2012

Non-Abelian Groups with Perfect Order Subsets

Hongying Zhao

NON-ABELIAN GROUPS WITH PERFECT ORDER SUBSETS

Hongying Zhao

Thesis Submitted to The College of Saint Benedict
Department of Mathematics
for the Degree of Bachelor of Art in Mathematics

Thesis Advisor: Dr. Bret Benesh

2012

ABSTRACT

The purpose of this paper is to explore non-abelian finite groups with *perfect order subsets*. A finite groups is said to have perfect order subsets (POS) if the number of elements of each given order can divide the order of the group. The study of such groups was initiated by Carrie E. Finch and Lenny Jones. In this paper, we construct POS-groups by considering semi-direct products of cyclic groups (and sometimes quaternions).

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor Dr. Bret Benesh for his unfailing support and guidance. He has taught me, both consciously and subconsciouly, how to think mathematically. His enthusiasim for math is motivational and contagious. He has been my inspiration as I hurdle all kinds of obstacles in the completion of my research work. I am truly thankful for all his contribution of time and ideas.

I would also like to thank Dr. Tom Sibley, Dr. Michael Gass and Dr. Jennifer Galovich for their steadfast encouragment and insightful suggestions.

Finally, none of this would have been possible without the Collge of Saint Benedict / Saint John's University Mathematics Department and Undergraduate Research program. I sincerely appreciate the opportunity and funding they provided to make my undergraduate experience stimulating.

Contents

CHAPTER 1

INTRODUCTION

In group theory, there are a lot of connections among orders of groups and orders of their subgroups. Among all of them, the most commonly used and well-known one is Lagrange's Theorem, which states a relationship between the order of a finite group and the order of every subgroup. In the paper *A Curious Connection Between Fermat Numbers and Finite Groups*, Carrie E. Finch and Lenny Jones studied groups with the property that the number of elements of every given order divides the order of a whole group.They referred to these groups as having *perfect order subsets* (POS).

By using techniques in elementary number theory and group theory, I investigated non-abelian groups, particularly semi-direct products with perfect order subsets. I wanted to focus on the semi-direct products because a fair amount of research has been done on abelian POS groups. Also, S_3 is an easy non-abelian example of a group with perfect order subsets, and S_3 can be expressed in the form of a semi-direct product: $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

When semi-direct products of groups are involved, it is always necessary to consider the action. Most of this paper assumes the action is inversion. I then further explore semi-direct products where the action is not inversion. While it is not unusual for POS to occur, it is suprising to see how many different categories of groups can be built up by only using a small number of prime components.

The introductory sections will mainly discuss Finch and Jones's orginal definitions and some simple examples as well as non-examples.

1.1 METHODOLOGY

In the beginning stage of this research, I used GAP to list all non-abelian groups with perfect order subsets whose orders are less than 250. This allowed me to look for patterns, make conjectures, and create a big picture of formats of POS groups. The GAP code I used is included in the last chapter of this paper.

Most of the groups with perfect order subsets resulting from the GAP code are categorized and all investigation is proven in detail. References of results that I used in this research are clearly provided.

1.2 NOTATIONS AND NEWLY INTRODUCED DEFINITIONS

Throughout this paper, all groups are finite, and for a group G, we denote $|G|$ to be the order of G and $o(x)$ to be the order of a group element x in G. As in [1], the **order subset** of G determined by an element $x \in G$ is defined to be the set $OS(x) = \{y \in G | o(y) = o(x)\}$.

The group G is said to have **perfect order subsets** (in short, G is called a POS-group) if $|OS(x)|$ is a divisor of $|G|$ for all $x \in G$. We use the standard notation $\mathbb{Z}_n$ to denote the cyclic group of order n with elements $0, 1, ..., n-1$ under addition.

1.3 BASIC EXAMPLES AND NON-EXAMPLES

Example 1.3.1. *Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$. It is easy to see $|G| = 24$. We can frame the following table:*

Element Order	*Cardinality of Order Subset*
1	*1*
2	*3*
3	*2*
4	*4*
6	*6*
12	*8*

Every element in the right column, i.e. the number of elements of every given order a divides $|G|$. Therefore, G has perfect order subsets.

The following is a short list of some abelian groups that have perfect order subsets that were proven in Finch and Jones' paper [1]:

- $\mathbb{Z}_{2^n}$ for all n
- $(\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$
- $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- $(\mathbb{Z}_2)^5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{31}$
- $(\mathbb{Z}_2)^{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \times \mathbb{Z}_{257}$

Not only abelian groups have perfect order subsets, but non-abelian groups can also be POS groups.

