classification algorithm

Fix a rational number $\rho \in \left[\frac{1}{2}, 1\right]$. In principle, by [Bors, 2016+, Corollary 1.1.8 and Theorem 2.5.2], we know how the periodic abelian FDGs (G, α) with $\lambda(\alpha) = \rho$ look like (note that if $\rho = \frac{1}{2}$ and G is not of prime power order, then (G, α) decomposes into a product of p-FDGs, each with λ-value greater than $\frac{1}{2}$). However, even for given group order, points 4 and 5 in our list in Subsubsection 2.1.1 correspond to various distinct FDG isomorphism types, and it is not clear at first sight whether one can write down the list of periodic abelian FDGs with λ-value ρ explicitly. This is what we will address in this subsection.

Write $\rho = \frac{a}{b}$ with $a, b \in \mathbb{N}^+$ and $\gcd(a, b) = 1$. Note that since $|G|$ is divisible by at most one odd prime (see [Bors, 2016+, Lemma 2.1.5(2) and Corollary 1.1.8]) and $b \mid |G|$, if b is divisible by more than one odd prime, there are no perodic (abelian) FDGs (G, α) with $\lambda(\alpha) = \rho$ at all. Therefore, we may henceforth assume that b is divisible by at most one odd prime. We distinguish three cases.

1. Let us first list those (G, α) where $|G|$ is an odd prime power. By [Bors, 2016+, Corollary 1.1.8], if ρ is not of the form $1 - \frac{1}{p^m}$ for some prime $p > 2$, there are no such FDGs. Otherwise, if $\rho = 1 - \frac{1}{p}$, then the complete list of such FDGs consists of those from point 1 of the list in Subsubsection 2.1.1 and of the "exceptional" elementary abelian FDGs from point 3. And if $\rho = 1 - \frac{1}{p^m}$ for some $m \geq 2$, then the list consists of the "standard" elementary abelian FDGs of order p^m from point 2.

2. We continue by listing those (G, α) where $|G|$ is a power of 2. If $\rho = \frac{1}{2}$, we know by [Bors, 2016+, Theorem 2.5.2] that there is precisely one possiblity for G which is neither primary cyclic nor elementary abelian, namely $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. It is also not difficult to check (e.g. with GAP [The GAP group, 2014]) that it corresponds, up to isomorphism, to precisely one FDG as we are

looking for, namely the FDG from point 3 in Theorem 1.1.4. We also know that the solutions where G is primary cyclic are precisely those from points 1 and 2 in Theorem 1.1.4. For a complete treatment of this case, it remains to list the FDGs (G, α) with $\lambda(\alpha) = \rho$ where G is elementary abelian of order 2^k, $k \geq 2$, for arbitrary $\rho \geq \frac{1}{2}$. By [Bors, 2016+, Theorem 2.3.3], the only such FDGs where the primary Frobenius blocks of α are *not* companion matrices of monic primitive irreducible polynomials over $\mathbb{F}_2$ with pairwise coprime degrees greater than 1 are the two FDGs listed in points 4 and 5 in Theorem 1.1.4 of the present paper and have λ-value $\frac{1}{2}$. As for the other solutions, denoting by $d_1, \ldots, d_r$ the dimensions of the primary Frobenius blocks of α in such a solution, we find that $\frac{a}{b} = \rho = \frac{\prod_{i=1}^r (2^{d_i}-1)}{2^{d_1+\cdots+d_r}}$. Since the numerator and denominator on the RHS are coprime, it follows that $a = \prod_{i=1}^r (2^{d_i} - 1)$ and $b = 2^{d_1+\cdots+d_r}$. Hence if b is not a power of 2, there are no such FDGs. Otherwise, set $k := \log_2(b)$. Then k is the $\mathbb{F}_2$-dimension of G in any such FDG, and we know that the d_i are pairwise coprime and form an (integer) partition of k. Furthermore, if $k \geq 2$, all d_i are greater than 1. It thus suffices to systematically go through the corresponding partitions $k = d_1 + \cdots + d_r$ and check for which we have $a = \prod_{i=1}^r (2^{d_i} - 1)$; note that in general, such a partition still corresponds to multiple solutions up to FDG isomorphism, since for $d \geq 2$, there are, in general, multiple monic primitive irreducible polynomials of degree d over $\mathbb{F}_2$.

