Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(5): 10734–10755.
DOI: 10.3934/math.2024524
Received: 18 January 2024
Revised: 05 March 2024
Accepted: 11 March 2024
Published: 19 March 2024

Research article

The conjugacy diameters of non-abelian finite p-groups with cyclic maximal subgroups

Fawaz Aseeri[1,*] **and Julian Kaspczyk**[2]

[1] Mathematics Department, Faculty of Sciences, Umm Al-Qura University, Makkah 21955, Saudi Arabia

[2] Institut für Algebra, Fakultät Mathematik, Technische Universität Dresden, 01069 Dresden, Germany

* **Correspondence:** Email: fiaseeri@uqu.edu.sa; Tel: +966542963559.

Abstract: Let G be a group. A subset S of G is said to normally generate G if G is the normal closure of S in G. In this case, any element of G can be written as a product of conjugates of elements of S and their inverses. If $g \in G$ and S is a normally generating subset of G, then we write $\|g\|_S$ for the length of a shortest word in $\mathrm{Conj}_G(S^{\pm 1}) := \{h^{-1}sh|h \in G, s \in S \text{ or } s^{-1} \in S\}$ needed to express g. For any normally generating subset S of G, we write $\|G\|_S = \sup\{\|g\|_S \mid g \in G\}$. Moreover, we write $\Delta(G)$ for the supremum of all $\|G\|_S$, where S is a finite normally generating subset of G, and we call $\Delta(G)$ the conjugacy diameter of G. In this paper, we derive the conjugacy diameters of the semidihedral 2-groups, the generalized quaternion groups and the modular p-groups. This is a natural step after the determination of the conjugacy diameters of dihedral groups.

Keywords: semidihedral group; quaternion group; modular p-groups; normally generating subsets; word norm; conjugacy diameter
Mathematics Subject Classification: 05E16, 20D15

1. Introduction

1.1. Background on norms and boundedness

Let G be a group. A *norm* on G is a function $\nu : G \longrightarrow [0, \infty)$ which satisfies the following axioms:
(i) $\nu(g) = 0 \iff g = 1$;
(ii) $\nu(g^{-1}) = \nu(g)$ for all $g \in G$;
(iii) $\nu(gh) \leq \nu(g) + \nu(h)$ for all $g, h \in G$;
We call ν *conjugation-invariant* if we also have

(iv) $\nu(g^{-1}hg) = \nu(h)$ for all $g, h \in G$.

The *diameter* of a group G with respect to a conjugation-invariant norm ν on G is defined as

$$\mathrm{diam}_{\nu}(G) := \sup\{\nu(g) | g \in G\}.$$

A group G is said to be *bounded* if every conjugation-invariant norm on G has a finite diameter. The concepts of conjugation-invariant norms and boundedness were introduced by Burago et al. [5], and they provided a number of applications to geometric group theory, Hamiltonian dynamics, and finite groups. Since then, there has been a large amount of interest in providing further applications, examples, and analogues of these notions in geometry, group theory, and topology; see [2–4, 11, 12, 15] for examples.

An important source of conjugation-invariant norm is a normally generating subset of a group. Let G be a group and $S \subseteq G$. The *normal closure of* S in G, denoted by $\langle\langle S \rangle\rangle$, is the subgroup of G that is generated by all conjugates of elements of S. In other words, it is the smallest normal subgroup of G containing S. We say that S *normally generates* G if $G = \langle\langle S \rangle\rangle$. In this case, any element of G can be written as a product of elements of

$$\mathrm{Conj}_G(S^{\pm 1}) := \{h^{-1}sh | h \in G, s \in S \text{ or } s^{-1} \in S\}. \tag{1.1}$$

If S normally generates G, then the *length* $\|g\|_S \in \mathbb{N}$ of $g \in G$ with respect to S is defined to be the length of a shortest word in $\mathrm{Conj}_G(S^{\pm 1})$ that is needed to express g. In other words,

$$\|g\|_S = \inf\{n \in \mathbb{N} | g = s_1 \cdots s_n \text{ for some } s_1, \ldots, s_n \in \mathrm{Conj}_G(S^{\pm 1})\}.$$

It is important to stress that $\|1\|_S$, i.e., the length of the identity element 1 of G with respect to S, is 0. The *word norm* $\| \,.\, \|_S : G \to [0, \infty)$, $g \mapsto \|g\|_S$ is a conjugation-invariant norm on G. The *diameter* of a group G with respect to the word norm $\| \,.\, \|_S$ is given by

$$\|G\|_S := \sup\{\|g\|_S | g \in G\}.$$

For other examples of conjugation-invariant norms, see [3, 5].

If G is a group and S is a finite normally generating subset of G, then G is bounded if and only if $\|G\|_S$ is finite (see [12, Corollary 2.5]). Therefore, word norms for finite normally generating subsets and their diameters are an important tool to study the boundedness of groups.

Moreover, word norms are used in the study of several refinements of the concept of bounded groups. To describe these refinements, we introduce some notation. For any group G and any $n \geq 1$, let

$$\Gamma_n(G) := \{S \subseteq G \mid |S| \leq n \text{ and } S \text{ normally generates } G\},$$
$$\Gamma(G) := \{S \subseteq G \mid |S| < \infty \text{ and } S \text{ normally generates } G\}.$$

Set

$$\Delta_n(G) := \sup\{\|G\|_S \; | S \in \Gamma_n(G)\},$$
$$\Delta(G) := \sup\{\|G\|_S \; | S \in \Gamma(G)\}.$$

For any group G, $\Delta(G)$ is said to be the *conjugacy diameter* of G. The group G is called *strongly bounded* if $\Delta_n(G) < \infty$ for all $n \in \mathbb{N}$ (see [12, Definition 1.1]). The group G is called *uniformly bounded* if $\Delta(G) < \infty$ (see [12, Definition 1.1]).

1.2. Motivation and statements of results

As we have seen in the previous section, word norms and their diameters emerge in the study of boundedness. Since any finite group is known to be uniformly bounded, the study of boundedness mainly focuses on infinite groups. However, word norms and their diameters are also of interest in finite group theory. For example, conjugacy diameters of finite groups can be used to study conjugacy class sizes (see [12, Proposition 7.1]). Recently, conjugacy diameters were studied for several classes of finite groups. For example, Kędra et al. showed that $\Delta(PSL(n,q)) \leq 12(n-1)$ for any $n \geq 3$ and any prime power q (see [12, Example 7.2]). Also, Libman and Tarry proved that $\Delta(S_n) = n-1$ for any $n \geq 2$ (see [14, Thereom 1.2]),and that, if G is a non-abelian group of order pq, where p and q are prime numbers with $p < q$, then $\Delta(G) = \max\{\frac{p-1}{2}, 2\}$ (see [14, Thereom 1.1]). The first author determined the conjugacy diameters of finite dihedral groups as described below.

Theorem 1.1. *([1, Theorem 6.0.2]) Let $n \geq 3$ be a natural number and $G := D_{2n} = \langle a, b | a^n = 1 = b^2, bab = a^{-1}\rangle$ be the dihedral group of order $2n$. Then,*

$$\Delta(G) = \begin{cases} 2 & \text{if } n \geq 3 \text{ and } n \text{ odd}, \\ 2 & \text{if } n = 4, \\ 3 & \text{if } n \geq 6 \text{ and } n \text{ even}. \end{cases}$$

For the case of the infinite dihedral group $D_\infty = \langle a, b | b^2 = 1, bab = a^{-1}\rangle$, we have $\Delta(D_\infty) \leq 4$ (see [12, Example 2.8]).

The goal of this paper is to take Theorem 1.1 further. For any natural number $n \geq 3$, the dihedral group D_{2n} is non-abelian and has a cyclic maximal subgroup. Thus, one way to extend Theorem 1.1 would be to prove further results about conjugacy diameters of non-abelian finite groups with cyclic maximal subgroups. Instead of looking at arbitrary non-abelian finite groups with cyclic maximal subgroups, let us restrict our attention to non-abelian finite p-groups with cyclic maximal subgroups.

Definition 1.2. *Let n be a natural number.*

(i) For $n \geq 4$, define

$$SD_n := \langle a, b | a^{2^{n-1}} = 1 = b^2, a^b = a^{-1+2^{n-2}}\rangle.$$

We call SD_n the semidihedral group of order 2^n.

(ii) For $n \geq 3$, define

$$Q_n := \langle a, b | a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, a^b = a^{-1}\rangle.$$

We call Q_n the (generalized) quaternion group of order 2^n.

(iii) Let p be a prime number and assume that $n \geq 4$ if $p = 2$ and $n \geq 3$ if p is odd. Define

$$M_n(p) := \langle a, b | a^{p^{n-1}} = 1 = b^p, a^b = a^{1+p^{n-2}}\rangle.$$

We call $M_n(p)$ the modular p-group of order p^n.

The groups introduced in Definition 1.2 turn out to be important in several contexts. For example, they appear in [6–9, 16], where various spectra and energies of commuting and non-commuting graphs of these groups have been computed.

The non-abelian finite p-groups with cyclic maximal subgroups are fully classified by applying the following theorem.

Theorem 1.3. *(see [10, Chapter 5, Theorem 4.4]) Let P be a non-abelian p-group of order p^n which contains a cyclic subgroup H of order p^{n-1}. Then, the following holds:*

(i) If $n = 3$ and $p = 2$, then P is isomorphic to D_8 or Q_3.

(ii) If $n > 3$ and $p = 2$, then P is isomorphic to $M_n(2), D_{2^n}, Q_n$, or SD_n.

(iii) If p is odd, then P is isomorphic to $M_n(p)$.

No two groups among D_{2^n}, Q_n, SD_n, or $M_n(p)$ are isomorphic to each other (see [10, Chapter 5, Theorem 4.3(iii)]). We will prove the following results:

Theorem 1.4. *Let $n \geq 4$ be a natural number and $G := SD_n$. Then,*

$$\Delta(G) = \begin{cases} 2 & \text{if } n = 4, \\ 3 & \text{if } n \geq 5. \end{cases}$$

Theorem 1.5. *Let $n \geq 3$ be a natural number and $G := Q_n$. Then,*

$$\Delta(G) = \begin{cases} 2 & \text{if } n = 3, \\ 3 & \text{if } n \geq 4. \end{cases}$$

Theorem 1.6. *Let p be a prime number and n be a natural number, where $n \geq 4$ if $p = 2$ and $n \geq 3$ if p is odd. Let $G := M_n(p)$. Then,*

$$\Delta(G) = \begin{cases} 2^{n-3} + 1 & \text{if } p = 2, \\ \frac{p^{n-2}+p-2}{2} & \text{if } p \text{ is odd.} \end{cases}$$

With Theorems 1.1 and 1.4–1.6, we are able to calculate all of the conjugacy diameters of non-abelian finite p-groups with cyclic maximal subgroups.