Example 1.3.2. *Let $G \cong \mathbb{S}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_7$.Then $|G| = 84$, and:*

Element Order	*Cardinatliy of Order Subset*
1	*1*
2	*7*
3	*2*
6	*2*
7	*6*
14	*42*
21	*12*
42	*12*

From the table, we know G has perfect order subsets.

Here are more examples of non-abelian POS groups that appear in Finch and Jones' paper [2]:

- $\mathbb{S}_3 \times (\mathbb{Z}_2)^2 \times \mathbb{Z}_5$
- $SL(2, q)$, where $q \in \{2, 3, 5, 7, 11, 17, 19, 41, 49, 127, 251\}$ and where $SL(2, q)$ denotes the group of all 2×2 matrices with determinant one and entries from the finite field $\mathbb{F}_q$ of q elements, where $q = p^n$ for some prime p.

However, it is not difficult to find examples of groups *not* having perfect order subsets. Consider $\mathbb{Z}_7$; it is not a POS group as it has 6 elements of order 7.

As noticed by Tuan and Hai in [11] and Das in [12], groups that do not have perfect order subsets include:

- the symmetric group S_n, when $n \geq 4$
- $\mathbb{D}_{2n}$, when n is an even integer.
- non-cyclic 2-groups

CHAPTER 2

ABELIAN POS GROUPS

In this chapter, we will examine several theorems for abelian POS groups that have been proved by Finch and Jones.

Lemma 2.0.3. *Let* $G \cong (\mathbb{Z}_{p^a})^t \times M$ *and* $\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$*, where a and t are positive integers and p is a prime that does not divide* $|M|$*. Suppose that d is the order of an element in* $\hat{G}$ *and that* p^{a+1} *does not divide d. Then both G and* $\hat{G}$ *contain the same number of elements of order d.*

Theorem 2.0.4. ***(Going-Up Theorem)*** *Let* $G \cong (\mathbb{Z}_{p^a})^t \times M$ *and* $\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^t \times M$*, where a and t are positive integers and p is a prime that does not divide* $|M|$*. If G has perfect order subsets, then* $\hat{G}$ *has perfect order subsets.*

Example 2.0.5. *In Example 1.3.1, we know* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ *has perfect order subsets. The Going-Up Theorem allows us to increase the exponent on any of the primes that appear to create new POS groups. In this case, we also know* $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ *has perfect order subsets.*

We can generate new POS groups not only by "going up", but also by going in the other direction.

Theorem 2.0.6. ***(Chopping-Off Theorem)*** *Suppose that G has perfect order subsets and that* $G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times ...\mathbb{Z}_{p^{a_{s-1}}} \times (\mathbb{Z}_{p^{a_s}})^t \times M$*, where p is a prime not divid-*

ing $|M|$ and $a_1 \leq a_2 \leq ... \leq a_{s-1} < a_s$ are positive integers. Then $\hat{G} \cong (\mathbb{Z}_{p^{a_s}})^t \times M$ also has perfect order subsets.

Theorem 2.0.7. ***(Going-Down Theorem)*** *Suppose that G has perfect order subsets and that $G \cong (\mathbb{Z}_{p^a})^t \times M$, where p is a prime not dividing $|M|$. Then $\hat{G} \cong (\mathbb{Z}_p)^t \times M$ also has perfect order subsets.*

We will illustrate the above two theorems by using the following example.

Example 2.0.8. *By Example 1.3.1, we know $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ has perfect order subsets. By applying Chopping-Off theorem, we have $\mathbb{Z}_4 \times \mathbb{Z}_3$ is a POS group. Then, according to the Going-Down Theorem, we know $\mathbb{Z}_2 \times \mathbb{Z}_3$ also has perfect order subsets.*

These powerful theorems indicate that we can generate infinitely many families of abelian groups with perfect order subsets. Therefore, there exist infinitely many abelian groups with perfect order subsets.

CHAPTER 3

EULER PHI FUNCTION

In this chapter, we will introduce the Euler Phi function, which will be used in this paper to count numbers of elements of given orders.

Definition 3.0.9. *Euler Phi Funcion, denoted by $\Phi(n)$, is the number of positive integers less than n and relatively prime to n.* *[80, Gallian]*

We are using an upper Φ here because we have the lower ϕ reserved for later use in our notation for functions.

Example 3.0.10. *It is true that $\Phi(10) = 4$ because 1,3,7 and 9 are relative prime to 10.*

Theorem 3.0.11. *If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\Phi(d)$.* *[80, Gallian]*

Furthermore, we would like to know how to calculate $\Phi(d)$, where d is a positive integer.