3. Finally, we discuss how to list the (G, α) with $\lambda(\alpha) = \rho$ where $|G|$ is *not* a prime power, i.e, $|G| = 2^k p^l$ for some odd prime p and $k, l \in \mathbb{N}^+$. Then $(G, \alpha) = (G_2, \alpha_2) \times (G_p, \alpha_p)$, where G_2 and G_p are the Sylow 2- and p-subgroup of G respectively, and α_2 and α_p the respective restrictions of α. We know that $\gcd(\Lambda(\alpha_2), \Lambda(\alpha_p)) = 1$, $\lambda(\alpha) = \lambda(\alpha_2) \cdot \lambda(\alpha_p)$, that $\lambda(\alpha_p) = 1 - \frac{1}{p^m}$ for some $m \in \mathbb{N}^+$ and that, denoting by $d_1, \ldots, d_r$ the dimensions of the primary Frobenius blocks of α_2, $\lambda(\alpha_2) = \frac{\prod_{i=1}^r (2^{d_i}-1)}{2^{d_1+\cdots+d_r}}$. Hence we conclude that $\frac{a}{b} = \rho = \frac{\prod_{i=1}^r (2^{d_i}-1)\cdot(p^m-1)}{2^{d_1+\cdots+d_r}p^m}$. In contrast to the case where $|G|$ is a power of 2, the numerator and denominator of the RHS are not coprime here. Still, when passing to the canceled form $\frac{a}{b}$ of the fraction, only prime factors 2 and p may cancel, so for all primes $q \neq 2, p$, we have $\nu_q(a) = \nu_q(\prod_{i=1}^r (2^{d_i} - 1) \cdot (p^m - 1))$. Note also that p may vary depending on the solution which we are considering and may not even be a prime divisor of a. Since we are not assuming that the d_i are ordered, we can make the following convention: If p divides any of the factors $2^{d_i} - 1$, w.l.o.g. we assume that $p \mid 2^{d_1} - 1$. Set $l' := \nu_p(2^{d_1} - 1)$, $t_1 := \frac{2^{d_1}-1}{p^{l'}}$ and $t_i := 2^{d_i} - 1$ for $i = 2, \ldots, r$. Also, note that if b is not a power of 2, we know that the unique odd prime divisor of b must be the prime p from above, i.e., we can read off its value from the input ρ. We distinguish another three subcases:

   (a) If $\nu_p(b) \geq 2$, then (G_p, α_p) must be one of the "standard" elementary abelian FDGs of type 2 from our classification, as the other two possibilities (G_p primary cyclic or (G_p, α_p) an "exceptional" elementary abelian FDG) lead to $\nu_p(b) = 1$ (since $p \mid \Lambda(\alpha_p)$ and thus $p \nmid \Lambda(\alpha_2)$ then). Since α_p is of order $|G_p| - 1 = p^l - 1$, we have $m = l$ in this case, and upon passing to the canceled form $\frac{a}{b}$ of ρ, the divisor $p^{l'}$ of $2^{d_1}-1$ must cancel completely, so $\nu_p(b)+l'=m$. It follows that

$$\rho = \frac{\prod_{i=1}^r (2^{d_i}-1)\cdot(p^m-1)}{2^{d_1+\cdots+d_r}p^m} = \frac{p^{l'}t_1\cdot t_2\cdots t_r(p^{\nu_p(b)+l'}-1)}{(p^{l'}t_1+1)(t_2+1)\cdots(t_r+1)p^{\nu_p(b)+l'}}$$
$$= (1-\frac{1}{p^{l'}t_1})(1-\frac{1}{t_2+1})\cdots(1-\frac{1}{t_r+1})\cdot(1-\frac{1}{p^{\nu_p(b)+l'}}). \quad (1)$$

Now note that by definition, the t_i are pairwise coprime, $t_2+1,\ldots,t_r+1$ are powers of 2 (and greater than 2), no t_i is divisible by p, and each t_i is a "full divisor of a", i.e., a product of pairwise distinct prime powers of the form $q^{\nu_q(a)}$. This leaves only finitely many possibilities for the tuple $(t_1,\ldots,t_r)$, over which we can loop and thus assume $(t_1,\ldots,t_r)$ to be fixed. Obviously, a necessary condition for (1) to hold is that $\prod_{i=2}^r(1-\frac{1}{t_i+1})>\rho$, and in that case, since $(1-\frac{1}{p^{l'}t_1})(1-\frac{1}{p^{\nu_p(b)+l'}})$ converges strictly monotonously to 1 as $l'\to\infty$, (1) holds for at most one value of l' within an effectively bounded range of numbers. Should it hold for some l', it remains to check whether $p^{l'}t_1+1$ is a power of 2 and $\gcd(t_i,p^{\nu_p(b)+l'}-1)=1$ for $i=1,\ldots,r$, and if so, one has found a parameter tuple $(t_1,\ldots,t_r,l')$ corresponding to a nonempty set of FDG isomorphism types as required.

(b) If $\nu_p(b)=1$, one can determine the list of (G,α) where (G_p,α_p) is a "standard" elementary abelian FDG like we just did in point (a). However, in this case, it may also be that G_p is primary cyclic or (G_p,α_p) is an exceptional elementary abelian FDG. If so, we have $p\mid\Lambda(\alpha_p)$, and so p cannot divide any of the $2^{d_i}-1$. It follows that $l'=0$, and fixing a tuple of values for the t_i with the same properties as listed above after (1), and such that additionally, t_1+1 is greater than 2 and a power of 2, and $\gcd(t_i,p-1)=1$ for $i=1,\ldots,r$, a necessary and sufficient condition for that tuple to correspond to at least one FDG isomorphism type as required (actually, an infinite class of them due to the variability of (G_p,α_p)) is that

$$\rho=(1-\frac{1}{t_1+1})\cdots(1-\frac{1}{t_r+1})\cdot(1-\frac{1}{p}),$$

which can be effectively checked.

