BOUND ON THE DIAMETER OF
SPLIT METACYCLIC GROUPS

KASHYAP RAJEEVSARATHY AND SIDDHARTHA SARKAR

Abstract. Let \( G_{m,n,k} = \mathbb{Z}_m \rtimes_k \mathbb{Z}_n \) be the split metacyclic group, where \( k \) is a unit modulo \( n \). We derive an upper bound for the diameter of \( G_{m,n,k} \) using an arithmetic parameter called the weight, which depends on \( n, k \), and the order of \( k \). As an application, we show how this would determine a bound on the diameter of an arbitrary metacyclic group.

1. Introduction

The diameter of a finite group \( G \) with respect to a generating set \( S \) is the graph diameter of the Cayley graph \( \Gamma(G, S) \) of \( G \) with respect to \( S \). Consider the semidirect product of the two cyclic groups \( \mathbb{Z}_m \) and \( \mathbb{Z}_n \) given by the presentation

\[
G_{m,n,k} := \mathbb{Z}_m \rtimes_k \mathbb{Z}_n = \langle x, y | x^m = y^n = 1, x^{-1}yx = y^k \rangle,
\]

where \( \mathbb{Z}_m = \langle x \rangle \), \( \mathbb{Z}_n = \langle y \rangle \), and \( k \in \mathbb{Z}_n^* \) of order \( \alpha \mid m \), where \( \mathbb{Z}_n^* \) denote the group of units of \( \mathbb{Z}_n \) with respect to multiplication. We define the diameter of \( G_{m,n,k} \) (in symbols \( \text{diam}(G_{m,n,k}) \)) to be the graph diameter of \( \Gamma(G_{m,n,k}, \{x, x^{-1}, y, y^{-1}\}) \).

The diameter of finite groups and their bounds have been widely studied, especially from the viewpoint of efficient communication networks (see [1, 2] and the references therein). In particular, the networks arising from the Cayley graphs of groups in the subfamily \( \{G_{c,k,c\ell,c\ell+1}\} \), also known in computer science parlance as super-toroids, have been extensively analyzed [11, 13]. For example, in [5, 6], it was shown that for \( c \geq 8 \), \( \text{diam}(G_{c,k,c\ell,c\ell+1}) = [ck/2] + [c\ell/2] \). However, to our knowledge, the diameter bounds for arbitrary groups in \( \{G_{m,n,k}\} \) have not been studied.

This problem also has connections with the well known degree-diameter problem pertaining to this family of graphs (see [7, 9, 12]). This is the main motivation behind undertaking such an analysis in this paper.

Every element of \( g \in G_{m,n,k} \) has the unique expression as \( g = x^ay^b \). A path \( P \) from 1 to an element \( g \in G_{m,n,k} \) would take the form \( g = \prod_{i=1}^{t} x^{a_i}y^{b_i} \). Such a path is said to be reduced if \( a_i \not\equiv 0 \pmod{m} \), for \( 2 \leq i \leq t \), and \( b_i \not\equiv 0 \pmod{n} \), for \( 1 \leq i \leq t - 1 \). We define \( t \) to be the syllable of the reduced path \( P \) (as above), and \( \sum_{i=1}^{t} |a_i| + |b_i| \) to be its length \( l(P) \). Denoting by \( \mathcal{P}_g \), the collection of all reduced paths in \( G \) from 1 to \( g \), we have \( \|x^ay^b\| = \min_{P \in \mathcal{P}_g} \{l(P) : P \in \mathcal{P}_g\} \), where \( \| \| \) is the usual word norm in \( G_{m,n,k} \). Thus, the diameter of \( G_{m,n,k} \) is given by

\[
\text{diam}(G_{m,n,k}) = \max \{\|x^ay^b\| : 0 \leq a \leq m - 1, 0 \leq b \leq n - 1\}.
\]

It is apparent that \( [m/2] \leq \text{diam}(G_{m,n,k}) \leq [m/2] + [n/2] \). In reality, \( \text{diam}(G_{m,n,k}) = [m/2] + \delta \), where \( \delta \) is significantly smaller than \( [n/2] \). For example, we can show that \( \text{diam}(G_{60,61,2}) = 31 \) (see Section 5). In order to obtain a better bound for \( \text{diam}(G_{m,n,k}) \), we begin by noting that

\[
\prod_{i=1}^{t} x^{a_i}y^{b_i} = x^{a_1 + \ldots + a_t}y^{b_1k^{a_2 + \ldots + a_t} + \ldots + b_{t-1}k^{a_t} + b_t}.
\]

Key words and phrases. Split metacyclic groups; Diameter; Finite rings; Finite fields.
Consequently, the problem of computing \( \|x^a y^b\| \) reduces to the following nonlinear optimization problem in the pair of rings \((\mathbb{Z}_m, \mathbb{Z}_n)\):

\[
\begin{align*}
\text{minimize} & \quad \sum_{i=1}^{t} |a_i| + |b_i| \quad (\text{in } \mathbb{Z}), \\
\text{subject to} & \quad a_1 + \ldots + a_t \equiv a \quad (\text{mod } m), \\
& \quad b_1 k^{a_2 + \ldots + a_t} + \ldots + b_{t-1} k^{a_t} + b_t \equiv b \quad (\text{mod } n).
\end{align*}
\]

Fix a positive integer \( n \geq 3 \), and consider a unit \( k \in \mathbb{Z}_n^\times \) of multiplicative order \( \text{ord}(k) = \alpha \geq 2 \). For \( 0 \leq i \leq \alpha - 1 \) and an integer \( 1 \leq \lambda \leq [n/2] \), a \( k \)-interval is a set of the form \( A(\lambda, i) = \{ak^j : -\lambda \leq a \leq \lambda\} \). We further reduce the problem of solving (†) to the problem of determining the least positive integer \( \lambda = \lambda_0 + \ldots + \lambda_{\alpha-1} \) so that

\[ \mathbb{Z}_n = \bigoplus_{i=0}^{\alpha-1} A(\lambda_i, i). \]

We will call this the problem of covering the ring \( \mathbb{Z}_n \) by sum sets of \( k \)-intervals. By showing that the solution to this covering problem in \( \mathbb{Z}_n \) depends on two parameters, namely \( \text{wt}(n, k; \alpha) \) and \( \deg(n, k; \alpha) \) (Section 2.4), we obtain our main result (Theorem 4.4), which gives a bound for \( \text{diam}(G_{m,n,k}) \).

**Theorem 1** (Main theorem). Let \( G_{m,n,k} \) be the split metacyclic group given by the presentation

\[ G_{m,n,k} = \langle x, y : x^n = 1 = y^m, xy^{-1}yx = y^k \rangle, \]

where \( k \) has order \( \alpha \) in the group \( \mathbb{Z}_n^\times \) of units. If \( \alpha \) is even and \( k^{\alpha/2} \equiv -1 \pmod{n} \), then

\[ \text{diam}(G_{m,n,k}) \leq \begin{cases} \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha), & \text{if } \alpha \neq m, \\ \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha) + \deg(n, k; \alpha), & \text{if } \alpha = m. \end{cases} \]

Based on our observations, we believe that \( \text{diam}(G_{m,n,k}) \leq \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha) \) should hold true, irrespective of the conditions on \( m, n, k, \) and \( \alpha \). As a direct application of our main result, we obtain an upper bound for the diameter of an arbitrary metacyclic group (Corollary 4.5).