Theorem 3.0.12. *The Euler Phi function is multiplicative. Moreover,*

$$\Phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

[58, Nathanson]

In particular, if $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ is the standard factorization of n, where $p_1, p_2, .., p_k$ are distinct primes and $r_1, r_2, .., r_k$ are positive integers, then

$$\Phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) = \prod_{i=1}^{k} p_i^{r_i} (1 - \frac{1}{p_i}) = \prod_{i=1}^{k} p_i^{r_i - 1} (p_i - 1)$$

Example 3.0.13. *Consider* $7875 = 3^2 5^3 7$. *Then* $\Phi(7875) = \Phi(3^2)\Phi(5^3)\Phi(7) = (3-1) \cdot 3 \cdot (5-1) \cdot 5^2 \cdot (7-1) = 3600$

Example 3.0.14. *Consider the group* $\mathbb{Z}_{384}$. *We have* $128|384$ *and there are* $\Phi(128) = \Phi(2^7) = (2-1)2^6 = 64$ *elements of order 128.*

In this paper, we mostly use the fact that in the group $\mathbb{Z}_m$, if $p^k|m$, where p^k is a power of a single prime, then there are $\Phi(p^k) = (p-1)p^{k-1}$ elements of order p^k.

CHAPTER 4

AN INTRODUCTION TO SEMIDIRECT PRODUCTS

In this chapter, we will explore the concept of semi-direct products, which will be frequently used later in this paper.

Let G be a group. Recall that G is a direct product of two groups if and only if G contains normal subgroups N_1, N_2 such that $N_1 \cap N_2 = \{e\}$ and $G = N_1 N_2$. Semidirect products are a generalization of this notion.

Definition 4.0.15. *A group G is a semidirect product of its subgroups N and H if and only if $N \lhd G$, $G = NH$, and $N \cap H = \{e\}$, where e is the identity of G. (Hence H is a complement of N).* *[213, Scott]*

Note that conjugation of N induces an automorphism of N. So there is a homomorphism $\phi : H \mapsto \mathrm{Aut}(N)$. Then we can denote a semidirect product of N and H as $N \rtimes_\phi H$ (or $N \rtimes H$ if the action is clear from context).

Suppose $G = NH$ with N and H as above. Notice that every element has a unique expression nh with $h \in H$ and $k \in K$. The uniqueness follows from $N \cap H = \{e\}$, since if $nh = n'h'$, then $(n')^{-1}n = h'h^{-1} \in N \cap H = \{e\}$, so $n = n'$ and $h = h'$. And, as N is normal in G, for each $h \in H$ we have an automorphism $\phi(h)$ of N given by $n \mapsto \phi_h(n) = hnh^{-1}$. Furthermore, the map $\phi : H \to Aut(N)$ given by $h \mapsto (n \mapsto hnh^{-1})$ is a group homomorphism. Therefore, given the subgroups N, H and the homomorphism φ, we can write down the multiplication on G. For, given n_1h_1, $n_2h_2 \in G$, we have $(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2)$.

Finally, if φ is not the trivial map, then $N \rtimes_\varphi H$ is non-abelian, even if N and H are both abelian. To show this, suppose $h \in H$ and $n \in N$ such that $\varphi_h(n) \neq n$. We then have:

$$(n, 1)(1, h) = (n, h)$$
$$(1, h)(n, 1) = (\varphi_h(n), h).$$

So $(n, 1)(1, h) \neq (1, h)(n, 1)$. Using semidirect products is a nice way to construct many but not all non-abelian groups.

We now give several examples of semidirect products.

Example 4.0.16. *Let $N = \mathbb{Z}_n$, let $H = \mathbb{Z}_2$, and let $\varphi : H \to Aut(N)$ be the homomorphism that sends e to e and the nontrivial element of H to the inverse map of N. The map $x \mapsto x^{-1}$ is a group automorphism of N since N is abelian, and this automorphism has order 2. Thus, it generates a subgroup of $Aut(N)$ isomorphic to H; we define the map φ to be the isomorphism of H onto this subgroup. Let $G = N \rtimes_\varphi H$. We claim that $G \cong D_n$, the dihedral group of order $2n$. Recall that D_n is the group generated by elements a, b, subject to the relation $a^n = b^2 = 1$ and $bab = a^{-1}$. Let $N = \langle x \rangle$ and $H = \langle y \rangle$. Then $(x, 1)$ has order n and $(1, y)$ has order 2. Note that φ_y is the inverse map on N. So,*

$$(1, y)(x, 1)(1, y) = (\varphi_y(x), y)(1, y) = (\varphi_y(x), y^2) = (\varphi_y(x), 1) = (x^{-1}, 1) = (x, 1)^{-1}.$$