2. Preliminaries

In this section, we present some results and the notation needed for the proofs of Theorems 1.4–1.6.

Definition 2.1. *([12, Section 2]) Let X be a subset of a group G. For any $n \geq 0$, we define $B_X(n)$ to be the set of all elements of G which can be expressed as a product of at most n conjugates of elements of X and their inverses.*

By Definition 2.1, we have

$$\{1\} = B_X(0) \subseteq B_X(1) \subseteq B_X(2) \subseteq \dots$$

The next result follows from the above definition.

Lemma 2.2. *([12, Lemma 2.3 (iii)]) Let G be a group, $X, Y \subseteq G$, and $n, m \in \mathbb{N}$. Then, $B_X(n)B_X(m) = B_X(n+m)$.*

The following terminology is not standard, but it will be useful in this paper.

Definition 2.3. *Let n be a natural number.*

(i) If $n \geq 4$ and $G = SD_n$, then a pair (a, b) of elements $a, b \in G$ is called a standard generator pair if $ord(a) = 2^{n-1}, ord(b) = 2, bab = a^{2^{n-2}-1}$.

(ii) If $n \geq 3$ and $G = Q_n$, then a pair (a, b) of elements $a, b \in G$ is called a standard generator pair if $ord(a) = 2^{n-1}, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1}$.

(iii) If $G = M_n(p)$, where $n \geq 4$ and $p = 2$ or $n \geq 3$ and p is an odd prime, then a pair (a, b) of elements $a, b \in G$ is called a standard generator pair if $ord(a) = p^{n-1}, ord(b) = p, b^{-1}ab = a^{p^{n-2}+1}$.

Lemma 2.4. *Let $G = SD_n$ for some $n \geq 4$ or $G = Q_n$ for some $n \geq 3$, and let (a, b) be a standard generator pair of G. Then, the subgroups $\langle a\rangle, \langle a^2\rangle\langle ab\rangle, \langle a^2\rangle\langle b\rangle$ are proper normal subgroups of G.*

Proof. We have

$$|\langle a\rangle| = |\langle a^2\rangle\langle b\rangle| = |\langle a^2\rangle\langle ab\rangle| = 2^{n-1}.$$

So, each of these subgroups is a maximal subgroup of G. This proves the lemma since each maximal subgroup of a finite 2-group is a proper normal subgroup. □

Remark 2.5. *Let $n \geq 4$ be a natural number and $G = SD_n$. Let (a, b) be a standard generator pair of G. If $m \in \mathbb{Z}$, then one can easily show that*

$$(a^{-1+2^{n-2}})^m = \begin{cases} a^{-m} & \text{if } m \textit{ is even}, \\ a^{-m}a^{2^{n-2}} & \text{if } m \textit{ is odd}. \end{cases}$$

Lemma 2.6. *Let $n \geq 4$ be a natural number and $G = SD_n$. Let (a, b) be a standard generator pair of G. Then, the following holds:*

(i) The conjugacy class of a^2b is $\{a^rb \,\big|\, r$ is even and $0 \leq r < 2^{n-1}\}$.

(ii) The conjugacy class of ab is $\{a^rb \,\big|\, r$ is odd and $0 < r < 2^{n-1}\}$.

(iii) If $0 \leq m < 2^{n-1}$, then the conjugacy class of a^m is $\{a^m, (a^{-1+2^{n-2}})^m\}$.

(iv) If $0 \leq m < 2^{n-1}$ is even, then $(a^mb)^{-1} = a^{m'}b$ for some even $0 \leq m' < 2^{n-1}$.

(v) If $0 < m < 2^{n-1}$ is odd, then $(a^mb)^{-1} = a^{m'}b$ for some odd $0 < m' < 2^{n-1}$.

Proof. Let $0 \leq m < 2^{n-1}$ and $\ell \in \mathbb{Z}$. For (i) and (ii), we have

$$\begin{aligned} (a^mb)^{a^\ell} &= a^{-\ell}\, a^mb\, a^\ell \\ &= a^{m-\ell}\, b\, a^\ell\, b\, b \\ &= a^{m-\ell}\, (b\, a\, b)^\ell\, b \\ &= a^{m-\ell}\, (a^{-1+2^{n-2}})^\ell\, b \end{aligned}$$

$$\overset{(2.5)}{=} \begin{cases} a^{m-2\ell}\, b\,, & \text{if } \ell \text{ is even}\,, \\ a^{m-2\ell+2^{n-2}}\, b\,, & \text{if } \ell \text{ is odd}\,. \end{cases}$$

$$\begin{aligned} (a^m b)^{a^\ell b} &= (a^\ell b)^{-1}(a^m b)(a^\ell b) \\ &= b\, a^{-\ell}\, a^m\, b\, a^\ell\, b \\ &= (b\, a^{-\ell}\, b)\,(b\, a^m\, b)\, a^\ell\, b \\ &= (b\, a\, b)^{-\ell}\,(b\, a\, b)^m\, a^\ell\, b \\ &= (a^{-1+2^{n-2}})^{-\ell}\,(a^{-1+2^{n-2}})^m\, a^\ell\, b \\ &= a^{2\ell-m+2^{n-2}(m-\ell)}\, b. \end{aligned}$$

Thus, if m is even, then the conjugacy class of $a^m b$ is $\{a^r b \big| \, r \text{ is even and } 0 \le r < 2^{n-1}\}$. In particular, (i) holds. If m is odd, then the conjugacy class of $a^m b$ is $\{a^r b \big| \, r \text{ is odd and } 0 < r < 2^{n-1}\}$. In particular, (ii) holds.

For (iii), we have

$$\begin{aligned} (a^m)^{a^\ell} &= a^{-\ell}\, a^m\, a^\ell \\ &= a^m. \end{aligned}$$

$$\begin{aligned} (a^m)^{a^\ell b} &= (a^\ell b)^{-1}\,(a^m)\,(a^\ell b) \\ &= b\, a^{-\ell}\, a^m a^\ell b \\ &= b\ a^m b \\ &= (b\ a\, b)^m \\ &= (a^{-1+2^{n-2}})^m. \end{aligned}$$

This completes the proof of (iii).

For (iv), we assume that $0 \le m < 2^{n-1}$ is even. We have $a^m b \in \langle a^2 \rangle \langle b \rangle$. Therefore, we have $(a^m b)^{-1} \in \langle a^2 \rangle \langle b \rangle$, and $(a^m b)^{-1} \notin \langle a^2 \rangle$ as $a^m b \notin \langle a^2 \rangle$. It follows that $(a^m b)^{-1} = a^{m'} b$ for some even $0 \le m' < 2^{n-1}$.

For (v), we assume that $0 < m < 2^{n-1}$ is odd. It is clear that $(a^m b)^{-1} \notin \langle a \rangle$. So we have $(a^m b)^{-1} = a^{m'} b$ for some $0 \le m' < 2^{n-1}$. Since $a^m b \notin \langle a^2 \rangle \langle b \rangle$, we have that m' is odd. □

Remark 2.7. *Let $n \ge 3$ be a natural number and $G = Q_n$. Let (a, b) be a standard generator pair of G. If $m \in \mathbb{Z}$, then one can easily show that*

(i) $b^{-1} a^m b = (b^{-1} ab)^m = a^{-m}$.

(ii) $b^4 = 1$.

Lemma 2.8. *Let $n \ge 3$ be a natural number and $G = Q_n$. Let (a, b) be a standard generator pair of G. Then, the following holds:*

(i) The conjugacy class of $a^2 b$ is $\{a^r b \big| \, r$ is even and $0 \le r < 2^{n-1}\}$.

(ii) The conjugacy class of ab is $\{a^r b \big| \, r$ is odd and $0 < r < 2^{n-1}\}$.

(iii) If $0 \le m < 2^{n-1}$*, then the conjugacy class of* a^m *is* $\{a^m, a^{-m}\}$.

(iv) If $0 \le m < 2^{n-1}$ *is even, then* $(a^m b)^{-1} = a^{m'} b$ *for some even* $0 \le m' < 2^{n-1}$.

(v) If $0 < m < 2^{n-1}$ *is odd, then* $(a^m b)^{-1} = a^{m'} b$ *for some odd* $0 < m' < 2^{n-1}$.

Proof. Let $0 \le m < 2^{n-1}$ and $\ell \in \mathbb{Z}$. For (i) and (ii), we have

$$\begin{aligned}
(a^m b)^{a^\ell} &= a^{-\ell}\, a^m b\, a^\ell \\
&= a^{m-\ell}\, b^2\, b^{-1}\, a^\ell\, b\, b^3 \\
&= a^{m-\ell}\, a^{2^{n-2}}\, (b^{-1}\, a\, b)^\ell\, b^2\, b \\
&= a^{m-\ell}\, a^{2^{n-2}}\, a^{-\ell}\, a^{2^{n-2}}\, b \\
&= a^{m-2\ell}\, b.
\end{aligned}$$

$$\begin{aligned}
(a^m b)^{a^\ell b} &= (a^\ell b)^{-1}\, (a^m b)\, (a^\ell b) \\
&= b^{-1}\, a^{-\ell}\, a^m b\, a^\ell b \\
&= b^{-1} (a^m b)^{a^\ell}\, b \\
&= b^{-1} a^{m-2\ell} b\, b \\
&= a^{2\ell - m}\, b.
\end{aligned}$$

Thus, if m is even, then the conjugacy class of $a^m b$ is $\{a^r b \,|\, r \text{ is even and } 0 \le r < 2^{n-1}\}$. In particular, (i) holds. If m is odd, then the conjugacy class of $a^m b$ is $\{a^r b \,|\, r \text{ is odd and } 0 < r < 2^{n-1}\}$. In particular, (ii) holds.