In practice, it is difficult to compute \( \text{wt}(n, k; \alpha) \), or provide a reasonable upper bound for it. Nevertheless, we show that for an odd prime \( p \), the growth of \( \text{wt}(p^n, k; \alpha) \) is at most linear in \( n \) (Corollary 3.7).

**Theorem 2.** Let \( p \) be an odd prime and \( k \in \mathbb{Z}_p^\times \) with \( \text{ord}(k) = p^{n-1}(p-1) \). Denote \( \text{wt}(p, s; p-1) \) by \( \text{wt}(p) \), where \( s \) is the image of \( k \) under the natural surjection \( \mathbb{Z}_p^n \to \mathbb{Z}_p \). Then,

\[ \text{wt}(p) \leq \text{wt}(p^n, k; p^{n-1}(p-1)) \leq 2n \text{wt}(p). \]

A similar bound is obtained for the case when \( p = 2 \). Finally, we derive an upper bound of \( \text{wt}(p) \), when \( p \) is an odd prime (Theorem 3.1).

**Theorem 3.** Let \( p \) be an odd prime, and let \( s \in \mathbb{Z}_p^\times \) with \( \text{ord}(s) = p-1 \). Then,

\[ \text{wt}(p) \leq \begin{cases} \frac{n-1}{p-1} & \text{if } p \equiv 1 \pmod{4}, \\ \frac{n-5}{p-5} & \text{if } p \equiv 3 \pmod{4}. \end{cases} \]

2. Some combinatorics pertaining to the covering problem in \( \mathbb{Z}_n \)

We will now introduce some formal notations to make the problem of covering of \( \mathbb{Z}_n \) more precise. Fix a positive integer \( n \geq 3 \), and consider a unit \( k \in \mathbb{Z}_n^\times \) of multiplicative order \( \text{ord}(k) = \alpha \geq 2 \).
Definition 2.1. Given a pair, \( \mathbf{i} = (i_1, i_2, \ldots, i_r) \) and \( \mathbf{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_r) \), of sequences of integers such that
\[
\alpha - 1 \geq i_1 > i_2 > \ldots > i_r \geq 0 \quad \text{and} \quad \lambda_j \geq 0, \quad \text{for } 1 \leq j \leq r,
\]
we define
\[
\Omega(\mathbf{i}, \mathbf{\lambda}) = \{ b_1 k^{i_1} + \ldots + b_r k^{i_r} \pmod{n} : |b_i| \leq \lambda_i, 1 \leq i \leq r \}.
\]
Sometimes we write \( \Omega(\mathbf{i}, \mathbf{\lambda}) \) as \( \Omega(k(\mathbf{i}, \mathbf{\lambda})) \), where \( k(\mathbf{i}) = (k^{i_1}, \ldots, k^{i_r}) \). We will refer to \( i_1 \) as the degree, and the smallest nonzero number among the \( i_k \), for \( 1 \leq k \leq r \) will be called the co-degree of the sequence \( \mathbf{i} \), which we denote by \( \deg(\mathbf{i}) \) and \( \text{codeg}(\mathbf{i}) \), respectively. The integer \( r \geq 1 \) will be referred as the length of \( \mathbf{i} \).

Since \( k \in \mathbb{Z}_n^\times \), we have \( k\mathbb{Z}_n = \mathbb{Z}_n \), and so for each sequence \( \mathbf{i} \) there exists a finite sequence \( \mathbf{\lambda} \pmod{n} \) such that \( \Omega(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \). This leads us to the following definition.

Definition 2.2. Given a pair, \( \mathbf{i} \) and \( \mathbf{\lambda} \) of sequences as in Definition 2.1, we define:

(i) The weight of \( \Omega = \Omega(\mathbf{i}, \mathbf{\lambda}) \) as
\[
\text{wt}(\Omega) := \lambda_1 + \lambda_2 + \ldots + \lambda_r.
\]

(ii) The weight of \( (n,k) \) with respect \( \mathbf{i} \) as
\[
\text{wt}(n,k;\mathbf{i}) := \min \{ \text{wt}(\Omega(\mathbf{i}, \mathbf{\lambda})) : \Omega(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \}.
\]

(iii) The weight of \( (n,k) \) of level \( r \) as
\[
\text{wt}(n,k;r) := \min \{ \text{wt}(n,k;\mathbf{i}) : \alpha - 1 \geq i_1 > i_2 > \ldots > i_r \geq 0 \}.
\]

Remark 2.3. From the definition of \( \text{wt}(n,k;\alpha) \), it is clear that \( \text{wt}(n,k;\alpha) = \text{wt}(n,k';\alpha) \) whenever \( k \) and \( k' \) generate the same cyclic subgroup of \( \mathbb{Z}_n^\times \).

In our calculations, we will require sequences \( \mathbf{i} \) with \( i_r = 0 \), which we call reduced sequences.

Definition 2.4. Given a sequence \( \mathbf{i} \) as in Definition 2.1, the complement of \( \mathbf{i} \) is the sequence \( I(\mathbf{i}) = (j_1, \ldots, j_r) \) defined by
\[
\alpha - 1 \geq j_1 = \alpha - (i_1 - i_2) > j_2 = \alpha - (i_1 - i_3) > \ldots > j_{r-1} = \alpha - (i_1 - i_r) > j_r = 0.
\]

In the following proposition, we show that \( I(\mathbf{i}) \) is a reduced sequence of length \( r \) having the same weight as \( \mathbf{i} \).

Proposition 2.5. Consider sequences \( \mathbf{i} \) and \( \mathbf{\lambda} \) as in Definition 2.1. If \( \Omega(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \), then

(i) \( \Omega(I(\mathbf{i}), \mathbf{\lambda}') = \mathbb{Z}_n \), where \( \mathbf{\lambda}' = (\lambda_2, \lambda_3, \ldots, \lambda_r, \lambda_1) \), and

(ii) \( \text{wt}(n,k;I(\mathbf{i})) = \text{wt}(n,k;I(\mathbf{i}, \mathbf{\lambda})). \)

Proof. Given any \( b \pmod{n} \), there exists \( b_1, \ldots, b_r \) such that \( |b_i| \leq \lambda_i \), for \( 1 \leq s \leq r \), and \( b = b_1 k^{i_1} + b_2 k^{i_2} + \ldots + b_{r-1} k^{i_{r-1}} + b_r k^{i_r} \). So, we have
\[
b k^{\alpha - i_1} = b_1 + b_2 k^{\alpha - (i_1 - i_2)} + \ldots + b_r k^{\alpha - (i_1 - i_r)} \in \Omega(I(\mathbf{i}, \mathbf{\lambda})).
\]
Hence, \( k^{\alpha - i_1} \Omega(I(\mathbf{i}, \mathbf{\lambda}) \subseteq \Omega(I(\mathbf{i}), \mathbf{\lambda}') \), and as \( k \) is a unit, we have \( k^{\alpha - i_1} \Omega(I(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \), which establishes (i).