(c) Finally, if b is a power of 2, we cannot read off the value of p from the input as before, but at least, we *do* know that (G_p,α_p) is a "standard" elementary abelian FDG. Moreover, we know that $l'\geq 1$ (otherwise, the power of p in the denominator could not have canceled upon passing to the canceled form $\frac{a}{b}$). We have the following restrictions on $(t_1,\ldots,t_r)$: The t_i are pairwise coprime, each of them is a full divisor of a, we have $t_2,\ldots,t_r>1$, and $t_2+1,\ldots,t_r+1$ are powers of 2. Fixing one such tuple and noting that

$$\rho=(1-\frac{1}{t_1p^{l'}+1})(1-\frac{1}{t_2+1})\cdots(1-\frac{1}{t_r+1})(1-\frac{1}{p^{l'}}),$$

we again find that necessarily $(1-\frac{1}{t_2+1})\cdots(1-\frac{1}{t_r+1})>\rho$, and in that case, since the term $(1-\frac{1}{t_1x+1})(1-\frac{1}{x})$ converges strictly monotonously to 1 as $x\to\infty$, there is at most one matching value for $p^{l'}$ within an effectively bounded range. Should that value match, it remains to check whether $t_1p^{l'}+1$ is a power of 2, whether $p\nmid t_i$ for $i=2,\ldots,r$, and whether $\gcd(t_i,p^{l'}-1)=1$ for $i=1,\ldots,r$. If so, the parameter tuple $(t_1,\ldots,t_r,p,l')$ corresponds to a nonempty set of FDG isomorphism types as required.

We conclude this subsection with a "by hands" application of our algorithm to the input $\rho=\frac{1}{2}$ to prove the following:

Proposition 2.3.1. *The FDGs from points 1–6 in Theorem 1.1.4 form, up to isomorphism, the complete list of periodic **abelian** FDGs with λ-value $\frac{1}{2}$.*

Proof. We follow our algorithm as described above. Since $\frac{1}{2}$ is not of the form $1-\frac{1}{p^m}$ for any prime $p>2$ and $m\in\mathbb{N}^+$, there are no FDGs (G,α) as required where $|G|$ is an odd prime power. As for the (G,α) with $|G|$ a power of 2, the number of such FDGs distinct from those listed in points 1–5 of Theorem 1.1.4 is bounded from above by the number of nonempty tuples $(t_1,\ldots,t_r)$ of full divisors greater than 1 of $a=1$, so there are no such solutions.

Finally, we need to check the case where $|G|$ is *not* a prime power. Since $b=2$ is a power of 2, we need to consider the tuples $(t_1,\ldots,t_r)$ where $t_1,\ldots,t_r$ are pairwise coprime full divisors of $a=1$ with $t_2,\ldots,t_r>1$, and $t_2+1,\ldots,t_r+1$ are powers of 2. Clearly, in such a tuple, $r=1$ and $t_1=1$. Now consider the equation $\frac{1}{2}=(1-\frac{1}{x+1})(1-\frac{1}{x})$, which has the unique solution $x=3$. Since 3 is an odd prime power, $3+1=2^2$ and $\gcd(1,3-1)=1$, we have found the last set of FDGs as required, which are of the form $(\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}/3\mathbb{Z}$, together with the product of an order 3 automorphism on $(\mathbb{Z}/2\mathbb{Z})^2$ with an order 2 automorphism on $\mathbb{Z}/3\mathbb{Z}$. Since there is precisely one monic primitive irreducible polynomial of degree 2 over $\mathbb{F}_2$ and of degree 1 over $\mathbb{F}_3$, they only correspond to one FDG up to isomorphism. □

3 Proofs of Theorems 1.1.4 and 1.1.5

3.1 Proof of Theorem 1.1.4

By Proposition 2.3.1, it suffices to show that any periodic FDG (G,α) such that $\lambda(\alpha)=\frac{1}{2}$ and G is nonabelian is isomorphic with one of the FDGs from points 7-10 in the theorem, and to verify the assertions on nonisomorphism made in each point.

The proof is structured into the following steps:

1. G has an abelian subgroup A of index 2.
2. A can be chosen to be α-invariant, which is clearly equivalent to the set S, consisting of all elements of G lying on the unique largest cycle of α, coinciding with $G\setminus A$.

3. (G,α) is isomorphic with one of the nonabelian FDGs from the theorem, and the dependency of the isomorphism type on the case-specific parameter (m or o respectively) is as asserted by the theorem.