For (iii), we have

$$\begin{aligned}
(a^m)^{a^\ell} &= a^{-\ell} a^m a^\ell \\
&= a^m.
\end{aligned}$$

$$\begin{aligned}
(a^m)^{a^\ell b} &= (a^\ell b)^{-1} (a^m) (a^\ell b) \\
&= b^{-1}\, a^{-\ell}\, a^m a^\ell b \\
&= b^{-1}\; a^m b \\
&= a^{-m}.
\end{aligned}$$

This completes the proof of (iii).

For (iv) and (v), we have similar arguments as in the proofs of Lemma 2.6(iv) and (v). □

Lemma 2.9. *Let* $G = SD_n$ *for some* $n \ge 4$ *or* $G = Q_n$ *for some* $n \ge 3$, *and let* (a, b) *be a standard generator pair of* G. *Let* S *be a normally generating subset of* G. *Then, there are elements* $x, y \in S$ *such that* $x = a^\ell b$ *for some* $0 \le \ell < 2^{n-1}$, *and such that* $y = a^m$ *for some odd* $0 < m < 2^{n-1}$ *or* $y = a^m b$ *for some* $0 \le m < 2^{n-1}$ *with* $\ell \not\equiv m \bmod 2$. *For each such* x *and* y, *we have* $\{x, y\} \in \Gamma(G)$.

Proof. If $S \subseteq \langle a \rangle$, then $\langle\langle S \rangle\rangle \le \langle a \rangle$ since $\langle a \rangle \trianglelefteq G$ (see Lemma 2.4), which is a contradiction to $S \in \Gamma(G)$. Thus, $S \nsubseteq \langle a \rangle$.

Let $x \in S \setminus \langle a \rangle$. Then, $x = a^\ell b$ for some $0 \le \ell < 2^{n-1}$. Assume that any element of S has the form a^m, where $0 \le m < 2^{n-1}$ is even, or the form $a^m b$ with $\ell \equiv m \bmod 2$. Then, $S \subseteq X_1 := \langle a^2 \rangle \langle b \rangle$

or $S \subseteq X_2 := \langle a^2\rangle\langle ab\rangle$. Since X_1 and X_2 are proper normal subgroups of G by Lemma 2.4, it follows that $\langle\langle S\rangle\rangle \neq G$, which is a contradiction. Consequently, there is some $y \in S$ such that $y = a^m$, where $0 < m < 2^{n-1}$ is odd, or $y = a^m b$, where $0 \leq m < 2^{n-1}$ and $\ell \not\equiv m \bmod 2$.

Let $x, y \in S$ be as above. We show that $X := \{x, y\} \in \Gamma(G)$. Assume that $y = a^m$ for some odd $0 < m < 2^{n-1}$. Then, $\langle a\rangle = \langle y\rangle \subseteq \langle\langle X\rangle\rangle$. It follows that $G = \langle a\rangle\langle x\rangle \subseteq \langle\langle X\rangle\rangle$. Thus, $G = \langle\langle X\rangle\rangle$ and we have $X \in \Gamma(G)$. Assume now that $y = a^m b$, where $0 \leq m < 2^{n-1}$ and $\ell \not\equiv m \bmod 2$. Then, every element of $S \setminus \langle a\rangle$ is conjugate to x or y by Lemmas 2.6 and 2.8, so $S \setminus \langle a\rangle \subseteq \langle\langle X\rangle\rangle$. Also, $a = ab \cdot b \in \langle\langle X\rangle\rangle$ if $G = SD_n$ and $a = a^{2^{n-2}+1} b \cdot b \in \langle\langle X\rangle\rangle$ if $G = Q_n$. It follows that $G = \langle\langle X\rangle\rangle$; hence,$X \in \Gamma(G)$. The proof is now complete. □

Lemma 2.10. *Let $n \geq 4$ be a natural number and $G = SD_n$. Let (a, b) be a standard generator pair of G. If $m_1, m_2 \in \mathbb{Z}$, then*

(i) $a^{m_1} b \cdot a^{m_2} b = a^{m_1 - m_2 + 2^{n-2} m_2}$;

(ii) $a^{m_1} b \cdot a^{m_2} = a^{m_1 - m_2 + 2^{n-2} m_2}\, b$;

(iii) $a^{m_1} \cdot a^{m_2} b = a^{m_1 + m_2} b$.

Proof. For (i), we have

$$\begin{aligned} a^{m_1} b \cdot a^{m_2} b &= a^{m_1}\,(b\,a\,b)^{m_2} \\ &= a^{m_1}\,(a^{-1+2^{n-2}})^{m_2} \\ &= a^{m_1 - m_2 + 2^{n-2} m_2}. \end{aligned}$$

For (ii), we have

$$\begin{aligned} a^{m_1} b \cdot a^{m_2} &= a^{m_1}\, b\, a^{m_2}\, b\, b \\ &= a^{m_1}\,(b\,a\,b)^{m_2}\, b \\ &= a^{m_1}\,(a^{-1+2^{n-2}})^{m_2}\, b \\ &= a^{m_1 - m_2 + 2^{n-2} m_2}\, b. \end{aligned}$$

Statement (iii) is clear. □

Lemma 2.11. *Let $n \geq 3$ be a natural number and $G = Q_n$. Let (a, b) be a standard generator pair of G. If $m_1, m_2 \in \mathbb{Z}$, then*

(i) $a^{m_1} b \cdot a^{m_2} b = a^{m_1 - m_2 + 2^{n-2}}$;

(ii) $a^{m_1} b \cdot a^{m_2} = a^{m_1 - m_2} b$;

(iii) $a^{m_1} \cdot a^{m_2} b = a^{m_1 + m_2} b$.

Proof. For (i), we have

$$\begin{aligned} a^{m_1} b \cdot a^{m_2} b &= a^{m_1} b\, b\, b^{-1}\, a^{m_2}\, b \\ &= a^{m_1} b^2\,(b^{-1}\, a\, b)^{m_2} \end{aligned}$$

$$= a^{m_1} a^{2^{n-2}} a^{-m_2}$$
$$= a^{m_1 - m_2 + 2^{n-2}}.$$

For (ii), we have

$$\begin{aligned} a^{m_1} b \cdot a^{m_2} &= a^{m_1} b\, b\, b^{-1} a^{m_2}\, b\, b^3 \\ &= a^{m_1} b^2\, (b^{-1} a\, b)^{m_2}\, b^2\, b \\ &= a^{m_1} a^{2^{n-2}}\, a^{-m_2}\, a^{2^{n-2}}\, b \\ &= a^{m_1 - m_2}\, b. \end{aligned}$$

Statement (iii) is clear. □

We now prove some properties of modular p-groups. From now until Lemma 2.19, we work under the following hypothesis.

Hypothesis 2.12. *Let p be a prime number and n be a natural number, where $n \geq 4$ if $p = 2$ and $n \geq 3$ if p is odd. Set $G := M_n(p)$; let (a, b) be a standard generator pair of G and $z := a^{p^{n-2}}$.*

Lemma 2.13. *$\Phi(G) = Z(G)$ is the unique maximal subgroup of $\langle a \rangle$. In particular, we have $z \in Z(G)$.*

Proof. This follows from [10, Chapter 5, Theorem 4.3(i)]. □

Lemma 2.14. *For each $k \in \mathbb{Z}$, we have $b^k a b^{-k} = z^{-k} a$.*

Proof. We show by induction that, for any non-negative integer k, we have $b^k a b^{-k} = z^{-k} a$ and $b^{-k} a b^k = z^k a$. This is clear for $k = 0$.

We now consider the case $k = 1$. We have $b^{-1} a b = a^{p^{n-2}+1} = za$. Since $z \in Z(G)$ by Lemma 2.13, we also have

$$\begin{aligned} a &= b(b^{-1} a b) b^{-1} \\ &= bzab^{-1} \\ &= zbab^{-1} \end{aligned}$$

and, thus, $bab^{-1} = z^{-1} a$.

Assume now that $k \geq 2$ is an integer such that $b^{k-1} a b^{-(k-1)} = z^{-(k-1)} a$ and $b^{-(k-1)} a b^{k-1} = z^{k-1} a$. Bearing in mind that $z \in Z(G)$ by Lemma 2.13 and that $bab^{-1} = z^{-1} a$, we see that

$$\begin{aligned} b^k a b^{-k} &= b(b^{k-1} a b^{-(k-1)}) b^{-1} \\ &= b z^{-(k-1)} a b^{-1} \\ &= z^{-(k-1)} b a b^{-1} \\ &= z^{-(k-1)} z^{-1} a \\ &= z^{-k} a. \end{aligned}$$

Similarly, we have

$$b^{-k} a b^k = b^{-1}(b^{-(k-1)} a b^{k-1}) b$$

$$\begin{aligned} &= b^{-1}z^{k-1}ab \\ &= z^{k-1}b^{-1}ab \\ &= z^k a. \end{aligned}$$

□

Lemma 2.15. *Let $\ell, j \in \mathbb{Z}$. For each positive integer k, we have*

$$(a^\ell b^j)^k = a^{k\ell} b^{kj} z^{-k\frac{(k-1)}{2} j\ell}. \tag{2.1}$$

Proof. We prove the lemma by induction on k.
For $k = 1$, we have

$$a^{k\ell} b^{kj} z^{-k\frac{(k-1)}{2} j\ell} = a^\ell b^j = (a^\ell b^j)^k.$$

Suppose now that k is a positive integer for which (2.1) holds. Then,

$$\begin{aligned} (a^\ell b^j)^{k+1} &= a^\ell b^j (a^\ell b^j)^k \\ &= a^\ell b^j a^{k\ell} b^{kj} z^{-k\frac{(k-1)}{2} j\ell} \\ &= a^\ell b^j a^{k\ell} b^{-j} b^{(k+1)j} z^{-k\frac{(k-1)}{2} j\ell} \\ &= a^\ell (b^j a b^{-j})^{k\ell} b^{(k+1)j} z^{-k\frac{(k-1)}{2} j\ell} \\ &\overset{2.14}{=} a^\ell (z^{-j} a)^{k\ell} b^{(k+1)j} z^{-k\frac{(k-1)}{2} j\ell} \\ &\overset{z\in Z(G)}{=} a^{(k+1)\ell} b^{(k+1)j} z^{-jk\ell - k\frac{(k-1)}{2} j\ell} \\ &= a^{(k+1)\ell} b^{(k+1)j} z^{(-k-\frac{k(k-1)}{2}) j\ell} \\ &= a^{(k+1)\ell} b^{(k+1)j} z^{(\frac{-(k+1)k}{2}) j\ell}. \end{aligned}$$

