Journal of Algebra 633 (2023) 887–905

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Counting isomorphism classes of groups of Fibonacci type with a prime power number of generators

Esamaldeen Mohamed [a,1], Gerald Williams [b,*]

[a] *Department of Mathematics, Faculty of Education, Omar-Almukhtar University, Albyda, Libya*
[b] *Department of Mathematical Sciences, University of Essex, Wivenhoe Park, Colchester, Essex CO4 3SQ, UK*

A R T I C L E I N F O

Article history:
Received 12 September 2022
Available online 18 May 2023
Communicated by Eamonn O'Brien

MSC:
20F05

Keywords:
Cyclically presented group
Fibonacci group
Isomorphism

A B S T R A C T

Cavicchioli, O'Brien, and Spaggiari studied the number of isomorphism classes of irreducible groups of Fibonacci type as a function $\sigma(n)$ of the number of generators n. In the case $n = p^l$, where p is prime and $l \geq 1$, $n \neq 2, 4$, they conjectured a function $C(p^l)$, that is polynomial in p, for the value of $\sigma(p^l)$. We prove that $C(p^l)$ is an upper bound for $\sigma(p^l)$. We introduce a function $\tau(n)$ for the number of abelianised groups and conjecture a function $D(p^l)$, that is polynomial in p, for the value of $\tau(p^l)$, when $p^l \neq 2, 4, 5, 7, 8, 13, 23$. We prove that $D(p^l)$ is an upper bound for $\tau(p^l)$. We pose three questions that ask if particular pairs of groups with common abelianisations are non-isomorphic. We prove that if $\tau(p^l) = D(p^l)$ and each of these questions has a positive answer then $\sigma(p^l) = C(p^l)$.

* Corresponding author.
E-mail addresses: essamadeen.mohamed@omu.edu.ly (E. Mohamed), gerald.williams@essex.ac.uk (G. Williams).

[1] The first named author acknowledges financial support of the Libyan Government.

https://doi.org/10.1016/j.jalgebra.2023.04.032

1. Introduction

The *groups of Fibonacci type* are the groups defined by the following cyclic presentations:

$$G_n(m,k) = \langle\, x_0, \ldots, x_{n-1} \mid x_i x_{i+m} = x_{i+k}\ (0 \leq i < n)\,\rangle$$

(subscripts mod n) which were introduced independently in [14,3] for algebraic and topological reasons. They include the *Fibonacci groups* $F(2,n) = G_n(1,2)$ [7], the *Sieradski groups* $S(2,n) = G_n(2,1)$ [22], and the *Gilbert-Howie groups* $H(n,m) = G_n(m,1)$ [11]. With the exception of two challenging cases $H(9,4), H(9,7)$, the finite groups $G_n(m,k)$ and the aspherical defining presentations were classified in [11,2,23,4,8], the hyperbolic groups $G_n(m,k)$ were classified and the Tits alternative proved for the class of groups $G_n(m,k)$ in [5,6], the groups $G_n(m,k)$ that are 3-manifold groups were classified in [12]. The perfect groups $G_n(m,k)$ were classified in [20,24]. A partial classification of the groups $G_n(m,k)$ that are Labelled Oriented Graph groups was obtained in [19]. The shift dynamics of the groups $G_n(m,k)$ were studied in [15]. Isomorphisms of groups within this class were considered in [2,4,15]. See [25] for a 2012 survey. We say that the group $G_n(m,k)$ is *irreducible* if $0 < m,k < n$, $m \neq k$, and the greatest common divisor $(n,m,k) = 1$ (this is essentially the definition given in [2] except we omit the additional condition that $m < k$, which is unnecessary for our purposes); the irreducibility condition prevents $G_n(m,k)$ decomposing as a free product of $d = (n,m,k)$ copies of $G_{n/d}(m/d, k/d)$ [2, Lemma 1.2] (see also [9]).

The problem of determining the number of isomorphism classes of irreducible groups $G_n(m,k)$ as a function $\sigma(n)$ was investigated in [4] and, when n is a prime power, its value was conjectured. (A similar investigation was carried out in [17] for the cyclically presented groups with length three positive relators $x_i x_{i+k} x_{i+l}$.) For prime p and $l \geq 1$ let

$$C(p^l) = \begin{cases} p^{l-1}(p+1)/2 - 1 & \text{if } p \geq 3 \text{ is prime,} \\ 3 \cdot 2^{l-2} & \text{if } p = 2 \text{ and } l \geq 2. \end{cases} \tag{1}$$

Conjecture A *([4, Conjecture 8]). If $n \neq 2,4$ is a prime power then $\sigma(n) = C(n)$.*

The hypothesis $n \neq 2,4$ is necessary in Conjecture A since $\sigma(4) = 2 = C(4) - 1$ (and $C(2)$ is not defined). In [4] Conjecture A was confirmed for $n = 3,5,7,8,9,11,13,16,25,27$, and for $n \in \{17,19,23\}$ (the remaining prime powers at most 27) it was shown that $\sigma(n) \in \{C(n), C(n)-1\}$, with $\sigma(n) = C(n)$ if and only if $G_n(1,3) \not\cong G_n(4,5)$, and for prime powers n where $28 \leq n \leq 200$ it was confirmed that $\sigma(n) \leq C(n)$.

A powerful technique for proving non-isomorphism of pairs of cyclically presented groups is to compare abelianisations. For this reason we similarly consider the number of isomorphism classes of irreducible abelianised groups $G_n(m,k)^{\mathrm{ab}}$ as a function $\tau(n)$ and, when n is a prime power, conjecture its value. For prime p and $l \geq 1$ let

$$D(p^l) = \begin{cases} p^{l-1}(p+1)/2 - 2 & \text{if } p \geq 5, \\ 2 \cdot 3^{l-1} - 1 & \text{if } p = 3, \\ 2^{l-1} + 1 & \text{if } p = 2 \text{ and } l \geq 2. \end{cases} \quad (2)$$

Conjecture B. *If $n \neq 2, 4, 5, 7, 8, 13, 23$ is a prime power then $\tau(n) = D(n)$.*

Note that $C(p^l) = D(p^l) + 1$ if $p \geq 5$ is prime, $C(p^l) = D(p^l)$ if $p = 3$ and $C(p^l) = 3(D(p^l)-1)/2$ if $p = 2$. The hypothesis $n \neq 2, 4, 5, 7, 8, 13, 23$ is necessary in Conjecture B since $\tau(n) = D(n) - 1$ for $n \in \{4, 23\}$, $\tau(n) = D(n) + 1$ for $n \in \{5, 7, 8, 13\}$, and $D(2)$ is not defined. The suggestion that for odd prime powers $n > 23$, $\tau(n) = C(n)$ or $C(n) - 1$ was essentially made in [4, Section 5.1] and confirmed for $n \leq 200$.

In support of Conjectures A, B our next two results prove that $C(n)$ is an upper bound for $\sigma(n)$ and, with a few exceptions, $D(n)$ is an upper bound for $\tau(n)$. (The functions $\sigma_i(n), \tau_i(n), C_i(n), D_i(n)$ $(i = 1, 2)$ will be introduced in Section 2.)

Theorem C. *Let $n \neq 2$ be a prime power. Then $\sigma_1(n) \leq C_1(n)$, $\sigma_2(n) \leq C_2(n)$, and hence $\sigma(n) \leq C(n)$.*

Theorem D. *Let $n \neq 2, 5, 7, 8, 13$ be a prime power. Then $\tau_1(n) \leq D_1(n)$, $\tau_2(n) \leq D_2(n)$, and hence $\tau(n) \leq D(n)$.*

In the case where n is prime Theorem C was proved in [4, Proposition 7]. In Section 6 we provide computational evidence that (for $n \neq 4, 23$) $D(n)$ is a lower bound for $\tau(n)$ (and hence for $\sigma(n)$). Supposing the truth of Conjecture B, in the next result we give necessary and sufficient conditions for the truth of Conjecture A (here k^{-1} denotes the inverse of $k \bmod n$ and we exclude the values $n = 2, 4, 5, 7, 8, 13, 23$ because the hypothesis $\tau(n) = D(n)$ does not hold in those cases):

Theorem E. *Let $n \neq 2, 4, 5, 7, 8, 13, 23$ be a power of a prime p and suppose $\tau(n) = D(n)$. Then $\sigma(n) = C(n)$ if and only if one of the following holds:*

(a) *$p \geq 5$ and $G_n(1,3) \not\cong G_n(4,5)$; or*
(b) *$p = 3$; or*
(c) *$p = 2$ and*
   (i) *$G_n(n/2,1) \not\cong G_n(n/4,1)$; and*
   (ii) *$G_n(1,k) \not\cong G_n(1,k^{-1})$ for all odd $3 \leq k \leq n-3$, where $k \neq n/2 \pm 1$.*

Thus, by Theorem E (and [4] for the excluded values of n), if Conjecture B holds, then Conjecture A holds if and only if each of the following questions has a positive answer:

Question 1.1. Is $G_{2^l}(1,k) \not\cong G_{2^l}(1,k^{-1})$ for all $l \geq 4$ and all odd k where $3 \leq k \leq 2^l - 3$, $k \neq 2^{l-1} \pm 1$?

