ON COVERS OF DIHEDRAL 2-GROUPS BY POWERFUL SUBGROUPS

RISTO ATANASOV, ADAM GREGORY, LUKE GUATELLI, AND ANDREW PENLAND

ABSTRACT. A finite p-group G is called *powerful* if either p is odd and $[G, G] \subseteq G^p$ or $p = 2$ and $[G, G] \subseteq G^4$. A *cover* for a group is a collection of subgroups whose union is equal to the entire group. We will discuss covers of p-groups by powerful subgroups. The size of the smallest cover of a p-group by powerful subgroups is called the *powerful covering number*. Our focus in this paper is to determine the powerful subgroup covering number of the Dihedral 2-groups.

1. INTRODUCTION

If G is a group, a *cover* of G is a collection of proper subgroups whose union is equal to G, and the *covering number* of G is the minimal number of proper subgroups that occur in any cover of G. We write $\sigma(G)$ for the covering number of G.

A finite p-group H is called *powerful* if either p is odd and $[H, H] \subseteq H^p$ or $p = 2$ and $[H, H] \subseteq H^4$. If G is a p-group, we define a *powerful cover* of G to be a covering of G by powerful subgroups. We define the *powerful covering number* of G to be the minimal number of subgroups in any powerful covering of G. Our main result in this paper is to establish the powerful covering number of the dihedral 2-groups.

Powerful groups were first introduced by Lubotzky and Mann [**?**], who later used them to provide a characterization of p-adic analytic groups [**?**]. Powerful groups have played an important role in the theory of p-groups since their introduction. Notably, powerful groups served an important role in the classification of finite p-groups by a property known as *coclass*, introduced by Leedham-Green and Newman in [**?**](see [**?**] for an overview of conjectures and their proofs).

Interest in coverings and covering numbers goes back to G.A. Miller, who considered covers by subgroups with pairwise trivial intersection [**?**]. Such a cover is known as a *partition.* reference and culminating in a theorem which completely classifies all finite groups with a partition. todo: references see `https://projecteuclid.org/download/pdf_1/euclid.ijm/1258488174` todo: Partition Numbers by Foguel

Scorza todo:reference, who first noted that there is no group with $\sigma(G) = 2$. There has been a lot of interest in calculating the covering number for todo: more references for $\sigma(G)$ – Cohn, Tomkinson, etc.

Additionally, one may consider coverings in which all subgroups share some certain property. Bargava (todo: reference) classified the groups which have coverings by normal subgroups. todo: look also at `https://mathoverflow.net/questions/266368/normal-covering-number-and-maximal-cyclic-subgroups`

Foguel and Ragland (todo: reference) investigated coverings by abelian groups, all of which are pairwise isomorphic. Atanasov, Foguel, and Penland considered coverings by subgroups that all have the same order and have mutually isomorphic pairwise intersections.

2. BACKGROUND

In the interest of making this paper self-contained and accessible to non-experts, we will make very few assumptions about the reader's knowledge of group theory. This section reviews all definitions and well-known facts necessary to establish our results. Most of this material is standard and can be found in a standard text such as [**?**].

Throughout the rest of this work, all groups are assumed to be finite.

2.1. **Group Theory.** Let G be a group. If S is a subset of G, the *group generated by S* is the smallest subgroup of G that contains S. If T is a set, we write $|T|$ for the cardinality of T. A subgroup generated by a single element $g \in G$ is denoted $\langle g \rangle$ in an abuse of notation. Such a subgroup is called *cyclic* . For $g \in G$, the *order* of g is $|\langle g \rangle|$. For g, h in G, the *commutator of g and h* is defined as $g^{-1}h^{-1}gh$. The *commutator*

Date: November 2018.
Key words and phrases.

subgroup of G, denoted $[G, G]$, is the group generated by all commutators of all pairs of elements in G. Let p be a fixed prime number. We say that G is a p-group if every element in G has order equal to a power of p. The subgroup G^p is defined as

$$G^p = \langle \{g^p \mid g \in G\} \rangle.$$

A subgroup K of G is *maximal* if whenever there exists a subgroup $H \subseteq G$ such that K is a proper subgroup of H, it follows that $H = G$. If H is any subgroup of G, the *index* of H in G is equal to $\dfrac{|G|}{|H|}$. For a p-group, it is known that all maximal subgroups have index p. If T is a group, a homomorphism is a map $\alpha : G \to T$ such that $\alpha(gh) = \alpha(g)\alpha(h)$ for all $g, h \in G$. If T is a group and $\alpha : G \to T$ is a homomorphism, then the index of $\ker \alpha$ is equal to the size of the image of α.