□

Lemma 2.16. *Let $S \in \Gamma(G)$. Then, S contains an element of order p^{n-1}.*

Proof. Since $S \nsubseteq \langle a^p, b\rangle = \langle a^p\rangle\langle b\rangle \trianglelefteq G$, the set S contains an element of the form $a^\ell b^j$, where $0 < \ell < p^{n-1}$ is not divisible by p and $0 \leq j < p$. By Lemma 2.15, we have

$$(a^\ell b^j)^p = a^{p\ell} b^{pj} z^{-p\frac{(p-1)}{2} j\ell} = (a^\ell)^p z^{-p\frac{(p-1)}{2} j\ell}.$$

If $p = 2$, then we have $(a^\ell b^j)^2 = (a^\ell)^2$ or $(a^\ell)^2 z$. In either case, $(a^\ell b^j)^2$ is of order 2^{n-2}, which implies that $a^\ell b^j$ is of order 2^{n-1}. If p is odd, then $(a^\ell b^j)^p = (a^\ell)^p$ is of order p^{n-2} and $a^\ell b^j$ is of order p^{n-1}. □

Lemma 2.17. *Let x be an element of G with order p^{n-1}. Then, there is some $y \in G$ such that (x, y) is a standard generator pair of G.*

Proof. Since x is of order p^{n-1} and G is of order p^n, the subgroup $\langle x\rangle$ is maximal in G. By Lemma 2.13, we have $\langle z\rangle \subseteq Z(G) = \Phi(G) \subseteq \langle x\rangle$. Because $\langle x\rangle$ is cyclic, $\langle x\rangle$ has only one subgroup of order p. Hence, $\langle z\rangle$ is the only subgroup of $\langle x\rangle$ with order p. Therefore, $\langle b\rangle$ is not contained in $\langle x\rangle$. Hence, $\langle b\rangle$ is a complement of $\langle x\rangle$ in G. Now, [13, Theorem 5.3.2] implies that there is some $y \in \langle b\rangle$ such that (x, y) is a standard generator pair of G. □

Lemma 2.18. *Let $S \in \Gamma(G)$. Then, there is a standard generator pair (x, y) of G such that $x \in S$ and $x^\ell y^j \in S$ for $0 \le \ell < p^{n-1}$ and $0 < j < p$.*

Proof. By Lemma 2.16, S contains an element x of order p^{n-1}. By Lemma 2.17, there is an element y of G such that (x, y) is a standard generator pair of G. Since $S \not\subseteq \langle x\rangle$, there exist $0 \le \ell < p^{n-1}$ and $0 < j < p$ such that $x^\ell y^j \in S$, as required. □

Given a group X and an element h of X, we write $\mathrm{Conj}_X(h)$ for the conjugacy class of h in X.

Lemma 2.19. *Let $0 \le \ell < p^{n-1}$ and $0 < j < p$. Then, the following holds:*

(i) $\mathrm{Conj}_G(a) = \{z^r a \big| 0 \le r < p\}$.

(ii) $\mathrm{Conj}_G(a^\ell b^j) = \{z^r a^\ell b^j \big| 0 \le r < p\}$.

(iii) $\mathrm{Conj}_G(a^{-1}) = \{z^r a^{-1} \big| 0 \le r < p\}$.

(iv) $\mathrm{Conj}_G((a^\ell b^j)^{-1}) = \{z^r a^{-\ell} b^{-j} \big| 0 \le r < p\}$.

Proof. (i) We have $a^b = za$. By induction, we conclude that $a^{b^r} = z^r a$ for all $r \ge 0$. It follows that

$$\mathrm{Conj}_G(a) = \{a^{b^r} \big| 0 \le r < p\} = \{z^r a \big| 0 \le r < p\}.$$

(ii) We have $b^a = a^{-1}ba = a^{-1}bab^{-1}b = a^{-1}a^{b^{p-1}}b = a^{-1}z^{p-1}ab = a^{-1}z^{-1}ab = z^{-1}b$. By induction, we conclude that $b^{a^s} = z^{-s}b$ for all $s \ge 0$. It follows that

$$\begin{aligned}\mathrm{Conj}_G(a^\ell b^j) &= \{(a^\ell b^j)^{a^s b^r} \big| 0 \le s < p^{n-1}, 0 \le r < p\}\\ &= \{(a^\ell)^{b^r} (b^j)^{a^s b^r} \big| 0 \le s < p^{n-1}, 0 \le r < p\}\\ &= \{(z^r a)^\ell (z^{-s} b)^j \big| 0 \le s < p^{n-1}, 0 \le r < p\}\\ &= \{z^{r\ell - sj} a^\ell b^j \big| 0 \le s < p^{n-1}, 0 \le r < p\}\\ &= \{z^r a^\ell b^j \big| 0 \le r < p\}.\end{aligned}$$

(iii) We have

$$\begin{aligned}\mathrm{Conj}_G(a^{-1}) &= \{(a^{-1})^g \big| g \in G\}\\ &= \{(a^g)^{-1} \big| g \in G\}\\ &\overset{\text{(i)}}{=} \{(z^r a)^{-1} \big| 0 \le r < p\}\\ &= \{z^r a^{-1} \big| 0 \le r < p\}.\end{aligned}$$

(iv) We have

$$z^{-j\ell}a^{-\ell}b^{-j}a^\ell b^j = z^{-j\ell}a^{-\ell}(z^j a)^\ell = z^{-j\ell}a^{-\ell}z^{j\ell}a^\ell = 1$$

and, hence,

$$(a^\ell b^j)^{-1} = z^{-j\ell}a^{-\ell}b^{-j}.$$

From (ii), we now see that

$$\begin{aligned}\mathrm{Conj}_G((a^\ell b^j)^{-1}) &= \{z^{-r}(a^\ell b^j)^{-1} \big| 0 \le r < p\}\\ &= \{z^r a^{-\ell} b^{-j} \big| 0 \le r < p\}.\end{aligned}$$

□

Lemma 2.20. *Let $G = SD_n$ for some $n \geq 4$, $G = Q_n$ for some $n \geq 3$, $G = M_n(2)$ for some $n \geq 4$, or $G = M_n(p)$ for some $n \geq 3$ and some odd prime p. Then,* $\Delta_2(G) = \Delta(G)$.

Proof. Since $\Gamma_2(G) \subseteq \Gamma(G)$, we have $\Delta_2(G) \leq \Delta(G)$. Now, we want to show that $\Delta(G) \leq \Delta_2(G)$. Let $S \in \Gamma(G)$. We see from Lemmas 2.9 and 2.18 that there is a subset T of S such that $T \in \Gamma_2(G)$. Since $\|G\|_S \leq \|G\|_T$, we have

$$\begin{aligned}\Delta(G) &= \sup\{\|G\|_S \mid S \in \Gamma(G)\}\\ &\leq \sup\{\|G\|_T \mid T \in \Gamma_2(G)\}\\ &= \Delta_2(G).\end{aligned}$$

□

3. Proof of Theorem 1.4

Proof of Theorem 1.4. Let $n \geq 4$ be a natural number , $G := SD_n$, and (a, b) be a standard generator pair of G. Let $0 < \hat{o}_1, \hat{o}_2 < 2^{n-1}$ be fixed and odd and $0 \leq v_1 < 2^{n-1}$ be fixed and even. Set

$$\begin{aligned}S_1 &:= \{a^{v_1}b, a^{\hat{o}_1}\},\\ S_2 &:= \{a^{\hat{o}_2}b, a^{\hat{o}_1}\},\\ S_3 &:= \{a^{\hat{o}_2}b, a^{v_1}b\}.\end{aligned}$$

From Lemmas 2.9 and 2.20, we see that we only need to consider $\|G\|_{S_j}$, where $1 \leq j \leq 3$, in order to determine $\Delta(G)$. In the sense of (1.1), and in view of Lemma 2.6, we have

$$\begin{aligned}C_1 &:= \mathrm{Conj}_G({S_1}^{\pm 1}) = \{a^v b \big| 0 \leq v < 2^{n-1} \text{ is even}\} \cup \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\},\\ C_2 &:= \mathrm{Conj}_G({S_2}^{\pm 1}) = \{a^{\hat{o}} b \big| 0 < \hat{o} < 2^{n-1} \text{ is odd}\} \cup \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\},\\ C_3 &:= \mathrm{Conj}_G({S_3}^{\pm 1}) = \{a^{\ell} b \big| 0 \leq \ell < 2^{n-1}\}.\end{aligned}$$

For the reader's convenience, and to make the proof easy to follow, we set the following:

$$\begin{aligned}\hat{C}_1 &:= G \setminus C_1 = \{a^{\hat{o}} b \big| 0 < \hat{o} < 2^{n-1} \text{ is odd}\} \cup \langle a\rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\},\\ \hat{C}_2 &:= G \setminus C_2 = \{a^{v} b \big| 0 \leq v < 2^{n-1} \text{ is even}\} \cup \langle a\rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\},\\ \hat{C}_3 &:= G \setminus C_3 = \langle a\rangle.\end{aligned}$$

Next, we study $\|G\|_{S_j}$, where $1 \leq j \leq 3$.

(i) We show that

$$\|G\|_{S_1} = \begin{cases} 2 & \text{if } n = 4,\\ 3 & \text{if } n \geq 5.\end{cases}$$

For every $g \in C_1$, we have

$$\|g\|_{S_1} = 1.$$

Now, suppose that $g \in \hat{C}_1 \setminus \{1\}$. Then, g is either

$$a^{\hat{o}}b = a^{\hat{o}_1} \cdot a^{v}b \in B_{S_1}(2),$$

where $0 < \hat{o} < 2^{n-1}$ is odd and $v = \hat{o} - \hat{o}_1$,

or

$$g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\}.$$

If the former holds, then $||g||_{S_1} = 2$. Assume now $g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\}$.

Case 1: $n = 4$.

It is easy to see that $\{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\} = \{a, a^3, a^5, a^7\}$. Hence, g can be written as

$$a^{v} = a^{v}b \cdot b \in B_{S_1}(2),$$

where $0 < v < 8$ is even. Thus, $||g||_{S_1} = 2$.

Case 2: $n \geq 5$.