Question 1.2. Is $G_{2^l}(2^{l-1},1) \not\cong G_{2^l}(2^{l-2},1)$ for all $l \geq 4$?

Question 1.3. Is $G_n(1,3) \not\cong G_n(4,5)$ for all prime powers $n \neq 5,7,13$ that are coprime to 6?

In Example 4.3 we show that Question 1.1 has a positive answer for $l = 4$; in Example 5.2 we show that Question 1.2 has a positive answer for $4 \leq l \leq 6$; and in Example 5.7 we show that Question 1.3 has a positive answer for $n = 11, 25$.

All isomorphisms stated in this paper can be obtained by applying (possibly repeatedly) the following proposition:

Proposition 1.4 *([4, Proposition 6], [2, Lemmas 1.1(3),1.3]).*

(a) $G_n(m,k) \cong G_n(m,n+m-k) \cong G_n(n-m,n-m+k)$;
(b) *if* $(n,t) = 1$ *then* $G_n(m,k) \cong G_n(mt,kt)$.

Further isomorphism theorems for the groups $G_n(m,k)$ were provided in [2, Theorem 1.1], [4, Theorem 2] (see also [16, Corollary 2]) and in [15, Lemma 3.2].

We make frequent use of the following expression for the order of the abelianisation:

$$|G_n(m,k)^{\mathrm{ab}}| = |\mathrm{Res}(f,g)| \tag{3}$$

where $f(t) = t^m - t^k + 1$ is the *representer polynomial* of $G_n(m,k)$, $g(t) = t^n - 1$, and $\mathrm{Res}(\cdot,\cdot)$ denotes the resultant [13, page 82].

2. Refining Conjectures A and B

For a group G we let $[G]$ denote the isomorphism class of G and for $n \geq 1$ we define

$$S(n) = \{[G_n(m,k)] \mid 0 < m,k < n, m \neq k, (n,m,k) = 1\},$$
$$T(n) = \{[G_n(m,k)^{\mathrm{ab}}] \mid 0 < m,k < n, m \neq k, (n,m,k) = 1\},$$

and set $\sigma(n) = |S(n)|,\ \tau(n) = |T(n)|$ (so $\tau(n) \leq \sigma(n)$). For a prime p and $l \geq 1$, where $p^l > 2$, we introduce the following notation:

$$S_1(p^l) = \{[G_{p^l}(m,k)] \mid 0 < m,k < p^l, m \neq k, (p^l,m,k) = 1, p|m\},$$
$$S_2(p^l) = \{[G_{p^l}(m,k)] \mid 0 < m,k < p^l, m \neq k, (p^l,m,k) = 1, p \nmid m\},$$
$$T_1(p^l) = \{[G_{p^l}(m,k)^{\mathrm{ab}}] \mid 0 < m,k < p^l, m \neq k, (p^l,m,k) = 1, p|m\},$$
$$T_2(p^l) = \{[G_{p^l}(m,k)^{\mathrm{ab}}] \mid 0 < m,k < p^l, m \neq k, (p^l,m,k) = 1, p \nmid m\},$$

and set $\sigma_1(p^l) = |S_1(p^l)|$, $\sigma_2(p^l) = |S_2(p^l)|$, $\tau_1(p^l) = |T_1(p^l)|$, $\tau_2(p^l) = |T_2(p^l)|$ (so $\tau_1(p^l) \leq \sigma_1(p^l)$, $\tau_2(p^l) \leq \sigma_2(p^l)$). Then

$$\begin{aligned} S(p^l) &= S_1(p^l) \cup S_2(p^l), \\ T(p^l) &= T_1(p^l) \cup T_2(p^l), \\ \sigma(p^l) &= \sigma_1(p^l) + \sigma_2(p^l) - |S_1(p^l) \cap S_2(p^l)|, \\ \tau(p^l) &= \tau_1(p^l) + \tau_2(p^l) - |T_1(p^l) \cap T_2(p^l)|. \end{aligned}$$

In addition to the functions $C(p^l), D(p^l)$ defined at (1), (2) we set

$$C_1(p^l) = \begin{cases} (p^{l-1} - 1)/2 & \text{if } p \geq 3 \text{ is prime}, \\ 2^{l-2} + 1 & \text{if } p = 2 \text{ and } l \geq 2, \end{cases}$$

$$C_2(p^l) = \begin{cases} (p^{l} - 1)/2 & \text{if } p \geq 3 \text{ is prime}, \\ 2^{l-1} - 1 & \text{if } p = 2 \text{ and } l \geq 2, \end{cases}$$

$$D_1(p^l) = \begin{cases} (p^{l-1} - 1)/2 & \text{if } p \geq 3 \text{ is prime}, \\ 2^{l-2} & \text{if } p = 2 \text{ and } l \geq 2, \end{cases}$$

$$D_2(n) = \begin{cases} (p^{l} - 3)/2 & \text{if } p \geq 5 \text{ is prime}, \\ (3^l - 1)/2 & \text{if } p = 3, \\ 2^{l-2} + 1 & \text{if } p = 2 \text{ and } l \geq 2. \end{cases}$$

We note the following: $C(p^l) = C_1(p^l) + C_2(p^l)$ and $D(p^l) = D_1(p^l) + D_2(p^l)$; if $p \geq 5$ then $C_1(p^l) = D_1(p^l)$ and $C_2(p^l) = D_2(p^l) + 1$; if $p = 3$ then $C_1(p^l) = D_1(p^l)$ and $C_2(p^l) = D_2(p^l)$; and if $p = 2$ then $C_1(p^l) = D_1(p^l) + 1$ and $C_2(p^l) = 2D_2(p^l) - 3$. Note also that $S_1(p^l) = T_1(p^l) = \emptyset$ if $l = 1$, so we often only consider $S_1(p^l), T_1(p^l)$, $\sigma_1(p^l), \tau_1(p^l)$ when $l \geq 2$.

In Corollaries 3.3 and 5.11 we show that (once $C(n), D(n)$ have been established as upper bounds for $\sigma(n), \tau(n)$, respectively) Conjectures A and B are, respectively, equivalent to the following conjectures:

Conjecture A′. *Suppose $n \neq 2, 4$ is a prime power. Then $S_1(n) \cap S_2(n) = \emptyset$, $\sigma_1(n) = C_1(n)$, and $\sigma_2(n) = C_2(n)$.*

Conjecture B′. *Suppose $n \neq 2, 4, 5, 7, 8, 13, 23$ is a prime power. Then $T_1(n) \cap T_2(n) = \emptyset$, $\tau_1(n) = D_1(n)$, and $\tau_2(n) = D_2(n)$.*

(Note that if $T_1(n) \cap T_2(n) = \emptyset$, as in Conjecture B′, then $S_1(n) \cap S_2(n) = \emptyset$, as in Conjecture A′.) Theorem C (stated in the Introduction) will show that (for $n \neq 2$) $C_1(n), C_2(n)$ are upper bounds for $\sigma_1(n), \sigma_2(n)$, respectively; and Theorem D will show that (for $n \neq 2,4,5,7,8,13$) $D_1(n), D_2(n)$ are upper bounds for $\tau_1(n), \tau_2(n)$, respectively. In Section 6 we provide computational evidence that they are also lower bounds for $\tau_1(n), \tau_2(n)$. The proof of Theorem D depends on Corollary 4.2, Lemma 5.1, and Lemma 5.5, which we now describe.

Corollary 4.2 will show that if $n = 2^l$ and k is odd then $G_n(1,k)^{\mathrm{ab}} \cong G_n(1,k^{-1})^{\mathrm{ab}}$, prompting Question 1.1 which asks if, nevertheless, the groups themselves are non-isomorphic. Lemma 5.1 will show, in particular, that if $n = 2^l$, $l \geq 4$ then $G_n(n/2,1)^{\mathrm{ab}} \cong G_n(n/4,1)^{\mathrm{ab}}$, prompting Question 1.2 which asks if the groups themselves are non-isomorphic. Lemma 5.5 will show, in particular, that if $n = p^l \geq 5$ where $p \geq 5$ is prime, then $G_n(1,3)^{\mathrm{ab}} \cong G_n(4,5)^{\mathrm{ab}}$, prompting Question 1.3 which asks if the groups themselves are non-isomorphic. (We ask Questions 1.2 and 1.3 for prime powers n, but they could reasonably be asked for all n divisible by 16, and all n coprime to 6, respectively.)