Therefore, in G we have elements $u = (x, 1)$ and $v = (1, y)$ satisfying $u^n = v^2 = 1$ and $vuv = u^{-1}$. So, there is a group homomorphism $D_n \to G$, and this map *is surjective since G is clearly generated by* $\{(x, 1), (1, y)\}$. *However,* $|G|$=$|N||H| = 2n$, *so* $|G| = |D_n|$. *This shows that* D_n *is isomorphic to G.*

Example 4.0.17. *Let* p, q *be primes such that* p *divides* $q-1$. *Then* $Aut(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$ *is a cyclic group of order* $q-1$, *so it has an element of order* p. *If* r *is an integer such that* $r^p \equiv 1$ *(mod q) but* $r \not\equiv 1$ *(mod q), then the automorphism* f *given by* $f(\alpha) = \alpha^r$ *has order* p. *If we send a generator of* $\mathbb{Z}_p$ *to this element, we get a homomorphism* $\varphi : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$. *Let G be the semidirect product of these groups. If* $\mathbb{Z}_p = \langle a \rangle$, *and* $\mathbb{Z}_q = \langle b \rangle$, *then* $\varphi_a(b) = f(b)$, *we have* $a^p = b^q = 1$ *and* $aba^{-1} = \varphi_a(b) = f(b) = b^r$. *So this semidirect product is a group of order* pq, *and since* $aba^{-1} = b^r \neq b$ *(as* $r \not\equiv 1$ *(mod q)), we see that G is non-abelian.*

CHAPTER 5

NONABELIAN GROUPS HAVING PERFECT ORDER SUBSETS

5.1 SOME PROPERTIES OF SEMIDIRECT PRODUCTS WITH PERFECT ORDER SUBSETS

Before I start to demonstrate properties of semi-direct product groups with perfect order subsets, I need to show these two lemmas first.

Lemma 5.1.1 (Z.). *If G is a POS group, then $|G|$ has to be even unless $|G| = 1$.*

Proof. If every element in G is of order 1 or 2, $|G|$ is even by Lagrange's Theorem. Suppose there exists an element in G of order other than 1 and 2. Then $|OS(x)|$ is even since every element in $|OS(x)|$ can be paired up with its inverse. Since G is POS, $OS(x)$ is a divisor of $|G|$. Thus, $|G|$ is even. □

Lemma 5.1.2 (Z.). *If $|G|$ is even, the number of elements of order 2 in G is odd.*

Proof. In a group G, there is always one element of order 1 and an even number of elements of order other than 1 and 2. Thus $|OS(2)| = |G| - 1 - \sum |OS(a_i)|$, with $o(a_i) \neq 1$ or 2. Since $|G|$ is even, $|OS(2)|$ has to be odd.

$\square$

By applying the previous lemmas, we can have the following theorems:

Theorem 5.1.3 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_{p^m} \rtimes \mathbb{Z}_{q^n}$, where p,q are primes and m, n are positive integers, and the action is nontrivial but otherwise arbitrary. If G has perfect order subsets, then p does not equal to 2 and q has to be 2.*

Proof. Let the cyclic groups $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{q^n}$ be generated by a and b, respectively. By Lemma 5.1.1, we know $|G|$ has to be even. Thus at least one of p, q has to be 2.

Suppose $p = q = 2$. Then $G = \mathbb{Z}_{2^m} \rtimes \mathbb{Z}_{2^n}$. Both $(a^{2^{m-1}}, e)$ and $(e, b^{2^{n-1}})$ are of order 2. Since G has even size, by Lemma 5.1.2, its number of elements of order 2 has to be odd, and it has to be greater than 2. So $|OS(2)|$ is odd and cannot divide $|G| = 2^{m+n}$. Therefore, $G = \mathbb{Z}_{2^m} \rtimes \mathbb{Z}_{2^n}$ does not have perfect order subsets.