Let $0 < \ell < 2^{n-1}$ such that $g = a^{\ell}$. If ℓ is even, then

$$a^{\ell} = a^{\ell}b \cdot b \in B_{S_1}(2)$$

and, hence, $||g||_{S_1} = 2$. Assume now that ℓ is odd. One can see from Lemma 2.10 that $||a^{\ell}||_{S_1} \neq 2$. But, we have

$$a^{\ell} = a^{\ell}b \cdot b \in B_{S_1}(2) \cdot B_{S_1}(1) = B_{S_1}(3)$$

by Lemma 2.2 ; hence, $||g||_{S_1} = 3$.

Now, let $g = 1$; then, by convention, $\{1\} = B_{S_1}(0)$ and, thus, $||g||_{S_1} = 0$. Hence, $||G||_{S_1} = 2$ when $n = 4$ and $||G||_{S_1} = 3$ when $n \geq 5$.

(ii) We show that

$$||G||_{S_2} = \begin{cases} 2 & \text{if } n = 4, \\ 3 & \text{if } n \geq 5. \end{cases}$$

For every $g \in C_2$, we have

$$||g||_{S_2} = 1.$$

Now, suppose that $g \in \hat{C}_2 \setminus \{1\}$. Then, g is either

$$a^{v}b = a^{\hat{o}_1} \cdot a^{\hat{o}}b \in B_{S_2}(2),$$

where $0 \leq v < 2^{n-1}$ is even and $\hat{o} = v - \hat{o}_1$,

or

$$g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\}.$$

If the former holds, then $||g||_{S_2} = 2$. Assume now $g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\}$.

Case 1: $n = 4$.

As in (i) above, we have $\{a^{\pm\hat{o}_1}, (a^{-1+2^{n-2}})^{\pm\hat{o}_1}\} = \{a, a^3, a^5, a^7\}$. Hence, g can be written as

$$a^{v} = a^{\hat{o}}b \cdot ab \overset{2.10(\mathrm{i})}{=} a^{\hat{o}-1+2^{n-2}} \in B_{S_2}(2),$$

where $0 < v < 8$ is even and $\hat{o} = v + 1 - 2^{n-2}$. Thus, $||g||_{S_2} = 2$.

Case 2: $n \geq 5$.

Let $0 < \ell < 2^{n-1}$ such that $g = a^\ell$. If ℓ is even, then

$$a^\ell = a^{\hat{o}} b \cdot ab \overset{2.10(i)}{=} a^{\hat{o}-1+2^{n-2}} \in B_{S_2}(2),$$

where $\hat{o} = \ell + 1 - 2^{n-1}$ and, hence, $||g||_{S_2} = 2$. Assume now that ℓ is odd. One can see from Lemma 2.10 that $||a^\ell||_{S_2} \neq 2$. But, we have

$$a^\ell = a^\ell b \cdot b \in B_{S_2}(1) \cdot B_{S_2}(2) = B_{S_2}(3)$$

by Lemma 2.2; hence, $||g||_{S_2} = 3$.

Now, let $g = 1$; then, by convention, $\{1\} = B_{S_2}(0)$ and, thus, $||g||_{S_2} = 0$. Hence, $||G||_{S_2} = 2$ when $n = 4$ and $||G||_{S_2} = 3$ when $n \geq 5$.

(iii) We show $||G||_{S_3} = 2$.

For every $g \in C_3$, we have

$$||g||_{S_3} = 1.$$

Now, suppose that $g \in \hat{C}_3 \setminus \{1\}$. Then, g can be written as

$$a^\ell = a^\ell b \cdot b \in B_{S_3}(2),$$

where $0 < \ell < 2^{n-1}$.

Now, let $g = 1$; then, by convention, $\{1\} = B_{S_3}(0)$ and, thus, $||g||_{S_3} = 0$. So, $||G||_{S_3} = 2$.

In view of (i)–(iii) and Lemma 2.9, we have $\Delta_2(G) = 2$ if $n = 4$ and $\Delta_2(G) = 3$ if $n > 4$. So, the result follows from that fact that $\Delta_2(G) = \Delta(G)$ (see Lemma 2.20). □

4. Proof of Theorem 1.5

Proof of Theorem 1.5. Let $n \geq 3$ be a natural number , $G := Q_n$, and (a, b) be a standard generator pair of G. Let $0 < \hat{o}_1, \hat{o}_2 < 2^{n-1}$ be fixed and odd and $0 \leq v_1 < 2^{n-1}$ be fixed and even. Set

$$S_1 := \{a^{v_1} b, a^{\hat{o}_1}\},$$
$$S_2 := \{a^{\hat{o}_2} b, a^{\hat{o}_1}\},$$
$$S_3 := \{a^{\hat{o}_2} b, a^{v_1} b\}.$$

From Lemmas 2.9 and 2.20, we see that we only need to consider $||G||_{S_j}$, where $1 \leq j \leq 3$, in order to determine $\Delta(G)$. In the sense of (1.1), and in view of Lemma 2.8, we have

$$C_1 := \mathrm{Conj}_G(S_1{}^{\pm 1}) = \{a^v b \big| 0 \leq v < 2^{n-1} \text{ is even}\} \cup \{a^{\pm \hat{o}_1}\},$$
$$C_2 := \mathrm{Conj}_G(S_2{}^{\pm 1}) = \{a^{\hat{o}} b \big| 0 < \hat{o} < 2^{n-1} \text{ is odd}\} \cup \{a^{\pm \hat{o}_1}\},$$
$$C_3 := \mathrm{Conj}_G(S_3{}^{\pm 1}) = \{a^\ell b \big| 0 \leq \ell < 2^{n-1}\}.$$

For the reader's convenience, and to make the proof easy to follow, we set the following:

$$\hat{C}_1 := G \setminus C_1 = \{a^{\hat{o}}b \big| 0 < \hat{o} < 2^{n-1} \text{ is odd}\} \cup \langle a \rangle \setminus \{a^{\pm\hat{o}_1}\},$$

$$\hat{C}_2 := G \setminus C_2 = \{a^{v}b \big| 0 \le v < 2^{n-1} \text{ is even }\} \cup \langle a \rangle \setminus \{a^{\pm\hat{o}_1}\},$$

$$\hat{C}_3 := G \setminus C_3 = \langle a \rangle.$$

Next, we study $||G||_{S_j}$, where $1 \le j \le 3$.

(i) We show that

$$||G||_{S_1} = \begin{cases} 2 & \text{if } n = 3, \\ 3 & \text{if } n \ge 4. \end{cases}$$

For every $g \in C_1$, we have

$$||g||_{S_1} = 1.$$

Now, suppose that $g \in \hat{C}_1 \setminus \{1\}$. Then, g is either

$$a^{\hat{o}}b = a^{\hat{o}_1} \cdot a^{v}b \in B_{S_1}(2),$$

where $0 < \hat{o} < 2^{n-1}$ is odd and $v = \hat{o} - \hat{o}_1$,

or

$$g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}\}.$$

If the former holds, then $||g||_{S_1} = 2$. Assume now $g \in \langle a \rangle \setminus \{a^{\pm\hat{o}_1}\}$.

Case 1: $n = 3$.

It is easy to see that $\{a^{\pm\hat{o}_1}\} = \{a, a^3\}$. Hence, g can be written as

$$a^2 = a \cdot a \in B_{S_1}(2).$$

Thus, $||g||_{S_1} = 2$.

Case 2: $n \ge 4$.

Let $0 < \ell < 2^{n-1}$ such that $g = a^{\ell}$. If ℓ is even, then

$$a^{\ell} \overset{2.11(i)}{=} b \cdot a^{2^{n-2}-\ell}b \in B_{S_1}(2)$$

and, hence, $||g||_{S_1} = 2$. Assume now that ℓ is odd. One can see from Lemma 2.11 that $||a^{\ell}||_{S_1} \ne 2$. But, we have

$$a^{\ell} = a^{\ell - 2^{n-2}}b \cdot b \in B_{S_1}(2) \cdot B_{S_1}(1) = B_{S_1}(3)$$

by Lemma 2.2; hence, $||g||_{S_1} = 3$.

Now, let $g = 1$; then, by convention, $\{1\} = B_{S_1}(0)$ and, thus,$||g||_{S_1} = 0$. Hence, $||G||_{S_1} = 2$ when $n = 3$ and $||G||_{S_1} = 3$ when $n \ge 4$.

(ii) We show that

$$||G||_{S_2} = \begin{cases} 2 & \text{if } n = 3, \\ 3 & \text{if } n \ge 4. \end{cases}$$

For every $g \in C_2$, we have

$$\|g\|_{S_2} = 1.$$

Now, suppose that $g \in \hat{C}_2 \setminus \{1\}$. Then, g is either

$$a^v b = a^{\hat{o}_1} \cdot a^{\hat{o}} b \in B_{S_2}(2),$$

where $0 \leq v < 2^{n-1}$ is even and $\hat{o} = v - \hat{o}_1$,
or

$$g \in \langle a \rangle \setminus \{a^{\pm \hat{o}_1}\}.$$

If the former holds, then $\|g\|_{S_2} = 2$. Assume now $g \in \langle a \rangle \setminus \{a^{\pm \hat{o}_1}\}$.
Case 1: $n = 3$.
As in (i) above, we have $\{a^{\pm \hat{o}_1}\} = \{a, a^3\}$. Hence, g can be written as

$$a^2 = a \cdot a \in B_{S_2}(2).$$

Thus, $\|g\|_{S_2} = 2$.
Case 2: $n \geq 4$.
Let $0 < \ell < 2^{n-1}$ such that $g = a^\ell$. If ℓ is even, then

$$a^\ell = a^{\hat{o}} b \cdot ab \overset{2.11(\mathrm{i})}{=} a^{\hat{o}-1+2^{n-2}} \in B_{S_2}(2),$$

where $\hat{o} = \ell + 1 - 2^{n-2}$ and, hence, $\|g\|_{S_2} = 2$. Assume now that ℓ is odd. One can see from Lemma 2.11 that $\|a^\ell\|_{S_2} \neq 2$. But, we have

$$a^\ell = a^{\ell - 2^{n-2}} b \cdot b \in B_{S_2}(1) \cdot B_{S_2}(2) = B_{S_2}(3)$$

by Lemma 2.2; hence, $\|g\|_{S_2} = 3$.