3. Upper bound for $\sigma(p^l)$

In this section we prove Theorem C.

3.1. Upper bound for $\sigma_1(p^l)$

Lemma 3.1. *Let $n = p^l$ where $p \geq 2$ is prime and $l \geq 2$. If $p \geq 3$ then*

$$S_1(n) = \{[G_n(\min(pi, pi(pi-1)^{-1} \bmod n), 1)] \mid 1 \leq i < p^{l-1}\}$$

and if $p = 2$ then

$$S_1(n) = \{[G_n(2,1)], [G_n(2^{l-1},1)], [G_n(2^{l-1}+2,1)]\} \cup \\ \{[G_n(\min(2i, 2i(2i-1)^{-1} \bmod n), 1)] \mid 2 \leq i < 2^{l-1}, i \neq 2^{l-2}, 2^{l-2}+1\}.$$

Hence $\sigma_1(n) \leq C_1(n)$.

Proof. Suppose $p|m$, $0 < m,k < n$, $m \neq k$ and let $G = G_n(m,k)$. Since $1 = (n,m,k) = (m,k)$ we have $p \nmid k$ so $(n,k) = 1$ so $G \cong G_n(mk^{-1},1)$ (where k^{-1} denotes the multiplicative inverse of k mod n). Therefore $G \cong G_n(pi,1)$ for some $1 \leq i < p^{l-1}$. Now $G_n(pi,1) \cong G_n(pi,pi-1)$. But $(pi-1,n) = 1$ so $(pi-1)$ has a multiplicative inverse $(pi-1)^{-1} \bmod p^l$. Then $G_n(pi,pi-1) \cong G_n(pi(pi-1)^{-1},1)$. That is, $G_n(pi,1) \cong G_n(pi(pi-1)^{-1},1)$. Therefore

$$S_1(n) = \{[G_n(\min(pi, pi(pi-1)^{-1} \bmod n), 1)] \mid 1 \leq i < p^{l-1}\}.$$

We now give an upper bound for the size of this set, and therefore of $\sigma_1(n)$. Suppose

$$pi \equiv pi(pi-1)^{-1} \bmod p^l. \tag{4}$$

Then (working mod p^l), with $1 \leq i < p^{l-1}$, the congruence (4) implies

$$pi(pi-2) \equiv 0 \bmod p^l. \tag{5}$$

Hence, since $l > 1$ and $1 \leq i < p^{l-1}$, p divides $(pi-2)$, so $p|2$, i.e. $p = 2$. Then (5) implies $4i(i-1) \equiv 0 \bmod 2^l$, so $i(i-1) \equiv 0 \bmod 2^{l-2}$, and hence $i \equiv 0 \bmod 2^{l-2}$ or $i-1 \equiv 0 \bmod 2^{l-2}$. That is, $i = 2^{l-2}$ or $i = 1$ or $i = 2^{l-2}+1$.

Therefore, if $p \geq 3$ then $\sigma_1(n) = |S_1(n)| \leq (p^{l-1}-1)/2 = C_1(n)$ and if $p = 2$ and $l \geq 2$ then

$$\begin{aligned} S_1(n) =& \{[G_n(2i,1)] \mid i \in \{1, 2^{l-2}, 2^{l-2}+1\}\} \cup \\ & \{[G_n(\min(2i, 2i(2i-1)^{-1} \bmod n), 1)] \mid 2 \leq i < 2^{l-1}, i \neq 2^{l-2}, 2^{l-2}+1\} \\ =& \{[G_n(2,1)], [G_n(2^{l-1},1)], [G_n(2^{l-1}+2,1)]\} \cup \\ & \{[G_n(\min(2i, 2i(2i-1)^{-1} \bmod n), 1)] \mid 2 \leq i < 2^{l-1}, i \neq 2^{l-2}, 2^{l-2}+1\} \end{aligned}$$

so $\sigma_1(n) = |S_1(n)| \leq 3 + (2^{l-1}-2-2)/2 = 2^{l-2}+1 = C_1(n)$, as required. □

3.2. Upper bound for $\sigma_2(p^l)$

Lemma 3.2. *Let $n = p^l$ where $p \geq 2$ is prime and $l \geq 1$.*

(a) *If $p \geq 3$ then $S_2(n) = \{[G_n(1,k)] \mid 2 \leq k \leq (p^l+1)/2\}$.*
(b) *If $p = 2$ then $S_2(n) = \{[G_n(1,k)] \mid 2 \leq k < 2^l,\ k \text{ odd}\}$.*

Hence $\sigma_2(n) \leq C_2(n)$.

Proof. If $G \in S_2(n)$ then $G \cong G_n(m,k)$ for some $m \neq k$ where $(n,m,k) = 1$ and $p \nmid m$. Therefore $(m,n) = 1$ so G is isomorphic to $G_n(1,k')$ for some $2 \leq k' < n$.

Suppose $p \geq 3$. If $(p^l+1)/2 \leq k' < n$ then $k'' = p^l+1-k'$ satisfies $2 \leq k'' \leq (p^l+1)/2$ and $G_n(1,k') \cong G_n(1,k'')$ so k' can be chosen to be one of the $C_2(n) = (p^l-1)/2$ values in the range $2 \leq k' \leq (p^l+1)/2$. Suppose then $p = 2$. If $1 < k < 2^l$ is even, then $n+1-k$ is odd and since $G_n(1,k) \cong G_n(1,n+1-k)$ we may assume k is odd, giving at most $C_2(n) = 2^{l-1}-1$ values for k. □

3.3. Proof of Theorem C and the equivalence of Conjectures A and A′

Proof of Theorem C. Lemmas 3.1 and 3.2 imply

$$\begin{aligned} \sigma(n) &= \sigma_1(n) + \sigma_2(n) - |S_1(n) \cap S_2(n)| \\ &\leq \sigma_1(n) + \sigma_2(n) \\ &\leq C_1(n) + C_2(n) \end{aligned}$$

$$= C(n). \quad \square$$

We now show that Conjectures A and A′ are equivalent.

Corollary 3.3. *Suppose $n \neq 2, 4$ is a prime power. Then $\sigma(n) = C(n)$ if and only if $S_1(n) \cap S_2(n) = \emptyset$, $\sigma_1(n) = C_1(n)$, and $\sigma_2(n) = C_2(n)$.*

Proof. Suppose first $S_1(n) \cap S_2(n) = \emptyset$, $\sigma_1(n) = C_1(n)$, and $\sigma_2(n) = C_2(n)$. Then

$$\begin{aligned}\sigma(n) &= \sigma_1(n) + \sigma_2(n) - |S_1(n) \cap S_2(n)| \\ &= \sigma_1(n) + \sigma_2(n) \\ &= C_1(n) + C_2(n) = C(n).\end{aligned}$$

Suppose then $\sigma(n) = C(n)$. Then

$$\begin{aligned}C(n) &= \sigma_1(n) + \sigma_2(n) - |S_1(n) \cap S_2(n)| \\ &\leq C_1(n) + C_2(n) - |S_1(n) \cap S_2(n)| \\ &= C(n) - |S_1(n) \cap S_2(n)|\end{aligned}$$

(where we used Theorem C for the inequality), and hence $S_1(n) \cap S_2(n) = \emptyset$. If $\sigma_1(n) < C_1(n)$ or $\sigma_2(n) < C_2(n)$ then

$$\begin{aligned}C(n) &= \sigma_1(n) + \sigma_2(n) \\ &< C_1(n) + C_2(n) \\ &= C(n)\end{aligned}$$

(again using Theorem C), a contradiction. Therefore $\sigma_1(n) = C_1(n)$ and $\sigma_2(n) = C_2(n)$. $\square$

4. An isomorphism theorem for abelianised groups $G_n(m,k)^{\mathrm{ab}}$

Theorem 4.1. *Let $n \geq 2$ be even, $0 < m, k < n$, where m is odd, and suppose $(\alpha, n) = 1$, where α is odd. Then*

$$G_n(m,k)^{\mathrm{ab}} \cong \begin{cases} G_n(\alpha(k-m), n-\alpha m)^{\mathrm{ab}} & \text{if } k \text{ is even,} \\ G_n(\alpha k, \alpha m)^{\mathrm{ab}} & \text{if } k \text{ is odd.}\end{cases}$$

Proof. For each $0 \leq j < n$ let $y_j = x_{\alpha^{-1}j \bmod n}$ if j is even and $y_j = x^{-1}_{\alpha^{-1}j \bmod n}$ if j is odd (where α^{-1} denotes the multiplicative inverse of α mod n). If αi mod n is even then $y_{\alpha i \bmod n} = x_i$ and $y_{\alpha i \bmod n} = x_i^{-1}$ otherwise. Since n is even, αi mod n is even if and only if i is even. Thus, $x_i = y_{\alpha i \bmod n}$ if i is even and $x_i = y^{-1}_{\alpha i \bmod n}$ if i is odd, i.e.