If G_1 and H are groups, then the *direct product* $G_1 \times G_2$ is a group with the set $\{(g, h) \mid g \in G, h \in H\}$ and group operation given componentwise.

2.2. **Powerful Groups.**

2.3. **Group Covers.** If G is a group, the *covering number of* G is defined as the minimal number of subgroups needed to cover the group. We define the *powerful covering number of* G as the minimal number of proper powerful subgroups needed to cover the group. We define the *abelian covering number of* G as the minimal number of abelian powerful subgroups needed to cover the G. We write $\sigma(G)$ for the covering number, $\sigma_P(G)$ for the powerful covering number, and $\sigma_A(G)$ for the abelian covering number.

Lemma 2.1. *Let G be a finite noncyclic p-group. Then G has a powerful covering.*

Proof. G has a covering by the set of all cyclic subgroups, and cyclic groups are powerful. □

Lemma 2.2. *If G is a finite p-group, the relationship*

$$\sigma_A(G) \leq \sigma_P(G) \leq \sigma(G)$$

always holds.

Proof. This follows immediately from the fact that abelian groups are powerful. □

Theorem 2.3. *Let G be a finite p-group. If K is a finite homomorphic image of G such that K is not cyclic, then $\sigma_P(K) \leq \sigma_P(G)$.*

Note (AP): I believe that the following claim is true, but it needs verification. Be careful! It is not true for covering numbers in general. Understanding why would be a good exercise.

Proof. Suppose $G = \bigcup_{i=1}^{n} H_i$, where each H_i is a proper powerful subgroup. Let $\alpha : G \to K$ be a surjective homomorphism. We see that each $\alpha(H_i)$ is also a powerful subgroup, and that

$$\bigcup_{i=1}^{n} \alpha(H_i) = K.$$

todo: It remains to show that each $\alpha(H_i)$ is proper. This is the stumbling block in the general (non-powerful) case. □

Theorem 2.4. *Let G be a finite p-group and let K be a powerful finite p-group. Then $\sigma_P(G \times K) = \sigma_P(G)$.*

Proof. Suppose that G has a minimal covering by powerful subgroups $H_1, \ldots, H_n$. In $G \times K$, each subgroup $H_i \times K$ is powerful, since the property of being powerful is preserved under direct products. Then we notice

$$G \times K = \left(\bigcup_{i=1}^{n} H_i \right) \times K = \bigcup_{i=1}^{n} (H_i \times K),$$

which establishes that $\sigma_P(G \times K) \leq n$.
todo: Establish the other direction, if possible.

□

todo: add reference to Cohn or Tomkinson for the theorem below.

Theorem 2.5. *Let G be a p-group. Then $\sigma(G) = p + 1$.*

This immediately leads to the following result for abelian p-groups.

Corollary 2.6. *Let G be an abelian p-group. Then $\sigma_A(G) = \sigma_P(G) = \sigma(G) = p + 1$.*

The covering number σ is well-behaved with respect to subgroup inclusion: if H is a subgroup of G, then $\sigma(H) \leq \sigma(G)$. However, for powerful covers, this may not be true, since not all subgroups of a powerful group are powerful.

todo: example of a subgroup where the powerful covering number is larger than the powerful covering number of a group?