Now, let $g = 1$; then, by convention, $\{1\} = B_{S_2}(0)$ and, thus, $\|g\|_{S_2} = 0$. Hence, $\|G\|_{S_2} = 2$ when $n = 3$ and $\|G\|_{S_2} = 3$ when $n \geq 4$.

(iii) We show $\|G\|_{S_3} = 2$.
For every $g \in C_3$, we have

$$\|g\|_{S_3} = 1.$$

Now, suppose that $g \in \hat{C}_3 \setminus \{1\}$. Then, g can be written as

$$a^\ell = a^{\ell - 2^{n-2}} b \cdot b \in B_{S_3}(2),$$

where $0 < \ell < 2^{n-1}$.
Now, let $g = 1$; then, by convention, $\{1\} = B_{S_3}(0)$ and, thus, $\|g\|_{S_3} = 0$. So, $\|G\|_{S_3} = 2$.

In view of (i)–(iii) and Lemma 2.9, we have $\Delta_2(G) = 2$ if $n = 3$ and $\Delta_2(G) = 3$ if $n \geq 4$. So, the result follows from the fact that $\Delta_2(G) = \Delta(G)$ (see Lemma 2.20). $\square$

5. Proof of Theorem 1.6

To establish Theorem 1.6, we need to prove a series of lemmas first. In what follows, we work under the following hypothesis.

Hypothesis 5.1. *Let p be a prime number and n be a natural number, where $n \geq 4$ if $p = 2$ and $n \geq 3$ if p is odd. Set $G := M_n(p)$; let (a, b) be a standard generator pair of G and $z := a^{p^{n-2}}$. Moreover, let $S := \{a, a^\ell b^j\}$ for some $0 \leq \ell < p^{n-1}$ and $0 < j < p$.*

Note that $z \in Z(G)$ by Lemma 2.13.

Lemma 5.2. *Let $g \in \langle a \rangle$. Then, we have the following:*

(i) If $p = 2$, then $\|g\|_S \leq 2^{n-3}$.

(ii) If p is odd and $(p, n) \neq (3, 3)$, then $\|g\|_S \leq \frac{p^{n-2}-1}{2}$.

(iii) If $p = 3 = n$, then $\|g\|_S \leq 2$.

Proof. Let $0 \leq r < p^{n-1}$ with $g = a^r$. Assume that r is divisible by p^{n-2}. Then, we have

$$g = a^r = (a^{p^{n-2}})^{\frac{r}{p^{n-2}}} = z^{\left(\frac{r}{p^{n-2}}\right)}.$$

So, with $s := \frac{r}{p^{n-2}}$, we have $g = z^s = a^{-1} \cdot z^s a \in B_S(2)$ by Lemma 2.19. Thus, $\|g\|_S \leq 2$ and, hence, (i)–(iii) hold when r is divisible by p^{n-2}.

We assume now that r is not divisible by p^{n-2}, and we treat the cases $p = 2$ and p is odd separately.

Case 1: $p = 2$.

We may write r in the form $r = m \cdot 2^{n-2} + s$, where $m \in \{0, 1, 2\}$ and $-2^{n-3} < s \leq 2^{n-3}$. Note that $s \neq 0$ by the choice of r. Then, $g = a^{m \cdot 2^{n-2}+s} = (a^{2^{n-2}})^m a^s = z^m a^s$.

If $s > 0$, then $g = z^m a \cdot a^{s-1} \in B_S(s)$ by Lemma 2.19; hence, $\|g\|_S \leq s \leq 2^{n-3}$.

If $s < 0$, then $g = z^m a^s = z^m a^{-1} a^{s+1} = z^m a^{-1} (a^{-1})^{(-s-1)} \in B_S(-s)$ by Lemma 2.19 and, hence, $\|g\|_S \leq -s < 2^{n-3}$.

Case 2: p is odd.

We may write r in the form $r = m \cdot p^{n-2} + s$, where $m \in \{0, 1, \ldots, p\}$ and $-\frac{p^{n-2}-1}{2} \leq s \leq \frac{p^{n-2}-1}{2}$. Note that $s \neq 0$ by the choice of r. Then, $g = a^{m \cdot p^{n-2}+s} = z^m a^s$.

If $s > 0$, then $g = z^m a \cdot a^{s-1} \in B_S(s)$ by Lemma 2.19 and, hence, $\|g\|_S \leq \frac{p^{n-2}-1}{2}$. In particular, if $(p, n) = (3, 3)$, then $\|g\|_S = 1 < 2$.

If $s < 0$, then $g = z^m a^s = z^m a^{-1} a^{s+1} = z^m a^{-1} (a^{-1})^{(-s-1)} \in B_S(-s)$ by Lemma 2.19 and, hence, $\|g\|_S \leq -s \leq \frac{p^{n-2}-1}{2}$. In particular, if $(p, n) = (3, 3)$, then $\|g\|_S = 1 < 2$. □

Lemma 5.3. *Let $g \in G \setminus \langle a \rangle$. Then, the following holds:*

(i) If $p = 2$, then $\|g\|_S \leq 2^{n-3} + 1$.

(ii) If p is odd and $(n, p) \neq (3, 3)$, then $\|g\|_S \leq \frac{p^{n-2}+p-2}{2}$.

Proof. Assume that $p = 2$. Since $g \in G \setminus \langle a \rangle$, we have $g = a^r b$ for some $0 \le r < 2^{n-1}$. By Lemma 5.2(i), we have $a^{r-\ell} \in B_S(2^{n-3})$. Also, we have $a^\ell b \in S \subseteq B_S(1)$. Now, Lemma 2.2 implies that $g = a^r b = a^{r-\ell} a^\ell b \in B_S(2^{n-3} + 1)$. In other words, $\|g\|_S \le 2^{n-3} + 1$, so (i) holds.

Assume now that p is odd and $(n, p) \neq (3, 3)$. Since $g \in G \setminus \langle a \rangle$, we have $g = a^r b^s$ for some $0 \le r < p^{n-1}$ and $0 < s < p$. Because $0 < j < p$ and $\operatorname{ord}(b) = p$, we have $\operatorname{ord}(b^j) = p$, and this easily implies that

$$\langle b \rangle = \langle b^j \rangle = \left\{ b^{jk} \mid -\frac{p-1}{2} \le k \le \frac{p-1}{2} \right\} = \left\{ b^{jk} \mid 0 \le k \le \frac{p-1}{2} \right\} \cup \left\{ b^{-jk} \mid 0 \le k \le \frac{p-1}{2} \right\}.$$

Since $1 \neq b^s \in \langle b \rangle$, we have $b^s = b^{jk}$ or $b^s = b^{-jk}$ for some $0 < k \le \frac{p-1}{2}$. By Lemma 2.15, we have

$$(a^\ell b^j)^k = a^{k\ell} b^{kj} z^{-\frac{k(k-1)}{2} j\ell}$$

and

$$(a^{-\ell} b^{-j})^k = a^{-k\ell} b^{-kj} z^{-\frac{k(k-1)}{2} j\ell}.$$

Suppose that $b^s = b^{jk}$. Then,

$$(a^\ell b^j)^k = a^{k\ell} z^{-\frac{k(k-1)}{2} j\ell} b^s.$$

Set $u := a^{k\ell} z^{-\frac{k(k-1)}{2} j\ell}$; then, $(a^\ell b^j)^k = u b^s$. We have $g = a^r b^s = a^r u^{-1} u b^s = a^r u^{-1} (a^\ell b^j)^k$. By Lemma 5.2(ii), we have $a^r u^{-1} \in B_S(\frac{p^{n-2}-1}{2})$. Moreover, $(a^\ell b^j)^k \in B_S(\frac{p-1}{2})$ since $k \le \frac{p-1}{2}$. Applying Lemma 2.2, we conclude that $g \in B_S(\frac{p^{n-2}-1}{2} + \frac{p-1}{2}) = B_S(\frac{p^{n-2}+p-2}{2})$; hence, $\|g\|_S \le \frac{p^{n-2}+p-2}{2}$. This completes the proof of (ii) for the case that $b^s = b^{jk}$.

Assume now that $b^s = b^{-jk}$. Then,

$$(a^{-\ell} b^{-j})^k = a^{-k\ell} z^{-\frac{k(k-1)}{2} j\ell} b^s.$$

With $u := a^{-k\ell} z^{-\frac{k(k-1)}{2} j\ell}$, we have that $(a^{-\ell} b^{-j})^k = u b^s$ and $g = a^r b^s = a^r u^{-1} u b^s = a^r u^{-1} (a^{-\ell} b^{-j})^k$. As in the case in which $b^s = b^{jk}$, we see that $a^r u^{-1} \in B_S(\frac{p^{n-2}-1}{2})$, and, from Lemma 2.19(iv), we see that $(a^{-\ell} b^{-j})^k \in B_S(k) \subseteq B_S(\frac{p-1}{2})$. As in the case in which $b^s = b^{jk}$, it follows that $\|g\|_S \le \frac{p^{n-2}+p-2}{2}$. The proof is now complete. □

Lemma 5.4. *Assume that $n = p = 3$. If $g \in G \setminus \langle a \rangle$, then $\|g\|_S \le 2$.*

Proof. Let $0 \le r < 9$ and $0 < s < 3$ such that $g = a^r b^s$. Note that $\langle b^s \rangle = \langle b \rangle = \langle b^j \rangle$.

Case 1: ℓ is not divisible by 3.
The elements $a^\ell, za^\ell, z^2 a^\ell, a^{-\ell}, za^{-\ell}, z^2 a^{-\ell}$ are easily seen to be mutually distinct, and they are not contained in $\langle z \rangle$. So, it follows that $\langle a \rangle \setminus \langle z \rangle = \{a^\ell, za^\ell, z^2 a^\ell, a^{-\ell}, za^{-\ell}, z^2 a^{-\ell}\}$. Likewise, one can see that $\langle a \rangle \setminus \langle z \rangle = \{a, za, z^2 a, a^{-1}, za^{-1}, z^2 a^{-1}\}$. Together with Lemma 2.19, it follows that

$$\begin{aligned} \{a^\ell, za^\ell, z^2 a^\ell, a^{-\ell}, za^{-\ell}, z^2 a^{-\ell}\} &= \langle a \rangle \setminus \langle z \rangle \\ &= \{a, za, z^2 a, a^{-1}, za^{-1}, z^2 a^{-1}\} \\ &= \operatorname{Conj}_G(a) \cup \operatorname{Conj}_G(a^{-1}). \end{aligned}$$

Case 1.1: r is not divisible by 3, $s = j$.