$x_i = y_{\alpha i \bmod n}^{(-1)^i}$. For the remainder of the proof, subscripts of generators x_i, y_i are to be taken $\bmod\, n$.

Writing $j = \alpha i \bmod n$, the i-th relation of $G_n(x_0 x_m x_k^{-1})^{\mathrm{ab}}$ is

$$x_i x_{i+m} x_{i+k}^{-1} = y_j^{(-1)^i} y_{j+\alpha m}^{(-1)^{(i+m)}} y_{j+\alpha k}^{-(-1)^{(i+k)}}$$

$$= \begin{cases} y_j y_{j+\alpha m}^{-1} y_{j+\alpha k}^{-1} & \text{if } k \text{ is even and } i \text{ is even,} \\ y_j^{-1} y_{j+\alpha m} y_{j+\alpha k} & \text{if } k \text{ is even and } i \text{ is odd,} \\ y_j y_{j+\alpha m}^{-1} y_{j+\alpha k} & \text{if } k \text{ is odd and } i \text{ is even,} \\ y_j^{-1} y_{j+\alpha m} y_{j+\alpha k}^{-1} & \text{if } k \text{ is odd and } i \text{ is odd.} \end{cases}$$

Cyclically permuting and inverting relators, and commuting generators, if required, the set of these relators is equivalent to the set of the following relators:

$$\begin{cases} y_j y_{j+\alpha(k-m)} y_{j+n-\alpha m}^{-1} & \text{if } k \text{ is even,} \\ y_j y_{j+\alpha k} y_{j+\alpha m}^{-1} & \text{if } k \text{ is odd,} \end{cases}$$

which are the relators of $G_n(\alpha(k-m), n-\alpha m)^{\mathrm{ab}}, G_n(\alpha k, \alpha m)^{\mathrm{ab}}$ respectively. □

Restricting to the case $n = 2^l$, $m = 1$, and odd k, by setting $\alpha = k^{-1} \bmod n$, we obtain the following corollary.

Corollary 4.2. *If $n = 2^l$, $l \geq 2$, $0 < k < n$, where k is odd, then $G_n(1,k)^{\mathrm{ab}} \cong G_n(1,k^{-1})^{\mathrm{ab}}$.*

Noting that for $n = 2^l$, $k \equiv k^{-1} \bmod n$ if and only if $k \equiv n/2 \pm 1$ or $\pm 1 \bmod n$, Corollary 4.2 prompts Question 1.1 which asks if $G_n(1,k) \not\cong G_n(1,k^{-1})$ for odd $k \not\equiv n/2 \pm 1 \bmod n$. The next example (which is implicit in [4, Section 5.1]) gives an affirmative answer for $n = 16$.

Example 4.3 *($G_{16}(1,3) \not\cong G_{16}(1,11)$, $G_{16}(1,5) \not\cong G_{16}(1,13)$).* Computations in GAP [10] show that the second derived quotients of $G_{16}(1,3)$ and $G_{16}(1,11)$ are $\mathbb{Z}_3^4$ and $\mathbb{Z}_3^{20}$, respectively, so $G_{16}(1,3) \not\cong G_{16}(1,11)$. Similarly, the second derived quotients of $G_{16}(1,5)$ and $G_{16}(1,13)$ are $\mathbb{Z}_4^8 \oplus \mathbb{Z}_{17}^{25} \oplus \mathbb{Z}^{16}$ and $\mathbb{Z}_4^8 \oplus \mathbb{Z}_{17}^{10} \oplus \mathbb{Z}_{289}$, respectively, so $G_{16}(1,5) \not\cong G_{16}(1,13)$.

5. Upper bound for $\tau(p^l)$

In this section we prove Theorem D.

5.1. Upper bound for $\tau_1(p^l)$

For $p \geq 3$, and since $\tau_1(p^l) \leq \sigma_1(p^l)$, Lemma 3.1 implies $\tau_1(p^l) \leq C_1(p^l) = D_1(p^l)$. Therefore it remains to consider the case $p = 2$. First we obtain a coincidence in abelianisations:

Lemma 5.1. *If n is even then $G_n(n/2,1)^{\mathrm{ab}} \cong \mathbb{Z}_{2^{n/2}-1}$ and if $16|n$ then $G_n(n/4,1)^{\mathrm{ab}} \cong \mathbb{Z}_{2^{n/2}-1}$.*

Proof. In the group $G_n(n/2,1)^{\mathrm{ab}}$ the i-th relation $x_i x_{i+n/2} = x_{i+1}$ and $(i+n/2)$-th relation $x_{i+n/2}x_i = x_{i+n/2+1}$ combine to show $x_{i+1} = x_{i+n/2+1}$, so $x_i = x_{i+n/2}$ for each $0 \leq i < n$. Therefore

$$\begin{aligned} G_n(n/2,1)^{\mathrm{ab}} &= \langle\, x_0,\ldots,x_{n-1} \mid x_i x_{i+n/2} = x_{i+1}, x_i = x_{i+n/2}\ (0 \leq i < n)\,\rangle^{\mathrm{ab}} \\ &= \langle\, x_0,\ldots,x_{n/2-1} \mid x_i x_i = x_{i+1}\ (0 \leq i < n/2)\,\rangle^{\mathrm{ab}} \\ &= G_{n/2}(0,1)^{\mathrm{ab}} \\ &\cong \mathbb{Z}_{2^{n/2}-1} \end{aligned}$$

by [2, Lemma 1.1(1)], thus proving the first statement.

We now consider the groups $G_n(n/4,1)^{\mathrm{ab}}$. We first show $|G_n(n/4,1)^{\mathrm{ab}}| = 2^{n/2}-1$, then show that there is an epimorphism from $G_n(n/4,1)^{\mathrm{ab}}$ onto $\mathbb{Z}_{2^{n/4}+1} \oplus \mathbb{Z}_{2^{n/4}-1} \cong \mathbb{Z}_{2^{n/2}-1}$ and so $G_n(n/4,1)^{\mathrm{ab}} \cong \mathbb{Z}_{2^{n/2}-1}$. Now

$$\begin{aligned} |G_n(n/4,1)^{\mathrm{ab}}| &= |\mathrm{Res}(1-t+t^{n/4}, t^n-1)| \\ &= |\mathrm{Res}(1-t+t^{n/4}, (t^{n/2}-1)(t^{n/2}+1))| \\ &= |\mathrm{Res}(1-t+t^{n/4}, t^{n/2}-1)| \cdot |\mathrm{Res}(1-t+t^{n/4}, t^{n/2}+1)| \\ &= |G_{n/2}(n/4,1)^{\mathrm{ab}}| \cdot |\mathrm{Res}(1-t+t^{n/4}, t^{n/2}+1)| \\ &= (2^{n/4}-1) \cdot |\mathrm{Res}(1-t+t^{n/4}, t^{n/2}+1)| \end{aligned}$$

by replacing n by $n/2$ in the first statement of the lemma and taking the order. Now

$$\begin{aligned} |\mathrm{Res}(1-t+t^{n/4}, t^{n/2}+1)| &= |\mathrm{Res}((1+t^{n/4})-t, (t^{n/4}-\sqrt{-1})(t^{n/4}+\sqrt{-1}))| \\ &= |\mathrm{Res}((1+\sqrt{-1})-t, t^{n/4}-\sqrt{-1})| \\ &\quad \cdot |\mathrm{Res}((1-\sqrt{-1})-t, t^{n/4}+\sqrt{-1})| \\ &= ((1+\sqrt{-1})^{n/4}-\sqrt{-1}) \cdot ((1-\sqrt{-1})^{n/4}+\sqrt{-1}) \\ &= 2^{n/4}+1 \end{aligned}$$

(since $16|n$). Therefore $|G_n(n/4,1)^{\mathrm{ab}}| = (2^{n/4}-1)\cdot(2^{n/4}+1) = 2^{n/2}-1$, as required.