2.4. **Cyclic and Dihedral Groups.** We define the *cyclic group of order t* to be the group generated by a single element of order t. We write C_t for the cyclic group of order t. We write τ to represent the generator of C_2.

todo: some facts about cyclic groups and the sizes of their subgroups

Lemma 2.7. *If G is a finite abelian group generated by two elements of order two, then G is isomorphic to $C_2 \times C_2$.*

Proof. Let G be a finite abelian group generated by two elements of order two. Call these two elements x and y. Since x and y commute, $(xy)^2 = x^2y^2 = e$, so xy also has order two. Since $(xy)x = x^2y = x$ and $(xy)y = xy^2 = x$, we see that G only has four elements: x, y, xy, and e. Hence G is an abelian group of order four with three elements of order two, it is isomorphic to $C_2 \times C_2$. □

For $n \geq 2$, we define $D(2^n)$ to be the set of isometries of a regular 2^n-gon. The group $D(2^n)$ has 2^{n+1} elements. todo: reflections vs. rotations, etc.

Lemma 2.8. *If G is a finite group generated by two elements of order two, then G is isomorphic to a dihedral 2-group.*

Proof. todo □

3. Elements and Subgroups of Dihedral Groups

In this section, we establish several facts regarding the subgroup structure of dihedral 2-groups. All of these facts are well-known (see todo: some references), but we will provide detailed proofs.

As noted before, we define the group $D(2^n)$ as the set of isometries of a regular 2^n-gon in the Cartesian plane. For definiteness and ease of calculation, let us take the vertices of this 2^n-gon are at the points $\left(\cos\left(\frac{2\pi k}{2^n}\right), \sin\left(\frac{2\pi^k}{2^n}\right)\right)$ for $i = 0, 1, \ldots, 2^n - 1$.

We will distinguish two elements of $D(2^n)$ as a generating set. Let a be the reflection of the 2^n-gon about the line $y =$.

Lemma 3.1. *Suppose $g \in D(2^n)$.*

(i.) *The element g can be written uniquely as $g = (ab)^j a^k$ for some integers j and k with $0 \leq j < 2^n$ and $0 \leq k \leq 1$.*

(ii.) *If $g = (ab)^j a$ for some j with $0 \leq j < 2^n$, then $|g| = 2$.*

(iii.) *If $g = (ab)^j$ for some j with $0 \leq j < 2^n$, then $|g| = \dfrac{2^{n-1}}{\gcd(j, 2^{n-1})}$.*

Proof. Proof of (i.)) This follows from well-known facts about cosets in a group. (todo: Provide lemma in the previous section.) (Proof of (ii.)) Suppose $g = (ab)^j a$ for some j with $0 \leq j \leq 2^{n-1}$. Then we calculate

$$\begin{aligned} ((ab)^j a)^2 &= (ab)^j a (ab)^j a \\ &= a(ba)^j (ab)^j a. \end{aligned}$$

Since $(ab)^j$ is the inverse of $(ba)^j$ and $a^2 = e$, $a(ba)^j(ab)^j a$ is trivial, and the result follows. (Proof of (iii.)) This follows from the fact that (ab) has order 2^{n-1} and Lemma **??**. □

Note that the form for elements given in Lemma **??** may not be the shortest or most intuitive form for writing the element. For instance, the generator $b \in D_4$ would be written as $(ab)^3a$ under the convention we've established. Lemma **??** also establishes the following characterization of elements of order two in $D(2^n)$.

Corollary 3.2. *Let $G = D_{2^n}$. If $g \in G$, then g has order two if and only if $g = (ab)^j a$ for some $0 \leq k \leq 2^n$, or $g = (ab)^{2^n}$.*

The element ab will play a crucial role in our future calculations. Geometrically, ab corresponds to a rotation about $\dfrac{2\pi}{2^n}$ radians.

Lemma 3.3. *Let $n \geq 2$. For the element $ab \in D(2^n)$, the following properties hold.*

(i.) *ab has order 2^n.*
(ii.) *For any r, $(ab)^r a = a(ab)^{-r}$.*
(iii.) *$(ab)^{2^{n-1}} = (ba)^{2^{n-1}}$.*
(iv.) *For any $g \in D(2^n)$, $g(ab)^{2^{n-1}} = (ab)^{2^{n-1}} g$.*