For 1: This is obtained by following [Bors, 2016+, proof of Theorem 1.1.7]. The point is that among the three types of nonabelian groups from Liebeck and MacHale's structure theorem [Liebeck, MacHale, 1972, Theorem 4.1.3] (the first of which are those with an abelian subgroup of index 2), one can exclude with almost verbatim the same argument as in [Bors, 2016+, proof of Theorem 1.1.7] that G is of type (II) or (III); one only needs to additionally refer to Corollary 2.1.2 to still be able to conclude $\lambda(\tilde{\alpha}) > \frac{1}{2}$ for the induced automorphism $\tilde{\alpha}$ on the central quotient of G.

For 2: Assume that $S \neq G \setminus A$. Then S intersects both with $A \setminus \zeta G$ and with $G \setminus A$, so as in [Bors, 2016+, proof of Theorem 1.1.7], we conclude that $[G : \zeta G] = 4$; in particular, G is nilpotent of class 2 with all Sylow subgroups except for the Sylow 2-subgroup being abelian. If $|G|$ is divisible by some odd prime p, then since $\lambda(\alpha)$ equals the product of the λ-values of the restrictions of α to the Sylow subgroups of G, $\lambda(G_2) > \frac{1}{2}$ for the Sylow 2-subgroup G_2 of G, which by [Bors, 2016+, Theorem 1.1.7] implies that G_2 and hence G is abelian, a contradiction. Therefore, G is a 2-group. Furthermore, the automorphism $\tilde{\alpha}$ of $G/\zeta G$ induced by α has λ-value at least $\frac{1}{2}$ by Lemma 2.1.1(2), but if $\lambda(\tilde{\alpha}) > \frac{1}{2}$, we arrive at the same contradiction as in [Bors, 2016+, proof of Theorem 1.1.7]. Hence $\lambda(\tilde{\alpha}) = \frac{1}{2}$, and $\mathrm{dom}(\sigma)$ is equal to the union of two cosets of ζG in G, one of them being $A \setminus \zeta G$. Setting $\beta := \alpha^2$, we find that β restricts to an automorphism $\overline{\beta}$ of A such that $\lambda(\overline{\beta}) = \frac{1}{2}$. Since A is a finite abelian 2-group, by Proposition 2.3.1 and nonabelianity of G, we have $|A| = 4$ or $|A| = 8$.

If $|A| = 4$, i.e., $|G| = 8$, then $G \cong \mathrm{D}_8$ or $G \cong \mathrm{Dic}_8 = \mathrm{Q}_8$. D_8 has a characteristic abelian subgroup of index 2, by which we can replace A. Q_8, in turn, does not have a characteristic subgroup of index 2, but it is not difficult to see that in this case, α, being an automorphism of order 4 of Q_8, has a fixed point f of order 4, so we may replace A by $\langle f \rangle$.

If $|A| = 8$, then $|G| = 16$ and $\mathrm{ord}(\alpha) = 8$ by Lagrange's theorem, since the elements of G whose cycle under α has length a divisor of 8 form a subgroup of G. Observe that $|\zeta G| = 4$, so the restriction of α to ζG only has cycles of length at most 2, whence $\overline{\beta}$ has, apart from its 4-cycle, four fixed points. However, up to FDG isomorphism either $A = (\mathbb{Z}/2\mathbb{Z})^3$ and $\overline{\beta}$ is given by the companion matrix of $(X-1)^3 \in \mathbb{F}_2[X]$, or $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $\overline{\beta}$ is given by the matrix $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$, and in both cases, $\overline{\beta}$ only has two fixed points, a contradiction.

For 3: Assuming w.l.o.g. that $S = G \setminus A$, which is a coset of A in G, we can conclude by Lemma 2.1.1(1) that, denoting by $\overline{\alpha}$ the restriction of α to A, fixing $x \in G \setminus A$ and letting $a_0 \in A$ be such that $\alpha(x) = xa_0$, we have $\lambda(\mathrm{A}_{a_0,\overline{\alpha}}) = 1$, whence we can derive some heavy restrictions on both A and α by Corollary 2.2.3. There are two cases to distinguish, according to whether or not A is cylic:

1. If A is cyclic, then G has a presentation of the form $\langle r, x \mid r^n = 1, x^2 = r^k, xrx^{-1} = r^l \rangle$ for some $n \geq 3$ and $k, l \in \mathbb{N}$, where $A = \langle r \rangle$. That $x^2 = r^k \in$