Now let

$$\phi : G_n(n/4,1)^{\mathrm{ab}} \to \mathbb{Z}_{2^{n/4}+1} \oplus \mathbb{Z}_{2^{n/4}-1}$$

be given by

$$\phi(x_i) = ((2^{n/8}+1)^i, 2^i)$$

for each $0 \le i < n$. Then, for each $0 \le i < n$, $\phi(x_i x_{i+n/4} x_{i+1}^{-1}) = (0,0)$, so ϕ is a homomorphism, and since $\phi(x_0) = (1,1)$, which generates $\mathbb{Z}_{2^{n/4}+1} \oplus \mathbb{Z}_{2^{n/4}-1}$, we deduce that ϕ is an epimorphism, as required. □

Lemma 5.1 prompts Question 1.2 which asks if (for $n = 2^l$, where $l \ge 4$) $G_n(n/2,1) \not\cong G_n(n/4,1)$. The following example gives a positive answer in the cases $4 \le l \le 6$ (the case $l = 4$ being implicit in [4, Section 5.1]); note, however, that these are the only cases where we have been able to answer Question 1.2.

Example 5.2 *($G_{2^l}(2^{l-2},1) \not\cong G_{2^l}(2^{l-1},1)$ for $4 \le l \le 6$).* Computations in GAP show that if $l = 4,5,6$ then each of $G_{2^l}(2^{l-1},1), G_{2^l}(2^{l-2},1)$ has a unique index 3 subgroup, and these index 3 subgroups have non-isomorphic abelianisations so $G_{2^l}(2^{l-1},1) \not\cong G_{2^l}(2^{l-2},1)$. The same argument also shows that $G_{48}(1,24) \not\cong G_{48}(1,12)$.

We now show that $D_1(2^l)$ is an upper bound for $\tau_1(2^l)$ when $l \ge 4$. (Note that $\tau_1(8) = D_1(8)+1$, $\tau_1(4) = D_1(4)-1$.)

Lemma 5.3. *Let $n = 2^l$ where $l \ge 4$. Then*

$$T_1(n) = \{[G_n(\min(2i, 2i(2i-1)^{-1} \bmod n), 1)^{\mathrm{ab}}] \mid 2 \le i < 2^{l-1}, i \ne 2^{l-2}+1\}.$$

Hence $\tau_1(n) \le D_1(n)$. Moreover, if $\tau_1(n) = D_1(n)$ then $\sigma_1(n) = C_1(n)$ if and only if $G_n(n/2,1) \not\cong G_n(n/4,1)$.

Proof. By Lemma 3.1

$$T_1(n) = \{[G_n(\min(2i, 2i(2i-1)^{-1} \bmod n), 1)^{\mathrm{ab}}] \mid 2 \le i < 2^{l-1}, i \ne 2^{l-2}, 2^{l-2}+1\}.$$

But by Lemma 5.1 $G_n(2^{l-2},1)^{\mathrm{ab}} \cong G_n(2^{l-1},1)^{\mathrm{ab}}$. The first of these groups corresponds to the value $i = 2^{l-3}$, and the second corresponds to $i = 2^{l-2}$. Therefore we may remove $i = 2^{l-2}$ from the set above to get the set in the statement, and hence $\tau_1(n) \le C_1(n) - 1 = D_1(n)$.

Now suppose $\tau_1(n) = D_1(n)$. Then $\sigma_1(n) > \tau_1(n) = D_1(n)$ if and only if $G_n(2^{l-2},1) \not\cong G_n(2^{l-1},1)$; that is, $\sigma_1(n) = C_1(n)$ if and only if $G_n(n/2,1) \not\cong G_n(n/4,1)$, as required. □

5.2. Upper bound for $\tau_2(p^l)$

For $p = 3$ Lemma 3.2 implies $\tau_2(p^l) \le \sigma_2(p^l) \le C_2(p^l) = D_2(p^l)$. Therefore it remains to consider the case $p \ge 5$ and the case $p = 2$.

5.2.1. Upper bound for $\tau_2(p^l)$ where $p \ge 5$

In this section (in Corollary 5.6) we show that $D_2(p^l)$ is an upper bound for $\tau_2(p^l)$ in the case $p \ge 5$, $p^l \ne 5, 7, 13$. For prime $p \ge 3$, and $l \ge 1$ let

$$\kappa = \begin{cases} (p^l + 5)/4 & \text{if } p^l \equiv 3 \bmod 4, \\ (p^l - 1)/4 & \text{if } p^l \equiv 1 \bmod 4, \end{cases} \tag{6}$$

and note that $\kappa = 3$ if and only if $p^l = 7$ or 13.

Lemma 5.4. *Let $n = p^l$, where $p \ge 3$ is prime, $l \ge 1$ and let κ be as defined at (6). Then $G_n(1, \kappa) \cong G_n(4, 5)$.*

Proof. First suppose $p^l \equiv 3 \bmod 4$. Then $4((p^l + 1)/4) \equiv 1 \bmod n$ so

$$G_n(4, 5) \cong G_n(1, 5(p^l + 1)/4) = G_n(1, (p^l + 5)/4) = G_n(1, \kappa).$$

Now suppose $p^l \equiv 1 \bmod 4$. Then $4((3p^l + 1)/4) \equiv 1 \bmod n$ so

$$\begin{aligned} G_n(4, 5) &\cong G_n(1, 5((3p^l + 1)/4)) = G_n(1, (3p^l + 1)/4 + 1) \\ &\cong G_n(1, p^l + 1 - ((3p^l + 1)/4 + 1)) = G_n(1, (p^l - 1)/4) = G_n(1, \kappa), \end{aligned}$$

as required. □

Lemma 5.5. *If $n \ge 2$ and $(n, 6) = 1$ (in particular, if $p \ge 5$ is prime and $n = p^l$ for $l \ge 1$) then $G_n(1, 3)^{\mathrm{ab}} \cong G_n(4, 5)^{\mathrm{ab}}$.*

We give two proofs of Lemma 5.5. The first is a direct argument using Tietze transformations, but involves pulling a rabbit out of a hat in the second equality. The second requires the use of matrices in companion rings, and provides the insight that led to the first proof. (Essentially, the expression of the relators $x_i x_{i+4} x_{i+5}^{-1}$ in the form $y_{i+2} y_{i+1}^{-1} y_i$ where $y_i = x_i x_{i+1} x_{i+3}^{-1}$ in the first proof is the group presentation equivalent of the factorisation of the representer polynomial $1 + t^4 - t^5 = (t^2 - t + 1)(1 + t - t^3)$.)

Proof of Lemma 5.5 using Tietze transformations.

$$\begin{aligned} G_n(4, 5)^{\mathrm{ab}} &= \langle\, x_i \mid x_i x_{i+4} x_{i+5}^{-1}\ (0 \le i < n)\,\rangle^{\mathrm{ab}} \\ &= \langle\, x_i \mid (x_{i+2} x_{i+3} x_{i+5}^{-1})(x_{i+1} x_{i+2} x_{i+4}^{-1})^{-1}(x_i x_{i+1} x_{i+3}^{-1})\ (0 \le i < n)\,\rangle^{\mathrm{ab}} \\ &= \langle\, x_i, y_i \mid y_{i+2} y_{i+1}^{-1} y_i, y_i = x_i x_{i+1} x_{i+3}^{-1}\ (0 \le i < n)\,\rangle^{\mathrm{ab}}. \end{aligned}$$

For every i, the relators $y_{i+2}y_{i+1}^{-1}y_i$ and $y_{i+3}y_{i+2}^{-1}y_{i+1}$ imply $y_i = y_{i+3}^{-1}$ and hence $y_i = y_{i+6}$. Since $(n,6) = 1$ the sequence of equalities $y_0 = y_6 = y_{12} = \cdots = y_{6(n-1)} = y_0$ includes each $y_0, \ldots, y_{n-1}$ so $y_i = y_0$ for all $0 \leq i < n$. Therefore

$$\begin{aligned} G_n(4,5)^{\mathrm{ab}} &= \langle\, x_i, y_i \mid y_{i+2}y_{i+1}^{-1}y_i, y_i = x_i x_{i+1} x_{i+3}^{-1}, y_i = y_0 \ (0 \leq i < n)\, \rangle^{\mathrm{ab}} \\ &= \langle\, x_i, y_0 \mid y_0 y_0^{-1} y_0, y_0 = x_i x_{i+1} x_{i+3}^{-1} \ (0 \leq i < n)\, \rangle^{\mathrm{ab}} \\ &= \langle\, x_i \mid 1 = x_i x_{i+1} x_{i+3}^{-1} \ (0 \leq i < n)\, \rangle^{\mathrm{ab}} \\ &= G_n(1,3)^{\mathrm{ab}}. \quad \square \end{aligned}$$

Proof of Lemma 5.5 using matrices in companion rings. The representer polynomial of $G_n(4,5)$ is $f(t) = 1 + t^4 - t^5 = (t^2 - t + 1)(1 + t - t^3) = \Phi_6(t)F(t)$, where $F(t) = 1 + t - t^3$, which is the representer polynomial of $G_n(1,3)$, and Φ_6 is the 6-th cyclotomic polynomial. Letting $g(t) = t^n - 1$, in the notation of [18], the relation matrices of $G_n(4,5)$ and $G_n(1,3)$ are $f(C_g)$ and $F(C_g)$, respectively.