In this case, $a^r \notin \langle z\rangle$. Therefore, by the above observations, we have $a^r = z^m a^\ell$ or $a^r = z^m a^{-\ell}$ for some $0 \le m < 3$. If the former holds, then $g = z^m a^\ell b^j \in \mathrm{Conj}_G(a^\ell b^j)$ by Lemma 2.19(ii) and, hence, $\|g\|_S = 1 < 2$. If $a^r = z^m a^{-\ell}$, then $g = z^m a^{-\ell} b^j = a^{-2\ell} z^m a^\ell b^j$. Since $a^{-2\ell} \in \langle a\rangle\backslash\langle z\rangle = \mathrm{Conj}_G(a) \cup \mathrm{Conj}_G(a^{-1})$ and $z^m a^\ell b^j \in \mathrm{Conj}_G(a^\ell b^j)$ by Lemma 2.19(ii), it follows that $\|g\|_S \le 2$.

Case 1.2: r is not divisible by 3, $s \neq j$.

In this case, $b^s = b^{-j}$. Also, $a^r = z^m a^\ell$ or $z^m a^{-\ell}$ for some $0 \le m < 3$. If the latter holds, then $g = z^m a^{-\ell} b^{-j} \in B_S(1)$ by Lemma 2.19(iv) and, hence, $\|g\|_S = 1 < 2$. If $a^r = z^m a^\ell$, then $g = z^m a^\ell b^{-j} = a^{2\ell} z^m a^{-\ell} b^{-j}$, and, since $a^{2\ell} \in \langle a\rangle \setminus \langle z\rangle = \mathrm{Conj}_G(a) \cup \mathrm{Conj}_G(a^{-1})$ and $z^m a^{-\ell} b^{-j} \in \mathrm{Conj}_G((a^\ell b^j)^{-1})$ by Lemma 2.19(iv), it follows that $\|g\|_S \le 2$.

Case 1.3: r is divisible by 3.

In this case, $g = z^m b^j$ or $g = z^m b^{-j}$ for some $0 \le m < 3$. In the former case, we have $g = a^{-\ell} z^m a^\ell b^j$, and, in the latter case, we have $g = a^\ell z^m a^{-\ell} b^{-j}$. We have $a^\ell, a^{-\ell} \in \langle a\rangle\backslash\langle z\rangle = \mathrm{Conj}_G(a) \cup \mathrm{Conj}_G(a^{-1})$; we also have that $z^m a^\ell b^j \in \mathrm{Conj}_G(a^\ell b^j)$ by Lemma 2.19(ii) and $z^m a^{-\ell} b^{-j} \in \mathrm{Conj}_G((a^\ell b^j)^{-1})$ by Lemma 2.19(iv), so it follows that $\|g\|_S \le 2$.

Case 2: ℓ is divisible by 3.

In this case, $a^\ell = z^t$ for some $0 \le t < 3$. Note that $g = a^r b^j$ or $g = a^r b^{-j}$. Assume that r is divisible by 3. Then $g = z^m b^j$ or $g = z^m b^{-j}$ for some $0 \le m < 3$. If the former holds, then $g = z^m b^j = z^{m-t} z^t b^j = z^{m-t} a^\ell b^j \in \mathrm{Conj}_G(a^\ell b^j)$ by Lemma 2.19(ii) and, hence, $\|g\|_S = 1 < 2$. Otherwise, if $g = z^m b^{-j}$, then $g = z^m b^{-j} = z^{m+t} z^{-t} b^{-j} = z^{m+t} a^{-\ell} b^{-j} \in \mathrm{Conj}_G((a^\ell b^j)^{-1})$ by Lemma 2.19(iv); hence, $\|g\|_S = 1 < 2$. Assume now that r is not divisible by 3. Then, $r-1$ or $r+1$ is divisible by 3; thus, a^{r-1} or a^{r+1} lies in $\langle z\rangle$. Hence, $a^r = z^m a$ or $z^m a^{-1}$ for some $0 \le m < 3$. If $a^r = z^m a$, then either $g = az^m b^j = az^{m-t} z^t b^j = az^{m-t} a^\ell b^j$ or $g = az^m b^{-j} = az^{m+t} z^{-t} b^{-j} = az^{m+t} a^{-\ell} b^{-j}$; so, it follows from Lemma 2.19(ii), (iv) that $\|g\|_S \le 2$. If $a^r = z^m a^{-1}$, then we either have $g = a^{-1} z^m b^j = a^{-1} z^{m-t} z^t b^j = a^{-1} z^{m-t} a^\ell b^j$ or $g = a^{-1} z^m b^{-j} = a^{-1} z^{m+t} z^{-t} b^{-j} = a^{-1} z^{m+t} a^{-\ell} b^{-j}$; then it once again follows from Lemma 2.19(ii), (iv) that $\|g\|_S \le 2$. □

Lemma 5.5. *Let* $X_1 := \langle z\rangle \cdot \{a, a^{-1}\}$, $X_2 := \langle z\rangle \cdot \{b, b^{-1}\}$, *and* $X := X_1 \cup X_2$. *Let* $g \in G$ *and* s, t *be non-negative integers such that* g *can be written in the form* $g = x_1 \cdots x_{s+t}$ *such that* $x_i \in X$ *for all* $1 \le i \le s+t$, $|\{1 \le i \le s+t \mid x_i \in X_1\}| = s$, *and* $|\{1 \le i \le s+t \mid x_i \in X_2\}| = t$. *Then,* $g = z^r a^{s_0} b^{t_0}$ *for some* $0 \le r < p$, $-s \le s_0 \le s$, *and* $-t \le t_0 \le t$.

Proof. We proceed by induction over $k := s+t$. If $k = 0$, then $g = 1 = z^0 a^0 b^0$; thus the lemma is true for $k = 0$. Assume now that $k \ge 1$ and suppose that the following holds: If $g' \in G$ and s', t' are non-negative integers with $s' + t' < k$ such that g' can be written in the form $g' = x'_1 \cdots x'_{s'+t'}$, where $x'_i \in X$ for all $1 \le i \le s'+t'$, $|\{1 \le i \le s'+t' \mid x'_i \in X_1\}| = s'$, and $|\{1 \le i \le s'+t' \mid x'_i \in X_2\}| = t'$, then $g' = z^{r'} a^{s'_0} b^{t'_0}$ for some $0 \le r' < p$, $-s' < s'_0 < s'$, $-t' < t'_0 < t'$ (induction hypothesis).

By the hypotheses of the lemma, we have $g = x_1 \cdots x_k$ for some $x_1, \ldots, x_k \in X$, where $|\{1 \le i \le k \mid x_i \in X_1\}| = s$ and $|\{1 \le i \le k \mid x_i \in X_2\}| = t$. Using the induction hypothesis, we are going to prove that $g = z^r a^{s_0} b^{t_0}$ for some $0 \le r < p$, $-s \le s_0 \le s$, and $-t \le t_0 \le t$. Set $h := x_1 \cdots x_{k-1}$. We split the proof into two cases.

Case 1: $x_k \in X_1$.

In this case, $|\{1 \le i \le k-1 \mid x_i \in X_1\}| = s-1$ and $|\{1 \le i \le k-1 \mid x_i \in X_2\}| = t$. Therefore, by the induction hypothesis, $h = z^{r'} a^{s'_0} b^{t'_0}$ for some $0 \le r' < p$, $-(s-1) \le s'_0 \le s-1$, and $-t \le t'_0 \le t$. Since $x_k \in X_1$, we have $x_k = z^{r''} a^\varepsilon$ for some $0 \le r'' < p$ and $\varepsilon \in \{\pm 1\}$. Thus, $g = h \cdot x_k = z^{r'} a^{s'_0} b^{t'_0} z^{r''} a^\epsilon =$

$z^{r'+r''}a^{s_0'}b^{t_0'}a^{\epsilon}$. From Lemma 2.14, one can easily see that $b^{t_0'}a^{\epsilon} = z^{r'''}a^{\epsilon}b^{t_0'}$, where $r''' \in \{t_0', -t_0'\}$. Then, it follows that $g = z^{r'+r''}a^{s_0'}b^{t_0'}a^{\epsilon} = z^{r'+r''+r'''}a^{s_0'}a^{\epsilon}b^{t_0'} = z^{r'+r''+r'''}a^{s_0'+\epsilon}b^{t_0'}$. Now, let $0 \le r < p$ with $r \equiv r' + r'' + r''' \bmod p$, and set $s_0 := s_0' + \epsilon, t_0 := t_0'$. Then, $g = z^r a^{s_0} b^{t_0}$, and we have that $-s \le -(s-1) + \epsilon \le s_0 \le (s-1) + \epsilon \le s, -t \le t_0 \le t$. This completes the proof of the lemma for the case of $x_k \in X_1$.

Case 2: $x_k \in X_2$.
In this case, $|\{1 \le i \le k-1 \mid x_i \in X_1\}| = s$ and $|\{1 \le i \le k-1 \mid x_i \in X_2\}| = t-1$. Therefore, by the induction hypothesis, $h = z^{r'}a^{s_0'}b^{t_0'}$ for some $0 \le r' < p, -s \le s_0' \le s$, and $-(t-1) \le t_0' \le t-1$. Since $x_k \in X_2$, we have that $x_k = z^{r''}b^{\varepsilon}$ for some $0 \le r'' < p$ and $\varepsilon \in \{\pm 1\}$. Then, $g = hx_k = z^{r'}a^{s_0'}b^{t_0'}x_k = z^{r'+r''}a^{s_0'}b^{t_0'+\epsilon}$. Let $0 \le r < p$ with $r \equiv r' + r'' \bmod p, s_0 := s_0'$, and $t_0 := t_0' + \epsilon$. Then, $g = z^r a^{s_0} b^{t_0}$, and we have that $-s \le s_0 \le s$ and $-t \le t_0 \le t$. This completes the proof of the lemma for the case of $x_k \in X_2$. □

Lemma 5.6. *Let $T := \{a, b\}$. Then,*

(i) $\|G\|_T \ge 2^{n-3} + 1$ *if* $p = 2$,

(ii) $\|G\|_T \ge \frac{p^{n-2}+p-2}{2}$ *if p is odd.*

Proof. Let $X_1 := \langle z \rangle \cdot \{a, a^{-1}\}$, $X_2 := \langle z \rangle \cdot \{b, b^{-1}\}$ and $X := X_1 \cup X_2$. From Lemma 2.19, we see that $X = \mathrm{Conj}_G(T^{\pm 1})$.