$\mathrm{C}_G(r) \cap \mathrm{C}_G(x)$ implies that

$$l^2 \equiv 1 \pmod{n} \tag{2}$$

and

$$k(l-1) \equiv 0 \pmod{n}. \tag{3}$$

Note that (2) and (3) impose restrictions solely on the structure of G, and not on α. By assumption and Lemma 2.1.1(1), there exist $m, a \in \mathbb{N}$ such that $\alpha(r) = r^m$, $\alpha(x) = xr^a$, and $y \mapsto my + a$ is an affine map of $\mathbb{Z}/n\mathbb{Z}$ with λ-value 1, which by Corollary 2.2.3 lets us infer the following restrictions on m and a:

$$\gcd(a, n) = 1, \tag{4}$$

and m is n-Knuthian, i.e.,

$$p \text{ prime and } p \mid n \Rightarrow m \equiv 1 \pmod{p}, \text{ and } 4 \mid n \Rightarrow m \equiv 1 \pmod{4}. \tag{5}$$

Additionally, a and m must be chosen such that the three defining relations are respected, which yields precisely one further restriction, namely, as an easy computation shows,

$$k(m-1) \equiv a(l+1) \pmod{n}. \tag{6}$$

Consider an *odd* prime divisor p of n and set $k_p := \nu_p(n)$. Then we can infer from (2) that $l \equiv \pm 1 \pmod{p^{k_p}}$ (since those are, by the cyclicity of the automorphism group of $\mathbb{Z}/p^{k_p}\mathbb{Z}$, the only solutions x of $x^2 = 1$ modulo p^{k_p}). However, if $l \equiv 1 \pmod{p^{k_p}}$, we get a contradiction, since (6) in view of (4) and (5) then implies that $0 \equiv k(m-1) \equiv 2a \not\equiv 0 \pmod{p}$. Hence we conclude that

$$l \equiv -1 \pmod{p^{k_p}} \text{ for all } p \in \mathbb{P}, p > 2, p \mid n, \tag{7}$$

which in view of (3) implies that

$$k \equiv 0 \pmod{p^{k_p}} \text{ for all } p \in \mathbb{P}, p > 2, p \mid n. \tag{8}$$

If $k_2 := \nu_2(n) > 0$, then (2) yields that $l \bmod 2^{k_2} \in \{1, 2^{k_2-1} - 1, 2^{k_2-1} + 1, 2^{k_2} - 1\}$. We will show that actually

$$l \equiv -1 \pmod{2^{k_2}}, \tag{9}$$

which in combination with (7) implies that the conjugation action of x on $\langle r \rangle$ is by inversion. Note that (9) is clear if $k_2 = 1$, so we may assume that $k_2 > 1$, whence by (5), $m \equiv 1 \pmod{4}$.

(a) If $l \equiv 1 \pmod{2^{k_2}}$, then by (6), we have $0 \equiv k \cdot \frac{m-1}{2} \equiv a \not\equiv 0 \pmod{2}$, a contradiction.

(b) If $l \equiv 2^{k_2-1} - 1 \pmod{2^{k_2}}$, then by (3), we find that $k \equiv 0 \pmod{2^{k_2-1}}$, whence by (6), $0 \equiv \frac{k}{2^{k_2-1}}(m-1) \equiv a \equiv 1 \pmod 2$, a contradiction.

(c) Finally, if $l \equiv 2^{k_2-1} + 1 \pmod{2^{k_2}}$, then by (3), $k \equiv 0 \pmod 2$, which by (6) yields the contradictory $0 \equiv \frac{k}{2} \cdot (m-1) \equiv a \cdot (2^{k_2-2}+1) \equiv 1 \pmod 2$. This concludes the proof of (9).

Now by (3) and (9), we conclude that $k \equiv 0 \pmod{2^{k_2-1}}$, whence we either have $k \equiv 0 \pmod{2^{k_2}}$, which in combination with (8) implies that $G \cong \mathrm{D}_{2n}$, or $k \equiv 2^{k_2-1} \pmod{2^{k_2}}$, i.e., $G \cong \mathrm{Dic}_{2n}$. In both cases, we find that choosing a and m according to (4) and (5), (6) is automatically satisfied because of (7)–(9), so any such choice of a and m leads to an automorphism α of λ-value $\frac{1}{2}$. Note that by definition of the concept of an FDG isomorphism, for automorphisms β, γ of G, the FDGs (G, β) and (G, γ) are isomorphic if and only if β and γ are conjugate in the automorphism group of G. Hence $m \mod n$ is determined by the FDG isomorphism type of (G, α) in both cases, since A is both cyclic (and thus has abelian automorphism group) and characteristic in G, except when $G \cong \mathrm{Dic}_8$, in which case necessarily $m \mod n = 1$ (by α-invariance of A). Hence in order to conclude the proof in this first case, it suffices to show that keeping m fixed and replacing a by 1 does not change the FDG isomorphism type. However, it is readily checked that conjugation by the automorphism sending $r \mapsto r^{a^{-1}}, x \mapsto x$ (with $a^{-1} \in \mathrm{Z}_n$ the multiplicative inverse of a modulo n) transforms α into the automorphism sending $r \mapsto r^m, x \mapsto xr$.