Now since $(n,6) = 1$ the resultant $\mathrm{Res}(\Phi_6, g) = \pm 1$ by [1], so by [18, Corollary 8] the Smith form of $f(C_g)$ is equal to the Smith form of $F(C_g)$ and thus $G_n(4,5)^{\mathrm{ab}} \cong G_n(1,3)^{\mathrm{ab}}$, as required. $\square$

Corollary 5.6. *Let $n = p^l \neq 5, 7, 13$ where $p \geq 5$ is prime, $l \geq 1$, and let κ be as defined at (6). Then*

$$\begin{aligned} T_2(n) &= \{[G_n(1,k)^{\mathrm{ab}}] \mid 2 \leq k \leq (p^l+1)/2, k \neq 3\} \\ &= \{[G_n(1,k)^{\mathrm{ab}}] \mid 2 \leq k \leq (p^l+1)/2, k \neq \kappa\}. \end{aligned}$$

Hence $\tau_2(n) \leq D_2(n)$. Moreover, if $\tau_2(n) = D_2(n)$ then $\sigma_2(n) = C_2(n)$ if and only if $G_n(1,3) \not\cong G_n(4,5)$.

Proof. First observe $\kappa \neq 3$ (since $n \neq 7, 13$) and $2 \leq \kappa \leq (p^l+1)/2$. Lemma 3.2 implies

$$T_2(n) = \{[G_n(1,k)^{\mathrm{ab}}] \mid 2 \leq k \leq (p^l+1)/2\}$$

but, by Lemmas 5.4 and 5.5, $G_n(1,3)^{\mathrm{ab}} \cong G_n(1,\kappa)^{\mathrm{ab}}$ so

$$T_2(n) = \{[G_n(1,k)^{\mathrm{ab}}] \mid 2 \leq k \leq (p^l+1)/2, k \neq 3\}$$

as required, and hence $\tau_2(n) \leq D_2(n)$.

By Lemma 3.2(a), $S_2(n) = \{[G_n(1,k)] \mid 2 \leq k \leq (p^l+1)/2\}$. Therefore $\sigma_2(n) < C_2(n)$ if and only if there exist distinct k_1, k_2 with $2 \leq k_1, k_2 \leq (p^l+1)/2$, such that $G_n(1,k_1) \cong G_n(1,k_2)$. This would imply $G_n(1,k_1)^{\mathrm{ab}} \cong G_n(1,k_2)^{\mathrm{ab}}$ so, if $\tau_2(n) = D_2(n)$, this can only happen for the pair $\{k_1, k_2\} = \{3, \kappa\}$. Therefore $\sigma_2(n) = C_2(n)$ if and only if $G_n(1,3) \not\cong G_n(1,\kappa)$, or equivalently that $G_n(1,3) \not\cong G_n(4,5)$ by Lemma 5.4. $\square$

(Note that the hypothesis $n \neq 5, 7, 13$ in Corollary 5.6 is necessary since $\tau_2(n) = D_2(n) + 1$ in these cases.) Lemma 5.5 prompts Question 1.3 which asks (for $n = p^l$, where $p \geq 5$ is prime) if $G_n(1,3) \not\cong G_n(4,5)$ for all prime powers $n \neq 5, 7, 13$ coprime to 6. (If $n = 7$ or 13 then $G_n(1,3) \cong G_n(4,5)$ by Lemma 5.4 and if $n = 5$ then $G_n(4,5)$ is not irreducible.) The following example (extracted from [4, Section 5.1]) confirms this in the cases $n = 11, 25$.

Example 5.7 *($G_n(1,3) \not\cong G_n(4,5)$ for $n \in \{11, 25\}$).* Let $G = G_{11}(1,3)$ and $H = G_{11}(4,5)$. Then $G'/G'' \cong \mathbb{Z}_2^{11}$ and $H'/H'' \cong \mathbb{Z}_3^{11}$ so $G_{11}(1,3) \not\cong G_{11}(4,5)$. As reported in [4, Section 5.1] GAP can be used to show that $G_{25}(1,3)$ has an epimorphism to $PSL(2,5)$ and $G_{25}(4,5)$ does not. An alternative computational proof is to observe that $G_{25}(1,3)$ has an index 5 subgroup, whereas $G_{25}(4,5)$ does not.

We now provide a theoretical proof of the epimorphism to $PSL(2,5)$ in Example 5.7.

Lemma 5.8. *For each $t \geq 1$ there exists an epimorphism from $G_{5t}(1,3)$ onto $SL(2,5)$ and hence onto $PSL(2,5)$.*

Proof. Adjoining the relations $x_i = x_{i+5}$ for each $0 \leq i < 5t$ to the presentation $G_{5t}(x_0 x_1 x_3^{-1})$ yields a presentation for $G_5(x_0 x_1 x_3^{-1}) = G_5(1,3) \cong SL(2,5)$, so $G_{5t}(1,3)$ maps onto $SL(2,5)$ and the result follows. □

In a similar spirit we have the following.

Lemma 5.9. *Let $n = p^l$ where p is prime, $l \geq 1$ and suppose $p|m$. Then there is an epimorphism from the group $G_{p^l}(m,k)$ onto $\mathbb{Z}_{2^{p^\alpha}-1}$ where α is the p-adic valuation of m. In particular, if $G \in S_1(p^l)$ then there is an epimorphism from G onto $\mathbb{Z}_{2^p-1}$.*

Proof. The group $G_{p^l}(m,k)$ is isomorphic to the free product of $d = (p^l, m, k)$ copies of $G_{p^l/d}(m/d, k, d)$ and so maps onto $G_{p^l/d}(m/d, k/d)$, and so we may assume $d = 1$, and hence $(p,k) = 1$. By adjoining relations $x_i = x_{i+p^\alpha}$ for each $0 \leq i < n$ we see that $G_n(m,k)$ maps onto $G_{p^\alpha}(0,k)$ which is isomorphic to $G_{p^\alpha}(0,1)$ by [2, Lemma 1.1(1)].

If $G \in S_1(p^l)$ then $G \cong G_{p^l}(m,k)$ for some $0 < m, k < p^l$, where $p|m$ and $(p,k) = 1$ (since $(p^l, m, k) = 1$), so G maps onto $\mathbb{Z}_{2^{p^\alpha}-1}$ (where α is the p-adic valuation of m), which maps onto $\mathbb{Z}_{2^p-1}$. □

Additional results like Lemmas 5.8 and 5.9 can be obtained using (for example) the finite groups $G_4(2,1) \cong SL(2,3)$ and the Gilbert-Howie group $H(8,3) = G_8(3,1)$ of order $3^{10} \cdot 5$.

5.2.2. Upper bound for $\tau_2(2^l)$

We now show that $D_2(2^l)$ is an upper bound for $\tau_2(2^l)$.

Lemma 5.10. *Let $n = 2^l$, where $l \geq 3$. Then*

$$T_2(n) = \{[G_n(1,k)^{\mathrm{ab}}] \mid k \in \{n/2-1, n/2+1, n-1\} \cup K\}$$

where

$$K = \{\min(k, k^{-1} \bmod n) \mid 3 \leq k \leq n-3, k \neq n/2 \pm 1, k \text{ odd}\}$$

(where $1 \leq k^{-1} < n$ denotes the multiplicative inverse of $k \bmod n$), and therefore $\tau_2(n) \leq D_2(n)$. Moreover, if $\tau_2(n) = D_2(n)$ then $\sigma_2(n) = C_2(n)$ if and only if $G_n(1,k) \not\cong G_n(1,k^{-1})$ for each odd k, $3 \leq k \leq n-3$, where $k \neq n/2 \pm 1$.