Proof. The order of ab follows directly from the fact that ab represents a rotation of $\dfrac{2\pi}{2^n}$ radians. For (ii.), notice that that $(ab)(ba) = e$, know that $ba = (ab)^{-1}$ and hence represents a rotation of $-\dfrac{2\pi}{2^n}$ radians. Since $(ab)^r a$ represents a reflection, it has order two, and thus $(ab)^r a$ is equal to its own inverse, which is equivalent to $a(ab)^{-r}$. Since a rotation of $2^{n-1}\dfrac{2\pi}{2^n} = \pi$ radians is the same as a rotation of $2^{n-1} \cdot -\dfrac{2\pi}{2^n} = -\pi$ radians, we have that $(ab)^{2^{n-1}} = (ba)^{2^{n-1}}$. To see (iv.), let $g \in D(2^n)$ and write $g = (ab)^j a^k$ as in Lemma **??**(i.). If $k = 0$, then the statement holds since powers of ab commute. If $k = 1$, then we have

$$\begin{aligned}
(ab)^{2^{n-1}} g &= (ab)^{2^{n-1}} (ab)^j a \\
&= (ab)^{2^{n-1}+j} a \\
&= (ab)^j (ab)^{2^{n-1}} a \\
&= (ab)^j a (ba)^{2^{n-1}} \\
&= (ab)^j a (ab)^{2^{n-1}} \\
&= g(ab)^{2^{n-1}}.
\end{aligned}$$

□

Proposition 3.4. *For any $n \geq 1$, $D(2^n)$ has three maximal subgroups. Two of these maximal subgroups are isomorphic to $D(2^{n-1})$, and one is isomorphic to C_{2^n}.*

Proof. We know that the index of the kernel of a homomorphism is equal to the size of its image, and that maximal subgroups in a p-group have index p. Hence the maximal subgroups of $D(2^n)$ correspond to the kernels of nontrivial homomorphisms from $D(2^n)$ to C_2. Such a homomorphism is completely determined by the images of the generators a and b. Let α_1 be the homomorphism for which $\alpha_1(a) = e$ and $\alpha_1(b) = \tau$ is not. Let $H_1 = \ker \alpha_1$. It is not hard to see that this group consists of all elements with an even number of b's, and therefore is generated by a and aba. Since a and aba both have order two, H_1 is isomorphic to a finite dihedral group by Lemma **??**. We know the order of H_1 is 2^n, so H_1 is isomorphic to $D(2^{n-1})$. Let α_2 be the homomorphism for which $\alpha_1(b) = e$ and $\alpha_1(a) = \tau$. Letting $H_2 = \ker \alpha_2$, an identical argument to that of α_1 establishes that $H_2 \cong D(2^{n-1})$. Finally, let α_3 be the homomorphism such that neither $\alpha_3(a) = \alpha_3(b) = \tau$ Let $H_3 = \ker \alpha_3$. It is clear that H_3 contains ab, so H_3 contains the cyclic subgroup $\langle ab \rangle$, which has order 2^n by Lemma **??**. Since H_3 is maximal in $D(2^n)$, we know that H_3 has order 2^n, so $H_3 = \langle ab \rangle \cong C_{2^n}$. □

Proposition 3.5. *Every subgroup of a dihedral 2-group $D(2^n)$ is either dihedral or cyclic.*

Proof. We will proceed by induction. For the base case $n = 2$, this fact is easy to see for $D(4)$. Now assume the statement is true for some $k \geq 2$, and consider $D(2^{k+1})$. By Proposition **??**, the maximal subgroups of this group are either dihedral or cyclic. Then, by the induction hypothesis and the fact that every proper subgroup is contained in some maximal subgroup, the desired result follows. □

Corollary 3.6. *If a subgroup H of $D(2^n)$ is powerful, then either $H \cong C_2 \times C_2$ or $H \cong C_k$ where k is a divisor of 2^{n-1}. If $H \cong C_k$ for $k > 2$, then H is a subgroup of $\langle ab \rangle$.*

Proof. The first statement follows from Proposition **??**. The second statement follows from Lemma **??**. ☐

Proposition 3.7. *Let $\mathcal{C} = \{H_1, \dots, H_q\}$ be any subgroup cover of $D(2^n)$. Then there is some i with $1 \leq i \leq q$ such that $H_i = \langle ab \rangle$.*

Proof. By definition of subgroup cover, there must be some $i \in \{1, \dots, q\}$ such that $ab \in H_i$. Since H_i contains ab, it follows that H_i contains the subgroup$\langle ab \rangle$. Since $\langle ab \rangle$ is maximal and H_i must be a proper subgroup, it follows that $H_i = \langle ab \rangle$. ☐

Note to Risto: I was able to do the proof without what we were calling "Lemma 2" in your office.