For (ii), note that if \( \text{wt}(n,k;\mathbf{i}) = \lambda \), then \( \Omega(I(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \), for some sequence \( \mathbf{\lambda}' = (\lambda_2, \lambda_3, \ldots, \lambda_r, \lambda_1) \) with \( \lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_r \) being the least possible value. As seen above, we have \( \Omega(I(\mathbf{i}, \mathbf{\lambda}) = \mathbb{Z}_n \), and furthermore \( \mathbf{\lambda}' = (\lambda_2, \lambda_3, \ldots, \lambda_r, \lambda_1) \) yields the same weight \( \lambda \). Thus, we have \( \text{wt}(n,k;I(\mathbf{i}, \mathbf{\lambda})) = \text{wt}(n,k;\mathbf{i}) \).

Suppose that \( \mu = \text{wt}(n,k;I(\mathbf{i})) < \text{wt}(n,k;\mathbf{i}) \). Then there exists a sequence \( \mathbf{\mu} = (\mu_2, \ldots, \mu_r, \mu_1) \) such that \( \Omega(I(\mathbf{i}), \mathbf{\mu}) = \mathbb{Z}_n \). Multiplying by \( k^i \), we get \( \Omega(I(\mathbf{i}), \mathbf{\mu}') = \mathbb{Z}_n \), where \( \mathbf{\mu}' = (\mu_1, \mu_2, \ldots, \mu_r) \). As this contradicts the minimality of \( \text{wt}(n,k;I(\mathbf{i})) = \lambda \), (iii) follows. \( \square \)
Lemma 2.6 implies that it suffices to consider only reduced sequences while computing \( wt(n, k; r) \).

**Remark 2.6.** For any length \( r \leq \alpha \), we can see that \( wt(n, k; r) \leq \lfloor n/2 \rfloor \), by considering the sequence \( \lambda = (\lambda_1, \ldots, \lambda_r) \), where \( \lambda_i = \lfloor n/2 \rfloor \) for a fixed \( i \), and \( \lambda_j = 0 \), for the indices \( j \neq i \).

**Definition 2.7.** Given a sequence \( \bar{\lambda}: \alpha - 1 \geq i_1 > i_2 > \ldots > i_r \geq 0 \), a sequence \( \bar{j} = \alpha - 1 \geq j_1 > j_2 > \ldots > j_q \geq 0 \) of length \( q \geq r \) is said to be **finer than** \( \bar{\lambda} \) (in symbols \( \bar{\lambda} \preceq \bar{j} \)), if it is obtained from \( \bar{\lambda} \) by adding one or more terms.

**Remark 2.8.** Let \( P(\alpha - 1) \) denote the collection of all sequences of length \( \leq \alpha \) as in Definition 2.1, and let \( P'(\alpha - 1) \) be the subcollection of all reduced sequences. Note that \( \preceq \) defines a partial order on \( P(\alpha - 1) \) under which \( P'(\alpha - 1) \) is a subposet of \( P(\alpha - 1) \).

**Proposition 2.9.** Consider the posets \( (P(\alpha - 1), \preceq) \) and \( (P'(\alpha - 1), \preceq) \) as in Remark 2.8. Then:

(i) For any two elements \( \bar{i}, \bar{j} \in P(\alpha - 1) \) (resp. \( P'(\alpha - 1) \)), there exists \( \xi \in P(\alpha - 1) \) (resp. \( P'(\alpha - 1) \)) such that \( \bar{i} \preceq \xi \) and \( \bar{j} \preceq \xi \).

(ii) \( (P'(\alpha - 1), \preceq) \) has a maximal element \( \Delta \), and a minimal element \( \delta \) given by

\[
\Delta = (\alpha - 1, \alpha - 2, \ldots, 1, 0), \quad \delta = (\alpha - 1, 0)
\]

of lengths are \( \alpha \) and 2, respectively.

(iii) The map \( \Psi : (P(\alpha - 1), \preceq) \to (\mathbb{N}, \leq) \) defined by

\[
\Psi(\bar{i}) := wt(n, k; \bar{i})
\]

is an order reversing function, where \( (\mathbb{N}, \leq) \) is regarded as a linearly ordered poset with respect to natural order.

**Proof.** Given sequences \( \bar{i}, \bar{j} \in P(\alpha - 1) \) (resp. \( P'(\alpha - 1) \)), consider the sequence \( \bar{\lambda} \) obtained by taking the union of elements in \( \bar{i} \) and \( \bar{j} \), rearranged in decreasing order. Then, clearly \( \bar{i} \preceq \bar{\lambda} \preceq \bar{j} \), from which (i) and (ii) follow.

For showing (iii), consider sequences \( \bar{i} \preceq \bar{j} \) with lengths \( r < s \) such that \( wt(n, k; \bar{i}) = \lambda \) is realized by a sequence \( \Delta = (\lambda_1, \lambda_2, \ldots, \lambda_r) \). Define \( \mu = (\mu_1, \ldots, \mu_s) \) by \( \mu_i = \lambda_i \), if \( j_i \) is an element in \( \bar{i} \), and \( \mu_i = 0 \) otherwise. Then \( \lambda = \mu_1 + \ldots + \mu_s \) and \( \Omega(\bar{j}, \bar{\mu}) = \mathbb{Z}_n \). Hence, we have that \( wt(n, k; \bar{j}) \leq \lambda = wt(n, k; \bar{\lambda}) \), and (iii) follows.

**Remark 2.10.** Clearly, \( wt(n, k; \delta) = \lfloor n/2 \rfloor \), and the only sequence of length \( \alpha \) is the maximal element \( \Delta \). Thus, \( wt(n, k; \Delta) = wt(n, k; \alpha) \), which shows the importance of analyzing \( wt(n, k; \Delta) \).

**Definition 2.11.** A sequence \( \bar{i} \in P'(\alpha - 1) \) is called a **minimal prime sequence realizing** \( wt(n, k; \alpha) \) if:

(i) \( \bar{i} \in S(\alpha) = \{ \bar{i} \in P'(\alpha - 1) : wt(n, k; \bar{i}) = wt(n, k; \alpha) \} \), and

(ii) \( \text{length}(\bar{i}) = \min \{ \text{length}(\bar{j}) : \bar{j} \in S(\alpha) \} \)

We denote the smallest possible degree of a minimal prime sequence realizing \( wt(n, k; \alpha) \) by \( \text{deg}(n, k; \alpha) \).