Assume that $p = 2$, and set $g := a^{2^{n-3}}b$. We show that $\|g\|_T \ge 2^{n-3} + 1$. Let $k \ge 1$ and $x_1, \dots, x_k \in X$ with $g = x_1 \cdots x_k$. Set $s := |\{1 \le i \le k \mid x_i \in X_1\}|$ and $t := |\{1 \le i \le k \mid x_i \in X_2\}|$. Then, by Lemma 5.5, we have $a^{2^{n-3}}b = g = z^r a^{s_0} b^{t_0}$ for some $r \in \{0, 1\}$ and $-s \le s_0 \le s$, $-t \le t_0 \le t$. This implies that $a^{2^{n-3}} = z^r a^{s_0}$ and $b = b^{t_0}$. If $s < 2^{n-3}$, then $z^r a^{s_0}$ has the form $a^m, a^{2^{n-1}-m}, a^{2^{n-2}+m}$, or $a^{2^{n-2}-m}$ for some $0 \le m < 2^{n-3}$; hence, $z^r a^{s_0} \ne a^{2^{n-3}}$. Thus, $s \ge 2^{n-3}$. Also, $t \ge 1$ because, otherwise, $b = b^{t_0} = b^0 = 1$. So, we have $k = s + t \ge 2^{n-3} + 1$. Since $x_1, \dots, x_k$ were arbitrarily chosen elements of $X = \mathrm{Conj}_G(T^{\pm 1})$ with $g = x_1 \cdots x_k$, we can now conclude that $\|g\|_T \ge 2^{n-3} + 1$. In particular, we have $\|G\|_T \ge 2^{n-3} + 1$, completing the proof of (i).

Assume now that p is odd, and set $g := a^{\frac{p^{n-2}-1}{2}}b^{\frac{p-1}{2}}$. We show that $\|g\|_T \ge \frac{p^{n-2}+p-2}{2}$. Let $k \ge 1$ and $x_1, \dots, x_k \in X$ with $g = x_1 \cdots x_k$. Set $s := |\{1 \le i \le k \mid x_i \in X_1\}|$ and $t := |\{1 \le i \le k \mid x_i \in X_2\}|$. Then, by Lemma 5.5, we have $a^{\frac{p^{n-2}-1}{2}}b^{\frac{p-1}{2}} = g = z^r a^{s_0} b^{t_0}$ for some $0 \le r < p$ as well as some $-s \le s_0 \le s$, $-t \le t_0 \le t$. This implies that $a^{\frac{p^{n-2}-1}{2}} = z^r a^{s_0}$ and $b^{t_0} = b^{\frac{p-1}{2}}$. If $s < \frac{p^{n-2}-1}{2}$, then one can see, similarly as in the case in which $p = 2$, that $z^r a^{s_0}$ cannot be $a^{\frac{p^{n-2}-1}{2}}$. So, it follows that $s \ge \frac{p^{n-2}-1}{2}$. Also, it follows from $b^{t_0} = b^{\frac{p-1}{2}}$ that $t \ge \frac{p-1}{2}$. Consequently, we have $k = s + t \ge \frac{p^{n-2}+p-2}{2}$. Since $x_1, \dots, x_k$ were arbitrarily chosen elements of $X = \mathrm{Conj}_G(T^{\pm 1})$ with $g = x_1 \cdots x_k$, we can now conclude that $\|g\|_T \ge \frac{p^{n-2}+p-2}{2}$. In particular, we have $\|G\|_T \ge \frac{p^{n-2}+p-2}{2}$, completing the proof of (ii). □

With the above lemmas at hand, we can now prove Theorem 1.6.

Proof of Theorem 1.6. Let p be a prime number and n be a natural number, where $n \ge 4$ if $p = 2$ and $n \ge 3$ if p is odd, and let $G := M_n(p)$. Let $S \in \Gamma_2(G)$. By Lemma 2.18, there is a standard generator pair (a, b) of G such that $S = \{a, a^{\ell}b^j\}$ for some $0 \le \ell < p^{n-1}$ and $0 < j < p$.

Assume that $p = 2$. By Lemmas 5.2(i) and 5.3(i), we have $\|G\|_S \le 2^{n-3} + 1$. Because of Lemma 5.6, we even have equality when $S = \{a, b\}$. So, it follows that $\Delta_2(G) = 2^{n-3} + 1$, and Lemma 2.20 implies that $\Delta(G) = 2^{n-3} + 1$.

Assume now that p is odd and $(n, p) \neq (3, 3)$. By Lemmas 5.2(ii) and 5.3(ii), we have $\|G\|_S \leq \frac{p^{n-2}+p-2}{2}$, and, because of Lemma 5.6, we even have equality when $S = \{a, b\}$. Applying Lemma 2.20, we conclude that $\Delta(G) = \Delta_2(G) = \frac{p^{n-2}+p-2}{2}$.

Assume now that $n = p = 3$. From Lemmas 5.2(iii) and 5.4, we see that $\|G\|_S \leq 2$, and, because of Lemma 5.6, we even have $\|G\|_S = 2$ when $S = \{a, b\}$. Applying Lemma 2.20, we conclude that $\Delta(G) = \Delta_2(G) = 2 = \frac{3^{3-2}+3-2}{2}$. □

6. Conclusions

After the derivation of the conjugacy diameters of dihedral groups in [1, Theorem 6.0.2] and [12, Example 2.8], we proved further results about conjugacy diameters of non-abelian finite groups with cyclic maximal subgroups. Namely, we have determined the conjugacy diameters of the semidihedral 2-groups, the generalized quaternion groups and the modular p-groups. In this manner, the conjugacy diameters of non-abelian finite p-groups with cyclic maximal subgroups have been comprehensively calculated. We believe that the strategies applied in the proofs of our results could also be used to study the conjugacy diameters of other finite groups. For example, we think that one could proceed similarly as in the proofs of Theorems 1.4 and 1.5 to study the conjugacy diameters of the generalized dihedral groups.

Our results also lead to a question concerning the relation between the conjugacy class sizes of a finite group and its conjugacy diameter. We found that the semidihedral 2-groups and the generalized quaternion groups have relatively small conjugacy diameters, while the elements not lying in a cyclic maximal subgroup have, in relation to the group order, relatively large conjugacy class sizes. On the other hand, we found that the conjugacy diameters of the modular p-groups $M_n(p)$ grow fast as n grows, while the conjugacy classes of $M_n(p)$ are relatively small (they have at most p elements). Considering this observation, it would be interesting to study how the conjugacy diameters of finite groups are influenced by conjugacy class sizes. Note that [12, Proposition 7.1] addresses this question.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We dedicate this paper to our former supervisor Professor Benjamin Martin. You have our deepest thanks.

Conflict of interest

The authors declare no conflict of interest.

References

1. F. Aseeri, Uniform boundedness of groups, Ph.D thesis, University of Aberdeen, 2022.
2. V. Bardakov, V. Tolstykh, V. Vershinin, Generating groups by conjugation-invariant sets, *J. Algebra Appl.*, **11** (2012), 1250071. https://doi.org/10.1142/S0219498812500715
3. M. Brandenbursky, Ś. Gal, J. Kędra, M. Marcinkowski, The cancellation norm and the geometry of bi-invariant word metrics, *Glasgow Math. J.*, **58** (2015), 153–176. https://doi.org/10.1017/S0017089515000129
4. M. Brandenbursky, J. Kędra, Fragmentation norm and relative quasimorphisms, *Proc. Amer. Math. Soc.*, **150** (2022), 4519–4531. https://doi.org/10.1090/proc/14683
5. D. Burago, S. Ivanov, L. Polterovich, Conjugation-invariant norms on groups of geometric origin, *Adv. Stud. Pure Math.*, **52** (2008), 221–250. https://doi.org/10.2969/aspm/05210221
6. P. Dutta, R. K. Nath, Various energies of commuting graphs of some super integral groups, *Indian J. Pure Appl. Math.*, **52** (2021), 1–10. https://doi.org/10.1007/s13226-021-00131-7
7. J. Dutta, R. K. Nath, Laplacian and signless Laplacian spectrum of commuting graphs of finite groups, *Khayyam J. Math.*, **4** (2018), 77–87. https://doi.org/10.22034/KJM.2018.57490
8. W. N. T. Fasfous, R. K. Nath, Inequalities involving energy and Laplacian energy of non-commuting graphs of finite groups, *Indian J. Pure Appl. Math.*, 2023. https://doi.org/10.1007/s13226-023-00519-7
9. W. N. T. Fasfous, R. Sharafdini, R. K. Nath, Common neighborhood spectrum of commuting graphs of finite groups, *Algebra Discret. Math.*, **32** (2021), 33–48. http://doi.org/10.12958/adm1332
10. D. Gorenstein, *Finite Groups*, 2 Eds., New York: Chelsea Publishing Co, 1980.
11. M. Kawasaki, Relative quasimorphisms and stably unbounded norms on the group of symplectomorphisms of the Euclidean spaces, *J. Symplect. Geom.*, **14** (2016), 297–304. https://doi.org/10.4310/JSG.2016.v14.n1.a11
12. J. Kędra, A. Libman, B. Martin, Strong and uniform boundedness of groups, *J. Topol. Anal.*, **15** (2023), 707–739. https://doi.org/10.1142/S1793525321500497
13. H. Kurzweil, B. Stellmacher, *The theory of finite groups*, New York: Springer-Verlag, 2004. https://doi.org/10.1007/b97433
14. A. Libman, C. Tarry, Conjugation diameter of the symmetric groups, *Involve*, **13** (2020), 655–672, https://doi.org/10.2140/involve.2020.13.655
15. A. Muranov, Finitely generated infinite simple groups of infinite square width and vanishing stable commutator length, *J. Topol. Anal.*, **2** (2010), 341–384. https://doi.org/10.1142/S1793525310000380
16. R. K. Nath, W. N. T. Fasfous, K. C. Das, Y. Shang, Common neighborhood energy of commuting graphs of finite groups, *Symmetry*, **13** (2021), 1651. https://doi.org/10.3390/sym13091651

AIMS Press