Lemma 3.8. *Let H be a subgroup of a dihedral 2-group. Then H is isomorphic to $C_2 \times C_2$ if and only if $H = \langle (ab)^s a, (ab)^t a \rangle$, where $t \neq s$ and $t + s = 2^{n-1}$.*

Proof. Let t and s be distinct positive integers $s + t = 2^{n-1}$. We let $x = (ab)^s a$ and $y = (ab)^t a$, and we let H be a group generated by x and y. First, notice that x and y each have order two, by Lemma **??**. We calculate that

$$\begin{aligned} xy &= (ab)^s a (ab)^t a \\ &= (ab)^s a (ab)^{2^{n-1}-s} a \\ &= (ab)^s aa (ba)^{2^{n-1}-s} \\ &= (ab)^s aa (ab)^{2^{n-1}-s} \\ &= (ab)^s (ab)^{2^{n-1}-s} \\ &= (ab)^{2^{n-1}}. \end{aligned}$$

A similar calculation establishes that $yx = (ba)^{2^{n-1}}$, and since $(ab)^{2^{n-1}} = (ba)^{2^{n-1}}$ by Lemma **??**, it follows that $xy = yx$. Hence $\langle x, y \rangle \cong C_2 \times C_2$ by Lemma **??**.

For the other direction, we suppose that H is a subgroup of $D(2^n)$ such that H is isomorphic to $C_2 \times C_2$. Note that H must contain an element of the form $(ab)^s a$, otherwise H would be contained in the cyclic group $\langle ab \rangle$. H must also contain another element g of order two. We consider two cases for g, following Corollary **??**.

Case 1: $g = (ab)^{2^{n-1}}$. From Lemma **??**, we know that $(ab)^s a = a(ab)^{-s}$ and $(ab)^s a$ commutes with $(ab)^{2^{n-1}}$, giving us

$$\begin{aligned} (ab)^{2^{n-1}} (ab)^s a &= (ab)^{2^{n-1}} a (ab)^{-s} \\ &= (ab)^{2^{n-1}} (ab)^{-s} a \\ &= (ab)^{2^{n-1}-s} a. \end{aligned}$$

Letting $t = 2^{n-1} - s$, we have shown that in this case, $H = \langle (ab)^s a, (ab)^t a \rangle$, where $s \neq t$ and $s + t = 2^{n-1}$.

Case 2: $g = (ab)^r a$ for some r. Without loss of generality, assume $s > r$. Then H also contains $(ab)^s a g$, which is equal to $(ab)^s a (ab)^r a$, which simplifies to $(ab)^{s-r}$. By Lemma **??**, if $s - r \neq 2^{n-1}$, then $(ab)^{s-r}$ generates a cyclic subgroup of order larger than two, contradicting our assumption that $H \cong C_2 \times C_2$. Thus it must be the case that $s - r = 2^{n-1}$, and the result follows. ☐

Corollary 3.9. *Let $g \in D(2^n)$ such that $g = (ab)^j a$ for some $0 \leq j \leq 2^{n-1}$. If H is a powerful subgroup of $D(2^n)$ that contains g, then H is either trivial, isomorphic to C_2, or isomorphic to $C_2 \times C_2$.*

Remark. From Lemma **??**, it follows that there are exactly 2^{n-1} subgroups of $D(2^n)$ that are isomorphic to $C_2 \times C_2$ – one for each pair of numbers s, t with $0 \leq s, t \leq 2^{n-1}$ and $s \neq t$ such that $s + t = 2^n$. It also follows from this Lemma that if H_i and H_j are distinct subgroups isomorphic to $C_2 \times C_2$, then $H_i \cap H_j k = \langle (ab)^{2^{n-1}} \rangle$.