**Example 2.12.** When \((n, k) = (30, 7)\), \( \text{ord}(7) = 4 \in \mathbb{Z}_{30}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \). We consider the sequences \( \bar{i}_1 : 1, 0, \bar{i}_2 : 2, 0, \) and \( \bar{i}_3 : 3, 0 \). For each sequence \( \bar{i}_k \), in Table 1 below, we list some possible choices of a sequence \( \Delta : \lambda_1, \lambda_2 \) (as in Definition 2.11), and the values of \( wt(\Omega(\bar{i}_k; \Delta)) \).
A direct calculation (using software written for Mathematica 11) shows that \( wt(30, 7; 4) = 5 \). Hence, \( i_1 \) and \( i_3 \) are minimal prime sequences that realize this weight, and \( S(4) = \{(3, 0), (1, 0)\} \).

This example shows that in practice it is difficult to compute \( wt(n, k; \alpha) \) in most situations. However, we will now obtain reasonable bounds on \( wt(n, k; \alpha) \) in case \( n \) is a prime power.

### 3. Bounds on the weight of a prime power

It is well known that when \( p \) is an odd prime, for \( n \geq 1 \), we have \( \mathbb{Z}_{p^n}^\times \cong \mathbb{Z}_{p^n-1}(p-1) \), and for \( n \geq 2 \), we have \( \mathbb{Z}_{p^n}^\times \cong \mathbb{Z}_p \times \mathbb{Z}_{2n-2} \). For \( n \geq 2 \), let \( \varphi_n \) denote the natural quotient ring homomorphism \( \mathbb{Z}_{p^n}^\times \rightarrow \mathbb{Z}_{p^n-1}^\times \). If \( k \in \mathbb{Z}_{p^n}^\times \) has order \( p^n-1(p-1) \), then \( \varphi_n(k) \) generates the cyclic group \( \mathbb{Z}_{p^n-1}^\times \). Denoting the epimorphism \( \varphi_n|_{\mathbb{Z}_{p^n}^\times} \) by \( \tilde{\varphi}_n \), for an arbitrary unit \( k \in \mathbb{Z}_{p^n}^\times \), we have

\[
\text{ord}(\tilde{\varphi}_n(k)) = \begin{cases} \text{ord}(k)/p, & \text{if } p \mid \text{ord}(k), \\ \text{ord}(k), & \text{otherwise.} \end{cases}
\]

When \( n \geq 1 \), we derive bounds for \( wt(p^n, k; \text{ord}(k)) \) in terms of the \( wt(p^n, \tilde{\varphi}_n(k); \text{ord}(\tilde{\varphi}_n(k))) \). We first consider the case when \( n = 1 \).

**Theorem 3.1.** Let \( p \) be an odd prime, and let \( s \in \mathbb{Z}_{p}^\times \) with \( \text{ord}(s) = p-1 \).

(i) If \( p \equiv 1 \pmod{4} \), then \( \text{wt}(p, s; p-1) \leq \frac{p+3}{4} \). Moreover, there exists a sequence \( i \) such that \( \text{deg}(i) = \frac{p-1}{4} \) and \( \text{wt}(p, s; i) \leq \frac{p+3}{4} \).

(ii) If \( p \equiv 3 \pmod{4} \), then \( \text{wt}(p, s; p-1) \leq \frac{p+3}{4} \). Moreover, there exists a sequence \( i \) such that \( \text{deg}(i) = \frac{p-3}{4} \) and \( \text{wt}(p, s; i) \leq \frac{p+3}{4} \).

**Proof.** We present a proof only for (i), as (ii) will follow from similar arguments. Consider the list of units \( A = \{s^i, s^{-1}, \ldots, s, 1\} \), where \( i_1 = \frac{p-1}{4} - 1 \). Since
would yield the bound \( \wt(p, s) \) in the proof of Theorem 3.1. However, this

Remark 3.2. Note that the only difficulty in the proof of Theorem 3.1 was to
represent \( s^\tau = -2 \not\in A \cup -A \). But this situation does not arise when \( 2 \not\in A \cup -A \),
in which case we have \( \lambda = (1, \ldots, 1) \), and we obtain the following slightly improved

bound

\[
\wt(p, s; p - 1) \leq \begin{cases} 
\frac{p - 1}{4}, & \text{if } p \equiv 1 \pmod{4}, \\
\frac{p + 1}{2}, & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

Remark 3.3. One might also consider applying a generalization of the Cauchy-
Davenport theorem ([10, Theorem 2.3]) in the proof of Theorem 3.1. However, this
would yield the bound \( \wt(p, s; p - 1) \leq \frac{p - 1}{2} \), which is significantly weaker than the
one we have derived.

Definition 3.4. For a prime \( p \) and \( s \in \mathbb{Z}_p^* \) with \( \ord(s) = p - 1 \) we define

\[
\wt(p) := \wt(p, s; p - 1)
\]

From the discussion after definition 2.2 it follows that \( \wt(p) \) does not depend on
the choice of \( s \).

Theorem 3.5 (An upper bound). For a fixed prime \( p \) and \( n > 1 \), consider \( k \in \mathbb{Z}_{p^n}^* \)
with \( \ord(k) = m \), and \( k_0 = \tilde{\varphi}(k) \in \mathbb{Z}_{p^{n-1}}^* \) with \( \ord(k_0) = m_0 \). Then,

\[
\wt(p^n, k; m) = \begin{cases} 
\wt(p^{n-1}, k_0; m_0) + 2\wt(p), & \text{if } p \mid m, \text{ and} \\
\wt(p^{n-1}, k_0; m_0) + [p/2], & \text{if } p \not\mid m.
\end{cases}
\]

Proof. First note that while \( p = 2 \), we must have \( 2 \nmid m \) and hence these are the only cases. Let \( \lambda' = \wt(p^{n-1}, \tilde{\varphi}(k); m_0) \) be realized by a sequence \( \lambda_{m_0}^{n-1} \), such that every \( a' \in \mathbb{Z}_{p^{n-1}}^* \) is expressed as

\[
a' \equiv b'_1 \tilde{\varphi}(k)^{m_0 - 1} + b'_2 \tilde{\varphi}(k)^{m_0 - 2} + \ldots + b'_{m_0 - 1} \tilde{\varphi}(k) + b'_{m_0} \pmod{p^{n-1}}
\]

for integers \( b'_j \) with \( |b'_j| \leq \lambda'_{n-1} \). Then every \( a \in \mathbb{Z}_{p^n}^* \) can be expressed as

\[
a \equiv b'_1 k^{m_0 - 1} + b'_2 k^{m_0 - 2} + \ldots + b'_{m_0 - 1} k + b'_{m_0} + z_a \pmod{p^n},
\]

with \( |b'_j| \leq \lambda'_{n-1} \), and \( z_a \in \ker(\varphi_n) \), which depends on \( a \). Note that

\[
\ker(\varphi_n) = \{ \xi^{p - 1} : 0 \leq \xi \leq p - 1 \} \quad \text{and} \quad \ker(\tilde{\varphi}_n) = \ker(\varphi_n) = \langle k \rangle = \mathbb{Z}_{p^n}^*.
\]