2. If A is not cyclic, then by Corollary 2.2.3, A is isomorphic with $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/o\mathbb{Z}$ for some odd $o \geq 1$. Any element $x \in G \setminus A$ acts on A by an automorphism of order 2, and hence on the Sylow 2-subgroup of A, $(\mathbb{Z}/2\mathbb{Z})^2$, by the identity or by an automorphism of order 2. We will first show that it must act by the identity. Otherwise, there exist two nontrivial elements $r_1, r_2 \in (\mathbb{Z}/2\mathbb{Z})^2$ swapped in a transposition by conjugation with x, from which we conclude that there exist $\epsilon_1, \epsilon_2 \in \{0,1\}$ and $k, l \in \mathbb{N}$ with $\gcd(l, o) = 1$ such that $G = \langle r_1, r_2, r, x \mid r_1^2 = r_2^2 = r^o = [r_1, r_2] = [r_1, r] = [r_2, r] = 1, x^2 = r_1^{\epsilon_1} r_2^{\epsilon_2} r^k, x r_1 x^{-1} = r_2, x r_2 x^{-1} = r_1, x r x^{-1} = r^l \rangle$. Observing that $x^2 = r_1^{\epsilon_1} r_2^{\epsilon_2} r^k$ lies in the centralizer of x, we deduce that $\epsilon_1 = \epsilon_2 =: \epsilon$. Fix $a, m \in \mathbb{N}$ and $f_1, f_2 \in \{0,1\}$ such that $\alpha(r) = r^m, \alpha(x) = x r_1^{f_1} r_2^{f_2} r^a$, and note that α restricts to an automorphism of $\langle r_1, r_2 \rangle$ of order 2 (by Corollary 2.2.3). Hence either α swaps r_1 and r_2 in a transposition, or w.l.o.g. $\alpha(r_1) = r_1, \alpha(r_2) = r_1 r_2$, and both cases are contradictory: If $\alpha(r_1) = r_2, \alpha(r_2) = r_1$, then since by Corollary 2.2.3, $r_1^{f_1} r_2^{f_2}$ must not be a fixed point of α, we can assume w.l.o.g. (swapping the indices of r_1 and r_2 if necessary) that $(f_1, f_2) = (1, 0)$. Considering that α must respect the defining relation $x^2 = r_1^{\epsilon} r_2^{\epsilon} r^k$, we obtain that $r_1^{1+\epsilon} r_2^{1+\epsilon} = r_1^{\epsilon} r_2^{\epsilon}$, a contradiction. If $\alpha(r_1) = r_1, \alpha(r_2) = r_1 r_2$, then it is easy to see that α cannot respect the defining relation $x r_1 x^{-1} = r_2$.

So far, we know that G has a presentation of the form $G = \langle r_1, r_2, r, x \mid r_1^2 = r_2^2 = r^o = [r_1, r_2] = [r_1, r] = [r_2, r] = 1, x^2 = r_1^{\epsilon_1} r_2^{\epsilon_2} r^k, [x, r_1] = 1, [x, r_2] = 1, x r x^{-1} = r^l \rangle$ for some $\epsilon_1, \epsilon_2 \in \{0,1\}$ and $k, l \in \mathbb{N}$, with $o > 1$ (since otherwise, G is abelian), $\gcd(l, o) = 1$, and w.l.o.g., we may assume that

$\alpha(r_1) = r_2, \alpha(r_2) = r_1, \alpha(x) = xr_1r^a, \alpha(r) = r^m$ for some $a, m \in \mathbb{N}$ with

$$\gcd(a, o) = 1 \tag{10}$$

and m being o-Knuthian, i.e.,

$$p \text{ prime and } p \mid o \Rightarrow m \equiv 1 \pmod{p}. \tag{11}$$

Again, using that $x^2 = r_1^{\epsilon_1} r_2^{\epsilon_2} r^k$ lies in the centralizer of x, we obtain $k(l-1) \equiv 0 \pmod{o}$. Also, we find that only the defining relation $x^2 = r_1^{\epsilon_1} r_2^{\epsilon_2} r^k$ imposes further restrictions, namely $\epsilon_1 = \epsilon_2 =: \epsilon$ and $k(m-1) \equiv a(l+1) \pmod{o}$. Hence just as before, we can conclude that $l \equiv -1 \pmod{o}$, whence the conjugation action of x on A is by inversion, and $k \equiv 0 \pmod{o}$. Conversely, for any choice of $\epsilon \in \{0, 1\}$ and of a, m as in (10) and (11), we obtain a periodic FDG (G, α) with λ-value $\frac{1}{2}$. It is readily verified that for both values of ϵ, the map $r_1 \mapsto r_1, r_2 \mapsto r_2, r \mapsto r^{a^{-1}}, x \mapsto x$ extends to an automorphism β of G such that $\beta \circ \alpha \circ \beta^{-1}$ maps $r_1 \mapsto r_2, r_2 \mapsto r_1, r \mapsto r^m, x \mapsto xr_1r$, so without changing the FDG isomorphism type, we may assume that $a = 1$. Since the order of G depends injectively on o, it remains to check that for fixed o and ϵ (and $a = 1$), different choices of $m \in \mathrm{Z}_o$ such that (11) holds lead to nonisomorphic FDGs. To see this, note that $[G : \zeta G] = 2o > 4$, and as observed in [Bors, 2016+, proof of Theorem 1.1.7], if A was not characteristic in G, then by comparing centralizer orders of elements from $A \setminus \zeta G$ and from $G \setminus A$, we would have $[G : \zeta G] = 4$. Hence A, and thus $\langle r \rangle$, is characteristic in G, and we are done. □