4. The Powerful Covering Number of Dihedral 2-Groups

Proposition 4.1. *There exists a powerful cover of $D(2^n)$ with $2^{n-1}+1$ subgroups.*

Proof. Let $H_1 = \langle ab \rangle$, and for $1 \leq r \leq 2^{n+1}$, let $H_{r+1} = \langle (ab)^r a, (ab)^{2^n - r} a \rangle$. There are $2^{n-1}+1$ subgroups, each H_i is abelian, and every element of $D(2^n)$ is contained in some H_i. □

Theorem 4.2. *The powerful subgroup covering number of $D(2^n)$ is $2^{n-1}+1$.*

Proof. By Proposition **??**, we know that the powerful covering number of $D(2^n)$ is at most $2^{n-1}+1$. Now we show that $D(2^n)$ can not be covered by fewer than $2^{n-1}+1$ powerful subgroups. Let $\mathcal{C} = \{H_1, \dots, H_q\}$ be a powerful cover of $D(2^n)$. Appealing to Proposition **??** and re-indexing if necessary, we may assume that $H_1 = \langle ab \rangle$, so $|H_1| = 2^n$. Now we claim that for each i with $2 \leq i \leq 1$, the subgroup H_i is isomorphic to to either C_2 or $C_2 \times C_2$. This follows from Proposition **??** ,and from the fact that if $H_i \cong C_k$ for some $k > 2$, we would have $H_i \subseteq \langle ab \rangle$. This would make the covering redundant, and hence not minimal. From Remark **??** each H_i that is isomorphic to $C_2 \times C_2$ contains e and $(ab)^{2^{n-1}}$, which are already in H_1, so each H_i that is isomorphic to $C_2 \times C_2$ contributes two new elements, while each H_i that is isomorphic to C_2 contributes one new element. This means that

$$\left| \bigcup_{i=1}^{q} H_i \right| \leq |H_1| + 2(q-1) = 2^n + 2(q-1).$$

In other words, the subgroups $H_2, \dots, H_q$ can contain at most $2(q-1)$ elements not contained in H_1. If $q < 2^{n-1}$, we would then have

$$\left| \bigcup_{i=1}^{q} H_i \right| < 2^n + 2(2^{n-1}) = 2^{n+1},$$

meaning that this collection of subgroups could not be a cover for the 2^{n+1} elements of $D(2^n)$. Thus, any cover of $D(2^n)$ by powerful subgroups must contain at least $2^{n-1}+1$ powerful subgroups. This completes the proof. □

Corollary 4.3. *For $n \geq 2$, $\sigma_P(D(2^n)) = \sigma_A(D(2^n))$.*

Proof. This follows from Theorem **??** and Corollary **??**. □

5. Conclusion

There are three 2-groups of coclass equal to 1. We have explicitly calculated the powerful covering number for one of them.

References

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 2004. 1

[2] Charles R Leedham-Green. The structure of finite p-groups. *Journal of the London Mathematical Society*, 50(1):49–67, 1994. 1

[3] CR Leedham-Green and MF Newman. Space groups and groups of prime-power order I. *Archiv der Mathematik*, 35(1):193–202, 1980. 1

[4] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. I. Finite groups. *Journal of Algebra*, 105(2):484–505, 1987. 1

[5] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. II. p-adic analytic groups. *Journal of Algebra*, 105(2):506–515, 1987. 1

[6] G. A. Miller. Groups in which all the operators are contained in a series of subgroups such that any two have only identity in common. *Bull. Amer. Math. Soc.*, 17:446–449, 1906/1907. 1

Department of Mathematics and Computer Science, Stillwell 426, Western Carolina University, Cullowhee, NC 28723 USA
E-mail address: ratanasov@email.wcu.edu

Department of Mathematics and Computer Science, Stillwell 426, Western Carolina University, Cullowhee, NC 28723 USA
E-mail address: adgregory1@catamount.wcu.edu

Department of Mathematics and Computer Science, Stillwell 426, Western Carolina University, Cullowhee, NC 28723 USA
E-mail address: lrguatelli1@catamount.wcu.edu

Department of Mathematics and Computer Science, Stillwell 426, Western Carolina University, Cullowhee, NC 28723 USA
E-mail address: adpenland@email.wcu.edu