Proof. By Lemma 3.2(b), $S_2(n) = \{[G_n(1,k)] \mid 2 \leq k < 2^l, k \text{ odd}\}$ so

$$T_2(n) = \{[G_n(1,k)^{\mathrm{ab}}] \mid 2 \leq k < 2^l, k \text{ odd}\}$$

and by Corollary 4.2 $G_n(1,k)^{\mathrm{ab}} \cong G_n(1,k^{-1})^{\mathrm{ab}}$. Now, for odd k, $k \equiv k^{-1} \bmod n$ if and only if $k \equiv \pm 1$ or $n/2 \pm 1 \bmod n$. Therefore

$$\begin{aligned} T_2(n) &= \{[G_n(1, \min(k, k^{-1} \bmod n))^{\mathrm{ab}}] \mid 2 \leq k < 2^l, k \text{ odd}\} \\ &= \{[G_n(1,k)^{\mathrm{ab}}] \mid k \in \{n/2-1, n/2+1, n-1\} \cup K\} \end{aligned}$$

where K is as given in the statement. There are $2^{l-1}-4$ odd numbers k with $3 \leq k \leq 2^l-3$ and $k \neq n/2 \pm 1$, and for each of these $k \not\equiv k^{-1} \bmod n$. Therefore $|K| = (2^{l-1}-4)/2 = 2^{l-2}-2$, and so

$$\tau_2(n) = |T_2(n)| \leq (2^{l-2}-2) + 3 = 2^{l-2}+1 = D_2(n).$$

Now suppose $\tau_2(n) = D_2(n)$. If $g_2(n) = D_2(n)$ then if $k_1 \not\equiv k_2, k_2^{-1} \bmod n$ then $G_n(1,k_1)^{\mathrm{ab}} \not\cong G_n(1,k_2)^{\mathrm{ab}}$ so $G_n(1,k_1) \not\cong G_n(1,k_2)$; if, in addition, $G_n(1,k) \not\cong G_n(1,k^{-1})$ for each odd k, $2 \leq k < n$, where $k \not\equiv n/2-1, n/2+1, n-1$ then

$$|\{[G_n(1,k)] \mid 2 \leq k < 2^l, k \text{ odd}\}| = (2^l-2)/2 = 2^{l-1}-1 = C_2(n).$$

Conversely, if $G_n(1,k) \cong G_n(1,k^{-1})$ for some odd k, $2 \leq k < n$, where $k \not\equiv n/2-1, n/2+1, n-1$ then $k \not\equiv k^{-1} \bmod n$, so $[G_n(1,k)] = [G_n(1,k^{-1})]$, so

$$\sigma_2(n) \leq |\{[G_n(1,k)] \mid 2 \leq k < 2^l, k \text{ odd}\}| < C_2(n). \quad \square$$

5.3. The proofs of Theorems D and E and the equivalence of Conjectures B and B′

We are now in a position to prove Theorem D.

Proof of Theorem D. If $p \geq 3$ then (using Theorem C) $\tau_1(p^l) \leq \sigma_1(p^l) \leq C_1(p^l) = D_1(p^l)$. If $n = 4$ then $\tau_1(n) = D_1(n)$. If $p = 2$ and $l \geq 4$ then $\tau_1(p^l) \leq D_1(p^l)$ by Lemma 5.3. If $p \geq 5$ then $\tau_2(p^l) \leq D_2(p^l)$ by Corollary 5.6. If $p = 3$ then (using Theorem C) $\tau_2(p^l) \leq \sigma_2(p^l) \leq C_2(p^l) = D_2(p^l)$. If $p = 2$ then $\tau_2(p^l) \leq D_2(p^l)$ by Lemma 5.10. Then

$$\begin{aligned}\tau(n) &= \tau_1(n) + \tau_2(n) - |T_1(n) \cap T_2(n)| \\ &\leq \tau_1(n) + \tau_2(n) \\ &\leq D_1(n) + D_2(n) = D(n). \quad \square\end{aligned}$$

We now show that Conjectures B and B′ are equivalent.

Corollary 5.11. *Let $n \neq 2, 4, 5, 7, 8, 13, 23$ be a prime power. Then $\tau(n) = D(n)$ if and only if $T_1(n) \cap T_2(n) = \emptyset$, $\tau_1(n) = D_1(n)$, $\tau_2(n) = D_2(n)$.*

Proof. Suppose first that $T_1(n) \cap T_2(n) = \emptyset$, $\tau_1(n) = D_1(n)$, $\tau_2(n) = D_2(n)$. Then

$$\tau(n) = \tau_1(n) + \tau_2(n) - |T_1(n) \cap T_2(n)| = \tau_1(n) + \tau_2(n) = D_1(n) + D_2(n) = D(n).$$

Suppose then $\tau(n) = D(n)$. Then

$$\begin{aligned}D(n) &= \tau_1(n) + \tau_2(n) - |T_1(n) \cap T_2(n)| \\ &\leq D_1(n) + D_2(n) - |T_1(n) \cap T_2(n)| \\ &= D(n) - |T_1(n) \cap T_2(n)|\end{aligned}$$

(where we used Theorem D for the inequality), and hence $T_1(n) \cap T_2(n) = \emptyset$. If $\tau_1(n) < D_1(n)$ or $\tau_2(n) < D_2(n)$ then

$$\begin{aligned}D(n) &= \tau_1(n) + \tau_2(n) \\ &< D_1(n) + D_2(n) \\ &= D(n)\end{aligned}$$

(again using Theorem D), a contradiction. Therefore $\tau_1(n) = D_1(n)$ and $\tau_2(n) = D_2(n)$. $\square$

We now prove Theorem E.

Proof of Theorem E. If $n = 8$ then the result follows from [4], so assume $n \neq 8$. Since $\tau(n) = D(n)$, Corollary 5.11 implies $\tau_1(n) = D_1(n)$, $\tau_2(n) = D_2(n)$, and $T_1(n) \cap T_2(n) = \emptyset$, so $S_1(n) \cap S_2(n) = \emptyset$. By Corollary 3.3 $\sigma(n) = C(n)$ if and only if $\sigma_1(n) = C_1(n)$ and $\sigma_2(n) = C_2(n)$. If $p \geq 3$ then $C_1(n) = D_1(n) = \tau_1(n) \leq \sigma_1(n) \leq C_1(n)$ (by

Lemma 3.1) so $\sigma_1(n) = C_1(n)$. If $p \geq 5$ then by Corollary 5.6 $\sigma_2(n) = C_2(n)$ if and only if $G_n(1,3) \not\cong G_n(4,5)$. If $p = 3$ then $C_2(n) = D_2(n) = \tau_2(n) \leq \sigma_2(n) \leq C_2(n)$ (by Theorem C) so $\sigma_2(n) = C_2(n)$. If $p = 2$ then Lemma 5.3 implies $\sigma_1(n) = C_1(n)$ if and only if $G_n(n/2,1) \not\cong G_n(n/4,1)$, and Lemma 5.10 implies $\sigma_2(n) = C_2(n)$ if and only if $G_n(1,k) \not\cong G_n(1,k^{-1})$ for each odd k, $3 \leq k \leq n-3$, $k \neq n/2 \pm 1$. □

6. Lower bound for $\tau(p^l)$: computational evidence

In this section we present computational evidence that (for prime powers $p^l \neq 4, 23$) $D(p^l)$ is a lower bound for $\tau(p^l)$. Since this is an upper bound for $\tau(p^l)$, by Theorem D, this presents evidence for Conjecture B. To prove non-isomorphism of pairs of abelianised groups $G_n(m,k)^{\mathrm{ab}}$, it is usually sufficient to show that they have different orders. (There are exceptions, however; for example, $G_{29}(1,10)^{\mathrm{ab}} \cong \mathbb{Z}_{59}^2$ versus $G_{29}(1,7)^{\mathrm{ab}} \cong \mathbb{Z}_{59^2}$ and $G_{41}(1,15)^{\mathrm{ab}} \cong \mathbb{Z}_{83} \oplus \mathbb{Z}_{83}^2$ versus $G_{41}(1,8)^{\mathrm{ab}} \cong \mathbb{Z}_{83} \oplus \mathbb{Z}_{83^2}$.) Recalling (3), these orders are given by resultants and these are typically faster to compute than the abelianisations themselves. For this reason we introduce sets $R(n) = \{|A| \mid A \in T(n)\}$ and $R_i(n) = \{|A| \mid A \in T_i(n)\}$, and set $\upsilon(n) = |R(n)|$ and $\upsilon_i(n) = |R_i(n)|$ ($i \in \{1,2\}$). Then $\upsilon(n) \leq \tau(n)$, $\upsilon_1(n) \leq \tau_1(n)$, $\upsilon_2(n) \leq \tau_2(n)$ and if $R_1(n) \cap R_2(n) = \emptyset$ then $T_1(n) \cap T_2(n) = \emptyset$. Moreover, if $\omega \in R_1(n)$, where n is a power of a prime p, then $\omega \equiv 0 \bmod (2^p - 1)$ by Lemma 5.9.