3.2 Proof of Theorem 1.1.5

For (a): Let $\rho \in \mathrm{im}(\lambda)$ and fix a periodic FDG (G, α) such that $\lambda(\alpha) = \rho$. Set $L := \Lambda(\alpha)$ and let $p_1, \ldots, p_r$ denote the odd prime divisors of L. Define o as the least common multiple of the multiplicative orders of 2 modulo the p_i, fix, for $n \in \mathbb{N}^+$, a monic primitive irreducible polynomial $P_n(X) \in \mathbb{F}_2[X]$ of degree $n \cdot o + 1$, set $H_n := (\mathbb{Z}/2\mathbb{Z})^{n \cdot o + 1}$, and let β_n be any automorphism of H_n having $\mathrm{M}(P_n(X))$ as its single primary Frobenius block. Finally, set $(G_n, \alpha_n) := (G, \alpha) \times (H_n, \beta_n)$. By construction, $\Lambda(\beta_n) = 2^{n \cdot o + 1} - 1 \equiv 1 \pmod{p_i}$ for $i = 1, \ldots, r$, so that in particular, $\gcd(\Lambda(\alpha), \Lambda(\beta_n)) = 1$. Therefore, $\lambda(\alpha_n) = \lambda(\alpha) \cdot \lambda(\beta_n) = \rho \cdot (1 - \frac{1}{2^{n \cdot o + 1}})$, which converges to ρ from below as $n \to \infty$.

For (b): Assume, for a contradiction, that there exists a periodic FDG (G, α) such that $\lambda(\alpha) \in \left(\frac{1}{2}, \rho_0\right]$. We recall that by Corollary 2.1.2, if G was an elementary abelian 2-group, then $\lambda(\alpha) > 0.63038 > \rho_0$, a contradiction. Therefore, by [Bors, 2016+, Corollary 1.1.8], G cannot be a p-group at all, since the interval $\left(\frac{1}{2}, \rho_0\right]$ also does not contain any numbers of the form $1 - \frac{1}{p^m}$ for odd primes p and $m \in \mathbb{N}^+$. Hence (G, α) decomposes as $(G, \alpha) = (G_2, \alpha_2) \times (G_p, \alpha_p)$, where G_2 is the Sylow 2-subgroup of G, p the unique odd prime divisor of $|G|$, and G_p the Sylow p-subgroup of G. The crucial observation now is the following: Still by Corollary 2.1.2, $\lambda(\alpha_2) > 0.63038 > \rho_0$, and the potential values of $\lambda(\alpha_p)$, i.e., the numbers $1 - \frac{1}{p^m}$ for odd p and $m \geq 1$, converge monotonously to 1 for $p^m \to \infty$. Hence there are only finitely many possibilities for $\lambda(\alpha_p)$; more precisely, it can be checked that $\frac{6}{7}\cdot 0.63038 > 0.54 > \rho_0$, whence $\lambda(\alpha_p) \in \{\frac{2}{3}, \frac{4}{5}\}$. It is clear by definition of ρ_0, by Corollary 2.1.2 and by the assumption $\lambda(\alpha) > \frac{1}{2}$ that $\lambda(\alpha) > \rho_0$ if $\lambda(\alpha_p) = \frac{4}{5}$, whence we conclude that $\lambda(\alpha_p) = \frac{2}{3}$. Let $d_1, \ldots, d_r$ be the dimensions of the primary Frobenius blocks of α_2 in increasing order. Then $d_1 > 2$, since otherwise $\lambda(\alpha) \leq \frac{2}{3}\cdot(1-\frac{1}{2^2}) = \frac{1}{2}$, a contradiction. Therefore, by Corollary 2.1.3, and using that $\prod_{n\geq m}(1-\frac{1}{2^n}) \geq \exp(-\frac{1}{2^{m-2}})$ for $m \in \mathbb{N}^+$ (see the proof of [Bors, 2016+, Corollary 2.3.4]), we find that $\lambda(\alpha) > \frac{2}{3}\cdot(1-\frac{1}{2^4})\cdot\prod_{p\geq 3}(1-\frac{1}{2^p}) > \frac{2}{3}\cdot\prod_{n=3,4,5}(1-\frac{1}{2^n})\cdot\exp(-\frac{1}{2^5}) > 0.51$, another contradiction.