If \( p \nmid m \), then we have \( m_0 = m/p \), and so

\[
\ker(\varphi_n) = \{ k^{m_0 - 1} : 0 \leq \tau \leq p - 1 \}.
\]
Corollary 3.7. The following is a direct consequence of Theorem 3.1.

where \(|\xi\rangle\) and that \(Z\) such that \(|\xi\rangle\) have that \(\ker(\varphi)\equiv 1\) (mod \(p^n\))

So, we have a bijection \(\ker(\varphi_n)\) onto itself given by

\[\theta_p^{n-1} \rightarrow k^{s_m} - 1\] whenever \(k^{r_m} - 1 \rightarrow \theta_p^{n-1}\),

satisfying \(i_0 = 0\) and \(\theta_0 = 0\). Now following the notations in Theorem 3.1 fix \(s \in \mathbb{Z}_p^\times\) of order \(p - 1\), and let \(\wt(p) = \wt(\Omega(\mu)) = \mu\), where \(\mu = (\mu_1, \ldots, \mu_p)\) and \(\hat{i} = (p - 1, 1, 0)\). Using Theorem 3.1, any \(\theta_p^{n-1} \in \ker(\varphi_n)\) is represented as

\[\theta_p^{n-1} \equiv c_1 s_p^{n-1} + \ldots + c_p s_p^{n-1} + c_p p^{n-1} \pmod{p^n}\]

\[\equiv c_1 (k_i^{s_m} - 1) + \ldots + c_p (k_i^{s_m} - 1) + c_p (k_i^{s_m} - 1) \pmod{p^n}\]

\[\equiv c_1 k^{s_m} + \ldots + c_p k^{s_m} + c_p k^{s_m} - (c_1 + \ldots + c_p) k^{s_m} \pmod{p^n},\]

where \(|c_i| \leq \mu_i\). By considering an appropriate rearrangement of the following sequences

\[k(i) = (k_i^{s_m}, k_i^{s_m}, k_i^{s_m}, k_i^{s_m} - 1, k_{m-2}, \ldots, k, 1)\]

\[m'(i) = (\mu_1, \ldots, \mu_p, \lambda_1, \ldots, \lambda_{m-1}, \lambda_m + 1, \ldots, \mu_p),\]

where \(m'(i)\) is the sequence of the exponents, we obtain sequences, \(m'\) an \(m''\), respectively, such that \(Z_p = \Omega(\lambda, m'')\). This proves the first inequality.

If \(p \nmid m\), then \(m = m_0\), and so \(p\) must be odd. From the discussion above, there exists \(\xi \in \mathbb{Z}_p\) so that

\[\frac{p^{n-1} - 1}{2} \equiv b'p^{m-1} + b'p^{m-2} + \ldots + b'p^{m-1} \equiv \xi p^{n-1} \pmod{p^n},\]

which implies that

\[(-2 \xi + 1)p^{n-1} \equiv 2b'p^{m-1} + 2b'p^{m-2} + \ldots + b'p^{m-1} + 2b'p^{m-1} \equiv 2b'p^{m-1} + 1 \pmod{p^n}\]

and that \(\xi p^{n-1} := (-2 \xi + 1)p^{n-1}\) is a non-trivial element of \(\ker(\varphi_n)\). Hence, we have that \(\ker(\varphi_n) = \{\tau \xi p^{n-1} : -[p/2] \leq \tau \leq [p/2]\}\). Now setting

\[\hat{i} = (m_0 - 1, 1, 0)\]

\[m' = (2[p/2] + 1, 2[p/2] + 1)\lambda'_{m-1} + (2[p/2] + 1)\lambda'_{m} + [p/2]\]

we see that \(Z_p = \Omega(\hat{i}, m'')\), which proves the second inequality.

Using arguments similar to the ones used in the second half of the proof of Theorem 3.1 we obtain the following corollary.

Corollary 3.6. For a fixed odd prime \(p\) and \(n > 1\), consider \(k \in \mathbb{Z}_p^\times\), with \(ord(k) = m\), and \(k_0 = \varphi_n(k) \in \mathbb{Z}_p^\times\), with \(ord(k_0) = m_0\). Assuming that \(p \nmid m\), for each \(\xi p^{n-1} \in \ker(\varphi_n)\), let \(\mu_\xi\) denote the minimum of all sums \(\mu_1 + \ldots + \mu_\xi m_0\) so that

\[\xi p^{n-1} \equiv b'p^{m-1} + b'p^{m-2} + \ldots + b'p^{m-1} + b'p^{m} \pmod{p^n},\]

where \(|b'| \leq \mu_j\). Then

\[\wt(p^n, k; m) \leq [p/2](2\mu_0 + 1) + \wt(p^{n-1}, k_0; \mu_0),\]

where \(\mu_0 = \min\{\mu_\xi : 1 \leq \xi \leq p - 1\}.

The following is a direct consequence of Theorem 3.1

Corollary 3.7. Let \(p\) be a prime.

(i) If \(p\) is odd and \(k \in \mathbb{Z}_p^\times\), with \(ord(k) = p^{n-1}(p - 1)\), then

\[\wt(p) \leq \wt(p^n, k; p^{n-1}(p - 1)) \leq 2\nu(\mu),\]

where \(\nu(\mu) = +1, if \mu \equiv 1 \pmod{4}, and is -1, otherwise.
(ii) If \( p = 2, \ n \geq 4, \) and \( k \in \mathbb{Z}_2^n \) with \( \text{ord}(k) = 2^n - 2 \), then
\[
\gamma(k) \leq \text{wt}(2^n, k; 2^n - 2) \leq \gamma(k) + 2(n - 1),
\]
where \( \gamma(k) = 4, \) if \( k^{2^n - 3} \equiv -1 \pmod{2^n} \), and is 2, otherwise.

Based on our observations, we believe that the following conjectures have to hold true. However, this will require much deeper combinatorics to establish them.

**Conjecture 1.** Let \( p \) be an odd prime. Then there exists a constant \( C(p) \approx 1 \) such that
\[
\text{wt}(p) \leq C(p) \log_2(p).
\]

**Conjecture 2.** Let \( p \) be an odd prime and \( n > 1 \). Let \( \varphi_n : \mathbb{Z}_{p^n}^* \rightarrow \mathbb{Z}_{p^n-1}^* \) denote the natural surjective morphism. Suppose \( k \in \mathbb{Z}_{p^n}^* \) with \( \text{ord}(k) = pn_0 \), and \( k_0 = \varphi_n(k) \in \mathbb{Z}_{p^n-1}^* \) with \( \text{ord}(k_0) = m_0 \). Then,
\[
\text{wt}(p^{n-1}, k_0; m_0) + \text{wt}(p - 1) \leq \text{wt}(p^n, k; pn_0) \leq \text{wt}(p^{n-1}, k_0; m_0) + \text{wt}(p).
\]

For a sequence \( \hat{i} \) realizing the weight corresponding to a unit of maximum order in \( \mathbb{Z}_{p^n}^* \), we have:
\[
\text{deg}(\hat{i}) \leq \begin{cases} \frac{p - 1}{2} + (n - 1)p - 1, & \text{if } p \equiv 1 \pmod{4}, \text{ and} \\ \frac{p - 3}{2} + (n - 1)p, & \text{if } p \equiv 3 \pmod{4} \end{cases}
\]
The final result in this section gives a bound on the degree of a minimal prime sequence realizing \( \text{wt}(n, k; \alpha) \), when \( \alpha \) is even and \( k^{\alpha/2} \equiv -1 \pmod{n} \).