Using the expressions for $T_1(n), T_2(n)$ given in (or directly implied by) Lemma 3.1, Lemma 5.3, Corollary 5.6, and Lemma 5.10 and performing computations in GAP we show the following for prime powers $n \neq 2, 4$:

- If $n \leq 3^8$ is a power of an odd prime p and $\omega \in R_2(n)$ then $\omega \not\equiv 0 \bmod (2^p - 1)$, and hence $R_1(n) \cap R_2(n) = \emptyset$.
- If $n = 2^l$, $3 \leq l \leq 12$ then $R_1(n) \cap R_2(n) = \emptyset$.
- If $n \leq 3^8$, $n \neq 8$ is a prime power then $D_1(n) \leq \upsilon_1(n)$.
- If $n \leq 41$, $n \neq 23$ is a prime power then $D_2(n) \leq \tau_2(n)$.
- If $41 < n \leq 3^8$ is a prime power then $D_2(n) \leq \upsilon_2(n)$.

Together with Theorem D this implies the following.

Theorem 6.1. *Suppose $n \leq 3^8$ is a prime power, $n \neq 2, 4, 5, 7, 8, 13, 23$. Then $T_1(n) \cap T_2(n) = \emptyset$, $\tau_1(n) = D_1(n)$, $\tau_2(n) = D_2(n)$, and hence $\tau(n) = D(n)$.*

7. Epilogue: decidability of the value of $\sigma(n)$

We close by observing that for arbitrary $n \geq 2$, there is an algorithm that decides if two irreducible groups of Fibonacci type with n generators are isomorphic, and hence there is an algorithm that determines the value of $\sigma(n)$.

Theorem 7.1. *There is an algorithm that, given input n, m_1, k_1, m_2, k_2 such that $n \geq 2$, $1 \leq m_1, k_1, m_2, k_2 < n$, $(n, m_1, k_1) = 1$, $(n, m_2, k_2) = 1$, $m_1 \neq k_1, m_2 \neq k_2$, decides if the groups $G_n(m_1, k_1), G_n(m_2, k_2)$ are isomorphic.*

Proof. If $n < 13$ then by [4] the values of m_1, k_1, m_2, k_2 for which $G_n(m_1, k_1), G_n(m_2, k_2)$ are isomorphic are known (see also [5, Table 1]). Thus we may assume $n \geq 13$.

For $i \in \{1, 2\}$ let $A_i = k_i, B_i = k_i - m_i$, $\Gamma_i = G_n(m_i, k_i)$. By [5, Corollary B] the following hold for each $i \in \{1, 2\}$:

(a) $\Gamma_i \cong \mathbb{Z}_{2^n-1}$ if and only if $A_i \equiv B_i \bmod n$;
(b) $\Gamma_i \cong \mathbb{Z}_{2^{n/2}-(1)^{m+n/2}}$ if and only if $A_i \equiv n/2 \bmod n$ or $B_i \equiv n/2 \bmod n$;
(c) Γ_i is isomorphic to the Sieradski group $S(2, n)$ if and only if $A_i + B_i \equiv 0 \bmod n$;
(d) Γ_i is isomorphic to the Gilbert-Howie group $H(n, n/2 + 2)$ if and only if $A_i + B_i \equiv n/2 \bmod n$;

and, moreover, Γ_i is elementary hyperbolic if and only if either (a) or (b) hold, and is non-hyperbolic if and only if either (c) or (d) hold. The groups $\mathbb{Z}_{2^n-1}, \mathbb{Z}_{2^{n/2}-(1)^{m+n/2}}, S(2, n)$, $H(n, n/2 + 2)$ are pairwise non-isomorphic, as the first two are finite of different orders, the second two are infinite [11], and $S(2, n)$ is a 3-manifold group, whereas $H(n, n/2+2)$ is not [12].

Thus we may assume that none of (a), (b), (c), (d) hold for either set of parameters $(n, m_1, k_1), (n, m_2, k_2)$. Then Γ_1, Γ_2 are (non-elementary) hyperbolic [5, Corollary B], and torsion-free [11,23], and so there is an algorithm that decides if $\Gamma_1 \cong \Gamma_2$ [21]. □

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors thank Martin Edjvet and the referee(s) for helpful comments.

References

[1] T.M. Apostol, Resultants of cyclotomic polynomials, Proc. Am. Math. Soc. 24 (1970) 457–462.
[2] V.G. Bardakov, A.Yu. Vesnin, A generalization of Fibonacci groups, Algebra Log. 42 (2) (2003) 131–160.
[3] Alberto Cavicchioli, Friedrich Hegenbarth, Dušan Repovš, On manifold spines and cyclic presentations of groups, in: Knot Theory, Warsaw, 1995, in: Banach Center Publ., vol. 42, Polish Acad. Sci. Inst. Math, Warsaw, 1998, pp. 49–56.
[4] Alberto Cavicchioli, E.A. O'Brien, Fulvia Spaggiari, On some questions about a family of cyclically presented groups, J. Algebra 320 (11) (2008) 4063–4072.
[5] Ihechukwu Chinyere, Gerald Williams, Hyperbolic groups of Fibonacci type and T(5) cyclically presented groups, J. Algebra 580 (2021) 104–126.
[6] Ihechukwu Chinyere, Gerald Williams, Hyperbolicity of $T(6)$ cyclically presented groups, Groups Geom. Dyn. 16 (1) (2022) 341–361.

[7] J.H. Conway, Advanced problem 5327, Am. Math. Mon. 72 (8) (1965) 915.
[8] Martin Edjvet, On the asphericity of one-relator relative presentations, Proc. R. Soc. Edinb., Sect. A 124 (4) (1994) 713–728.
[9] Martin Edjvet, On irreducible cyclic presentations, J. Group Theory 6 (2) (2003) 261–270.
[10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.12.2, 2022.
[11] N.D. Gilbert, James Howie, LOG groups and cyclically presented groups, J. Algebra 174 (1) (1995) 118–131.
[12] James Howie, Gerald Williams, Fibonacci type presentations and 3-manifolds, Topol. Appl. 215 (2017) 24–34.
[13] D.L. Johnson, Topics in the Theory of Group Presentations, London Mathematical Society Lecture Note Series, vol. 42, Cambridge University Press, Cambridge, New York, 1980.
[14] D.L. Johnson, H. Mawdesley, Some groups of Fibonacci type, J. Aust. Math. Soc. 20 (2) (1975) 199–204.
[15] Kirk McDermott, Shift dynamics of the groups of Fibonacci type, J. Group Theory 26 (1) (2023) 55–82.
[16] Esamaldeen Mohamed, Gerald Williams, Isomorphism theorems for classes of cyclically presented groups, Int. J. Algebra Comput. 29 (6) (2019) 1009–1017.
[17] Esamaldeen Mohamed, Gerald Williams, An investigation into the cyclically presented groups with length three positive relators, Exp. Math. 31 (2) (2022) 537–551.
[18] Vanni Noferini, Gerald Williams, Matrices in companion rings, Smith forms, and the homology of 3-dimensional Brieskorn manifolds, J. Algebra 587 (2021) 1–19.
[19] Vanni Noferini, Gerald Williams, Cyclically presented groups as labelled oriented graph groups, J. Algebra 605 (2022) 179–198.
[20] R.W.K. Odoni, Some Diophantine problems arising from the theory of cyclically-presented groups, Glasg. Math. J. 41 (2) (1999) 157–165.
[21] Z. Sela, The isomorphism problem for hyperbolic groups. I, Ann. Math. (2) 141 (2) (1995) 217–283.
[22] Allan J. Sieradski, Combinatorial squashings, 3-manifolds, and the third homology of groups, Invent. Math. 84 (1) (1986) 121–139.
[23] Gerald Williams, The aspherical Cavicchioli-Hegenbarth-Repovš generalized Fibonacci groups, J. Group Theory 12 (1) (2009) 139–149.
[24] Gerald Williams, Unimodular integer circulants associated with trinomials, Int. J. Number Theory 6 (4) (2010) 869–876.
[25] Gerald Williams, Groups of Fibonacci type revisited, Int. J. Algebra Comput. 22 (8) (2012) 1240002.