For (c): Consider the following sequence $((G_n, \alpha_n))_{n\geq 0}$ of periodic FDGs: Set $G := \mathbb{Z}/5\mathbb{Z}$, let α be an order 4 automorphism on G, choose, for $i \in \mathbb{N}^+$, a monic primitive irreducible polynomial $P_i(X) \in \mathbb{F}_2[X]$ of degree p_i, the i-th prime (starting with $p_1 = 2$), and let (G_n, α_n) be the FDG product of (G, α) with the FDG given by $(\mathbb{Z}/2\mathbb{Z})^{p_1+\cdots+p_n}$ together with any automorphism having as primary Frobenius blocks the companion matrices of $P_1(X), \ldots, P_n(X)$. Then $\lambda(\alpha_n) = \frac{4}{5}\cdot\prod_{i=1}^{n}(1-\frac{1}{2^{p_i}})$, which converges to ρ_0 as $n \to \infty$. □

4 Concluding remarks

After having extensively studied the periodic FDGs (G, α) with $\lambda(\alpha) \geq \frac{1}{2}$ now, the following two questions about extensions of our results are near-lying:

Question 4.1. Can we extend our classification to finite groups or periodic FDGs whose λ-value is greater than ρ for some fixed $\rho < \frac{1}{2}$ as well? For example, what about $\rho = \frac{1}{3}$?

Question 4.2. Can we give any classification of finite groups G with $\lambda_{\mathrm{aff}}(G) > \rho$ for some fixed $\rho \in (0, 1)$? For example, what about $\rho = \frac{1}{2}$?

Each of these questions may serve as a starting point for further research. As for Question 4.2, we remark that, while having classified the *abelian* periodic gFDGs where all elements are moved in one cycle in Corollary 2.2.3, there do exist nonabelian groups having such a bijective affine map, too. For instance, it is not difficult to check that for the finite dihedral group $\mathrm{D}_{2n} = \langle r, x \mid r^n = x^2 = 1, xrx^{-1} = r^{-1}\rangle$, denoting by α the automorphism determined by $r \mapsto r, x \mapsto xr$, the bijective affine map $\mathrm{A}_{x,\alpha}$ moves all elements of D_{2n} in one cycle. Therefore, an implication of abelianity as for λ in [Bors, 2016+, Theorem 1.1.7] is excluded for λ_{aff} (and actually, even classifying the finite groups G with $\lambda_{\mathrm{aff}}(G) = 1$ does not seem trivial).

5 Acknowledgements

The author would like to thank Peter Hellekalek, Harald Niederreiter, Alina Ostafe and Igor Shparlinski for their many helpful comments.

References

[1] Bors, A. (2016+). Classification of finite group automorphisms with a large cycle. To appear in *Comm. Algebra*, arXiv:1410.2284 [math.GR].

[2] The GAP Group (2014). *GAP – Groups, Algorithms, and Programming. Version 4.7.5*. `http://www.gap-system.org`.

[3] Hegarty, P.V. (2003). On a conjecture of Zimmerman about group automorphisms. *Arch. Math. (Basel)* 80(1):1–11.

[4] Hegarty, P.V. (2009). Finite groups with an automorphism cubing a large fraction of elements. *Math Proc. R. Ir. Acad.* 109(1):79–99.

[5] Hernández-Toledo, R.A. (2005). Linear finite dynamical systems. *Comm. Algebra* 33(9):2977–2989.

[6] Hillar, C.J., Rhea, D.L. (2007). Automorphisms of finite abelian groups. *Amer. Math. Monthly* 114(10):917–923.

[7] Horoševskiĭ, M.V. (1974). On automorphisms of finite groups. *Math. USSR Sb.* 22(4):584–594.

[8] Knuth, D.E. (1998). *The art of computer programming. Vol. 2, Seminumerical algorithms*. 3rd ed. Reading, MA: Addison-Wesley.

[9] Lidl, R., Niederreiter, H. (1997). *Finite Fields*. 2nd ed. Cambridge: Cambridge University Press (Encyclopedia of Mathematics and its Applications, 20).

[10] Liebeck, H., MacHale, D. (1972). Groups with automorphisms inverting most elements. *Math. Z.* 124:51–63.

[11] Liebeck, H. (1973). Groups with an automorphism squaring many elements. *J. Austral. Math. Soc.* 16:33–42.

[12] MacHale, D. (1975). Groups with an automorphism cubing many elements. *J. Austral. Math. Soc.* 20(2):253–256.

[13] Miller, G.A. (1929). Groups which admit automorphisms in which exactly three-fourths of the operators correspond to their inverses. *Bull. Amer. Math. Soc.* 35(4):559–565.

[14] Potter, W.M. (1988). Nonsolvable groups with an automorphism inverting many elements. *Arch. Math. (Basel)* 50(4):292–299.