**Proposition 3.8.** Let \( k \in \mathbb{Z}_n^* \) with \( \text{ord}(k) = \alpha > 1 \), where \( \alpha \) is even and \( k^{\alpha/2} \equiv -1 \pmod{n} \). Then \( \text{deg}(n, k; \alpha) \leq \alpha/2 \).

**Proof.** We know from Remark 2.10 that \( \text{wt}(n, k; \Delta) = \text{wt}(n, k; \alpha) \), where \( \Delta : \alpha - 1, \ldots, 1, 0 \). For this \( \Delta \), let \( \text{wt}(n, k; \alpha) \) be realized by a sequence \( \hat{\lambda} : \lambda_1, \ldots, \lambda_\alpha \), so that each element of \( \Omega(\hat{\lambda}) \) has a representation of the form
\[
b_1k^{\alpha-1} + b_2k^{\alpha-2} + \ldots + b_{\alpha-1}k + b_\alpha,
\]
where \( |b_j| \leq \lambda_j \). Replacing the powers \( k^j \), for \( \alpha - 1 \geq j > \alpha/2 \), in this representation by \(-k^{\alpha-j/2}\), we obtain an expression of the form
\[
(b_{\alpha/2+1} - b_1)k^{\alpha/2-1} + (b_{\alpha/2+2} - b_2)k^{\alpha/2-2} + \ldots + (b_{\alpha-1} - b_{\alpha-2})k + (b_\alpha - b_{\alpha/2}),
\]
which represents an element of \( \Omega(\hat{\lambda}') \), where \( \hat{\lambda}' : \alpha/2 - 1, \ldots, 1, 0 \) and \( \lambda' : \lambda_{\alpha/2+1} + \lambda_1, \ldots, \lambda_{\alpha-1} + \lambda_{\alpha/2} \). The result now follows from the definition of a minimal prime sequence realizing \( \text{wt}(n, k; \alpha) \). \( \square \)

4. Bounding the diameter of split metacyclic groups

There are two key steps involved in solving our main optimization problem (†). In the first step (first reduction), we restrict our optimization to the component ring \( \mathbb{Z}_n \). In the second step (second reduction), we build on the results of the first step towards arriving at a solution to (†). We fix the notation that \( k \in \mathbb{Z}_n^* \) with \( \text{ord}(k) = \alpha \), and regard the elements of \( \mathbb{Z}_n \) as formal sums
\[
w(\underline{b}, \underline{c}) = b_1k^{c_1} + b_2k^{c_2} + \ldots + b_\ell k^{c_\ell},
\]
where \( \underline{b} = (b_1, b_2, \ldots, b_\ell) \) and \( \underline{c} = (c_1, c_2, \ldots, c_\ell) \) are two arbitrary integer sequences. Further, we will abuse notation by using the same expression of \( \text{wt}(\underline{b}, \underline{c}) \) while treating the sum as an element of \( \mathbb{Z}_n \). The first reduction step (Proposition 1.2) will connect these to the sequences which we have introduced in Definition 2.1.
Definition 4.1. The formal sum $w(b, c)$ is called primal, if for any $c$ (mod $\alpha$), there is at most one non-zero entry among $b_t$ with $c_t \equiv c$ (mod $\alpha$). We call the number $|b_1| + |b_2| + \ldots + |b_1|$ as the absolute coefficient sum of $w(b, c)$, which we denote by $acs(w(b, c))$. The ordered sequence relative to $w(b, c)$ is defined to be $S(w(b, c)) = (i_1, \ldots, i_r)$ such that

$$\alpha - 1 \geq i_1 > \ldots > i_r \geq 0 \quad \text{and} \quad \{k^{c_1}, \ldots, k^{c_r}\} = \{k^{i_1}, \ldots, k^{i_r}\}.$$ 

For example, the sum $1.k^2 + 0.k^2 + 1.k + 1$ is primal, while $2.k^2 - 1.k^2 + 1.k + 1$ is not, and the ordered sequence related to both of them is $(2, 1, 0)$. Our first step of reduction process involves reducing the absolute coefficient sum of $w(b, c)$ without changing the value of $w(b, c)$ (mod $\alpha$), and the powers $k^{c_1}, k^{c_2}, \ldots, k^{c_r}$, while retaining their multiplicities. For example we want to reduce $2.k^2 - 1.k^2 + 1.k + 1$ to $1.k^2 + 0.k^2 + 1.k + 1$. Keeping the same powers of $k$ with zero coefficient in the reduction leads to the idea of connecting the main optimization problem to the problem of covering finite rings by powers of the same unit.

Proposition 4.2 (First reduction step). Consider the formal sum $w(b, c)$, and let $\bar{i} = (i_1, \ldots, i_r)$ be the (ordered) sequence with $\alpha - 1 \geq i_1 > \ldots > i_r \geq 0$ and

$$\{k^{c_1}, \ldots, k^{c_r}\} = \{k^{i_1}, \ldots, k^{i_r}\}.$$ 

Then there exists a sequence $\bar{b}' = (b'_1, b'_2, \ldots, b'_r)$ of integers such that

(i) $w(b'_1, c')$ is primal, as a formal element,
(ii) $w(b'_1, c') \equiv w(b, c)$ (mod $\alpha$),
(iii) $acs(w(b'_1, c')) \leq acs(w(b, c))$, and
(iv) $acs(w(b'_1, c')) \leq wt(n, k; \bar{i})$.

Proof. We first write

$$w(b, c) = b_1 k^{c_1} + b_2 k^{c_2} + \ldots + b_t k^{c_t} = s_1 k^{i_1} + s_2 k^{i_2} + \ldots + s_r k^{i_r},$$

where $\alpha - 1 \geq i_1 > i_2 > \ldots > i_r \geq 0$ with $r$ being the number of distinct powers of $k$ in the formal sum on the left, and $s_j = \sum_{c_t = j} (mod \alpha) b_t$. Then any sequence $b': b'_1, b'_2, \ldots, b'_r$ obtained by replacing exactly one of the elements in each collection $\{b_t : c_t \equiv i_j (mod \alpha)\}$ by $s_j$, and the remaining by 0 satisfies conditions (i) - (ii). We obtain (iii) by applying the triangle inequality to the expression for $s_j$. Finally, if $acs(w(b'_1, c')) > wt(n, k; \bar{i})$, then by definition of $wt(n, k; \bar{i})$, we may replace the sequence $s_1, \ldots, s_r$ by a sequence $s'_1, \ldots, s'_r$ so that

$$s_1 k^{i_1} + s_2 k^{i_2} + \ldots + s_r k^{i_r} \equiv s'_1 k^{i_1} + s'_2 k^{i_2} + \ldots + s'_r k^{i_r} (mod \alpha),$$

where $|s'_1| + \ldots + |s'_r| \leq wt(n, k; \bar{i}) < acs(w(b'_1, c'))$. Thus, replacing the terms $s_j$ by $s'_j$ and then reconstructing the sequence $\bar{b}'$ yields (iv). □

At this point we need to clarify the requirement of introducing the concept of formal sum. Let $M = x^n y^k \in G_{m,n,k}$ be connected to 1 by a fixed reduced path $P: x^{a_1} y^{b_1} x^{a_2} y^{b_2} \ldots x^{a_t} y^{b_t} = x^n y^k$.

Set $c_i := a_{i+1} + \ldots + a_t$, for $1 \leq i \leq t - 1$, and $c_t = 0$. The first reduction step essentially reduces the length of the path $l(P) = \sum_{i=1}^t |a_i| + |b_i|$ without changing $\sum_{i=1}^t |a_i|$. To do this we need to keep the recursive sequence $c_i$ intact, and this was the main outline of the proof above. Also, note that while $r = \alpha$ in the first reduction step, we have reduced to the case $acs(w(b'_1, c')) \leq wt(n, k; \alpha)$ since there is a unique (ordered) sequence of length $\alpha$ in terms of the powers of $k$. 


Now recall that the number $t$ is called the syllable of $P$ (which we denoted by $\text{syl}(P)$ in Section 1). Also, we denote the collection of all reduced paths from 1 to $g \in G_{m,n,k}$ by $\mathcal{P}_g$.

**Proposition 4.3** (Second reduction step). Let $P : \prod_{i=1}^{t} x^{a_i}y^{b_i}$ be a reduced path from 1 to an element $g = x^{a}y^{b} \in G_{m,n,k}$. Suppose that $r$ is the number of distinct terms in the formal element $w(lG) = \prod_{i=1}^{t} b_i k^{c_i}$.

(i) If $w(lG)$ is not primal as a formal element, then there is another $P' \in \mathcal{P}_g$ such that $l(P') \leq l(P)$.

(ii) If $\text{acs}(w(lG)) > \text{wt}(n, k; \xi)$ (where $\xi$ is as denoted in Proposition 4.2), then $P$ cannot be a shortest path in $\mathcal{P}_g$.

(iii) If $P \in \mathcal{P}_g$ is a path of shortest length, then $\text{syl}(P) \leq \text{ord}(k)$.

**Proof.** Parts (i)-(ii) follow directly from Proposition 4.2. For (iii), note that the length of the ordered sequence $S(w(lG))$ is $\leq \alpha$. Using Proposition 4.2, we reduce the path $P$ to $P'$ and combine the terms that are powers of $x$ (which does not change the length of the path $P'$).

Using the second reduction we may assume that $|b_1| + \ldots + |b_t| \leq \text{wt}(n, k; \alpha)$, which finally brings us to the main result in this paper.

**Theorem 4.4** (Main theorem). Let $G_{m,n,k}$ be the split metacyclic group given by the presentation

$$G_{m,n,k} = \langle x, y : x^m = 1 = y^n, x^{-1}yx = y^k \rangle,$$

where $k$ has order $\alpha$ in the group $\mathbb{Z}_n^\times$ of units. If $\alpha$ is even and $k^{\alpha/2} \equiv -1 \pmod{n}$, then

$$\text{diam}(G_{m,n,k}) \leq \begin{cases} \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha), & \text{if } \alpha \neq m, \\ \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha) + \text{deg}(n, k; \alpha), & \text{if } \alpha = m. \end{cases}$$

**Proof.** We wish to bound the length of a path from 1 to an element $g = x^{a}y^{b} \in G$. Set $i_1 = \deg(n, k; \alpha)$, and assume without loss of generality that $-\lfloor m/2 \rfloor \leq a \leq \lfloor m/2 \rfloor$. We break our argument into three cases.

Case 1: Assume that $i_1 \leq a \leq \lfloor m/2 \rfloor$. Let $\xi$ denote a minimal prime sequence with degree $i_1 = \deg(n, k; \alpha)$ given by

$$\alpha - 1 \geq i_1 > i_2 > \ldots > i_{t-1} > i_t = 0.$$

First, we express $b \in \mathbb{Z}_n$ as

$$b \equiv b_1 k^{i_1} + b_2 k^{i_2} + \ldots + b_{t-1} k^{i_{t-1}} + b_t \pmod{n},$$

with $\sum_{j=1}^{t} |b_j| \leq \text{wt}(n, k; \alpha)$. Take $\xi = a - i_1 \geq 0$, and consider the path

$$P : x^{\xi} y^{-b_1} x^{a-i_1} y^{b_2} x^{i_2 - i_1} y^{b_3} \ldots x^{a - i_{t-1}} y^{b_{t-1}} x^{i_t - i_{t-1}} y^{b_t}.$$

Clearly, $P \in \mathcal{P}_g$, and since every exponent of $x$ in $P$ is non-negative, we have

$$l(P) = (a - i_1) + (i_1 - i_2) + \ldots + (i_{t-2} - i_{t-1}) + i_{t-1} + \sum_{j=1}^{t} |b_j| \leq \lfloor m/2 \rfloor + \text{wt}(n, k; \alpha),$$

which proves the result for this case.

Case 2: Assume that $-\lfloor m/2 \rfloor \leq a \leq -i_1$. Note that for any path $P \in \mathcal{P}_g$, we have $P^{-1} \in \mathcal{P}_{g^{-1}}$ and $l(P) = l(P^{-1})$, where $P^{-1} = \prod_{i=1}^{t-1} y^{-b_i} x^{-a_{i-1}}$. Consider $b' \in \mathbb{Z}_n$ such that $y^{-b'} x^{-a} = x^{-a} y^{b'}$. Since the exponent $-a$ of $x$ satisfies the hypothesis of Case 1, the result for this case follows.
Case 3: Finally, assume that $-i_1 < a < i_1$. As in previous case, it suffices to assume that $0 < a < i_1$. Write $b$ as in Equation 1 above, set $\xi = a - i_1$, and consider a path $P'$ of the form in Equation 2. Clearly, $P' \in P_y$, and further note that every other exponent, except the first exponent of $x$ in $P'$ is non-negative. Hence, we have

\[ l(P) = -a + i_1 + (i_1 - i_2) + (i_2 - i_3) + \ldots + (i_{t-2} - i_{t-1}) + i_{t-1} = -a + 2i_1. \]

Applying Proposition 5.8, we get

\[ l(P) \leq [m/2] + i_1. \]

The result now follows from the fact that $\alpha \leq \left\{ \begin{array}{ll} [m/2], & \text{if } \alpha \text{ is a proper divisor of } m, \\ [m/2] + i_1, & \text{otherwise.} \end{array} \right.$

Note that the third case of Theorem 4.4 used the fact that $2i_1 \leq \alpha$. However, when $n$ is a prime $p \equiv 1 \pmod{4}$, we know that $2i_1 \leq \lceil \alpha/2 \rceil$, which leads to a better bound. More generally, we have the following:

Corollary 4.5. Let $G_{m,n,k}$ be the split metacyclic group given by the presentation

\[ G_{m,n,k} = \langle x, y : x^m = 1 = y^n, x^{-1}yx = y^k \rangle, \]

where $k$ has order $\alpha$ in the group $\mathbb{Z}_n^\times$ of units. If $\alpha$ is even with $k^{\alpha/2} \equiv -1 \pmod{n}$ and $2 \deg(n, k; \alpha) \leq [\alpha/2]$, then

\[ \text{diam}(G_{m,n,k}) \leq [m/2] + \text{wt}(n, k; \alpha). \]

The fact that every metacyclic group $G$ is a quotient of a split metacyclic group yields a bound for $\text{diam}(G)$.

Corollary 4.6. Let $G_{m_0,\ell,n,k}$ be an arbitrary metacyclic group given by the presentation

\[ G_{m_0,\ell,n,k} = \langle x, y : x^{m_0} = y^\ell, y^n = 1, x^{-1}yx = y^k \rangle, \]

where $k^{m_0} \equiv 1 \pmod{n}$, $n \mid \ell(k-1)$ and $\ell \mid n$. Then

\[ \text{diam}(G_{m_0,\ell,n,k}) \leq \text{diam}(G_{m_0n/\ell,n,k}) \leq \left[ \frac{m_0n/\ell}{2} \right] + \text{wt}(m_0n/\ell, k; m_0). \]

Proof. First, we note that the condition $\ell \mid n$ does not violate the generality of the above presentation (see [8, Lemma 2.1]). Clearly, there exists a natural surjection $G_{m_0n/\ell,n,k} \twoheadrightarrow G_{m_0,\ell,n,k}$, and the result follows. \hfill $\square$

5. Some explicit computations

When $n$ is a prime $p \equiv 1 \pmod{4}$ (resp. $\equiv 3 \pmod{4}$), we showed in Theorem 3.1 that $\text{wt}(p, k; p - 1) \leq \frac{p+1}{2}$ (resp. $\leq \frac{p+3}{2}$). Nevertheless, in practice (as we will see), the value of $\text{wt}(p, k; p - 1)$ is much less than these bounds.

In Tables 2 and 3 below, we list several computations of $\text{wt}(n, k; \alpha)$ for various primes $n$ and primitive units $k \in \mathbb{Z}_n^\times$. Further, for these values of $n$, we consider $m = n - 1$, and indicate how the values of the bound (derived in Corollary 4.5) compares with the actual values of $\text{diam}(G_{m,n,k})$. These computations were made using software written in Mathematica 11 [11].
Table 2. Values of wt(p, k; p − 1), for some primes p ≡ 1 (mod 4).

| (m, n, k) | wt(n, k; α) | \(\lambda\) realizing wt(n, k; α) | diam\(\left(G_{m,n,k}\right)\) | \([m/2] + \text{wt}(n, k; \alpha)\) |
|----------|-------------|----------------------------------|-------------------------------|-------------------------------|
| (12, 13, 2) | 3 | 1, 1, 1 | 7 | 9 |
| (16, 17, 3) | 3 | 0, 1, 1 | 9 | 11 |
| (28, 29, 2) | 4 | 0, 0, 0, 1, 1, 1 | 15 | 18 |
| (36, 37, 2) | 4 | 0, 0, 0, 1, 0, 1, 1 | 19 | 22 |
| (40, 41, 6) | 4 | 0, 0, 0, 0, 1, 0, 1, 1 | 21 | 24 |
| (52, 53, 2) | 4 | 0, 0, 0, 1, 1, 0, 0, 0, 0, 1 | 27 | 30 |
| (60, 61, 2) | 4 | 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1 | 31 | 34 |

Table 3. Values of wt(p, k; p − 1), for some primes p ≡ 3 (mod 4).

| (m, n, k) | wt(n, k; α) | \(\lambda\) realizing wt(n, k; α) | diam\(\left(G_{m,n,k}\right)\) | \([m/2] + \text{wt}(n, k; \alpha)\) |
|----------|-------------|----------------------------------|-------------------------------|-------------------------------|
| (6, 7, 3) | 2 | 0, 1, 1 | 4 | 5 |
| (10, 11, 2) | 3 | 0, 0, 1, 2 | 6 | 8 |
| (18, 19, 2) | 3 | 0, 1, 0, 0, 1, 1 | 10 | 12 |
| (22, 23, 5) | 3 | 1, 0, 0, 0, 0, 1, 1 | 12 | 14 |
| (30, 31, 3) | 4 | 0, 0, 0, 0, 0, 0, 1, 1, 2 | 16 | 19 |
| (42, 43, 3) | 4 | 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 2 | 22 | 25 |
| (46, 47, 5) | 4 | 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1 | 24 | 27 |
| (58, 59, 2) | 4 | 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1 | 30 | 33 |

References

[1] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky, and Á. Seress. On the diameter of finite groups. In 31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990), pages 857–865. IEEE Comput. Soc. Press, Los Alamitos, CA, 1990.

[2] Fan RK Chung. Diameters and eigenvalues. Journal of the American Mathematical Society, 2(2):187–196, 1989.

[3] Richard N Draper. A fast distributed routing algorithm for supertoroidal networks. Supercomputing Research Center, 1990.

[4] Richard N Draper. An overview of supertoroidal networks. In Proceedings of the third annual ACM symposium on Parallel algorithms and architectures, pages 95–102. ACM, 1991.

[5] Richard N Draper and Vance Faber. The diameter and mean diameter of supertoroidal networks. Supercomputing Research Center, 1990.

[6] Richard N Draper and Vance Faber. The diameter and average distance of supertoroidal networks. Journal of Parallel and Distributed Computing, 31(1):1–13, 1995.

[7] Grahame Erskine. Diameter 2 Cayley graphs of dihedral groups. Discrete Math., 338(6):1022–1024, 2015.

[8] C. E. Hempel. Metacyclic groups. Comm. Algebra, 28(8):3865–3897, 2000.

[9] Heather Macbeth, Jana ’Siagiová, and Jozef ’Sirá’ n. Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups. Discrete Math., 312(1):94–99, 2012.

[10] Melvyn B. Nathanson. Additive number theory, volume 165 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[11] Wolfram Research. Mathematica 11.0, 2016.

[12] Tomáš Vetřík. Abelian Cayley graphs of given degree and diameter 2 and 3. Graphs Combin., 30(6):1587–1591, 2014.

[13] Fen Lin Wu, S Lakshminarahan, and Sudarshan K. Dhall. Routing in a class of cayley graphs of semidirect products of finite groups. Journal of Parallel and distributed computing, 60(5):539–565, 2000.