Suppose $p = 2$ and $q \neq 2$. Then $G = \mathbb{Z}_{2^m} \rtimes \mathbb{Z}_{q^n}$. It is commonly known that $\mathrm{Aut}(\mathbb{Z}_{2^m}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$, and so we have $|\mathrm{Aut}(\mathbb{Z}_{2^m})| = 2^{m-1}$. Let $\sigma = \phi_w \in \mathrm{Aut}(\mathbb{Z}_{2^m})$ for some $w \in \mathbb{Z}_{q^n}$. We have $o(\sigma)|2^{m-1}$. Also, $o(\sigma)|q^n$, which is not possible unless $o(\sigma) = 1$. Thus, G does not have perfect order subsets.

From above, if $G \cong \mathbb{Z}_{p^m} \rtimes \mathbb{Z}_{q^n}$ is a POS group, then $p \neq 2$ and $q = 2$.

$\square$

Example 5.1.4. *The group $G \cong \mathbb{Z}_9 \rtimes \mathbb{Z}_4$ with inversion has perfect order subsets. In G, there is 1 element of order 1, 1 element of order 2, 2 elements of order 3, 18 elements of order 4, 2 elements of order 6, 6 elements of order 9 and 6 elements of order 18.*

5.2 SEMIDIRECT PRODUCTS WITH INVERSIONS

We start this section by a lemma that will be used frequently in the proofs of theorems afterwards.

Lemma 5.2.1 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$, where p is a prime and m, n are positive integers. Suppose a, b are generators of $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{2^n}$ respectively and $\phi_b(a) = a^{-1}$. For $(a^l, b^k) \in \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$, $b^k \notin ker(\phi)$ if and only if $o(b^y) = 2^n$.*

Proof. If $o(b^k) = 2^n$, then $\mathbb{Z}_{2^n} = \langle b^k \rangle = \langle 1 \rangle$. So $\phi(1) \in \ker(\phi)$ and therefore $c \in ker(\phi)$ for all $c \in \mathbb{Z}_{2^l}$. This cannot be true, and so a contradiction. Morever, if $o(b^k) \neq 2^n$, then $o(b^k) = o(b^{2^i})$ for some $1 \leq i < n$, and $\phi(b^k) = \phi(b^{2^i}) = [\phi(b)]^{2^i} = e_b$. Thus $b^k \in \ker(\phi)$. $\square$

Theorem 5.2.2 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$, where p is a prime and m, n are positive integers. Suppose a, b are generators of $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{2^n}$, respectively, and $\phi_b(a) = a^{-1}$. Then G has perfect order subsets if and only if $p = 3$ or 5. When $p = 3$, $n \geq 1$; when $p = 5, n \geq 2$.*

The following lemma will be useful in the proof of Theorem 5.2.2.

Lemma 5.2.3 (Z.). *Let $G \cong \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$, where p is a prime and m, n are positive integers. Suppose a, b are generators of $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{2^n}$, respectively, and $\phi_b(a) = a^{-1}$. Then the table of sizes of order sets for G is Table 5.1.*

Proof. Let $(a^l, b^k) \in \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$. By Lemma 5.2.1, we have $b^k \notin ker(\phi)$ if and only $o(b^k) = 2^n$ in $\mathbb{Z}_{2^n}$. Then, when $o(b^k) \neq 2^n$, we can calculate the order of (a^l, b^k) the same way as in direct product $\mathbb{Z}_{p^m} \times \mathbb{Z}_{2^n}$, i.e. $o(a^l, b^k) = \text{lcm}(o(a^l), o(b^k))$. Furthermore, since $o(a^l)$ is a divisor of p^m and $o(b^k)$ is a divisor of 2^n, $o(a^l, b^k) = o(a^l) \cdot o(b^k)$.

Orders of Elements	Cardinalities of Order Subsets
1	1
$2^i(1 \leq i \leq n-1)$	2^{i-1}
2^n	$2^{n-1}p^m$
$p^i(1 \leq i \leq m)$	$p^{i-1}(p-1)$
$2^i p^j(1 \leq i \leq n-1, 1 \leq j \leq m)$	$2^{i-1}p^{j-1}(p-1)$

Table 5.1

When $o(b^k) = 2^n$, k is an odd positive integer, and $(a^l, b^k)(a^l, b^k) = (a^{l+(-1)^k l}, b^{2k}) = (e, b^{2k})$. So for $(a^l, b^k)^w$, where w is a positive integer, if w is odd, $(a^l, b^k)^w = (a^l, b^{wk})$; if w is even, $(a^l, b^k)^w = (e, b^{wk})$. Therefore, $o(a^l, b^k) = 2^n$.

By using the analysis above, we can prove Table 5.1 in detail.

- The identity is the only element of order 1.
- Elements of order $2^i(1 \leq i < n)$ in G are exactly those in $\mathbb{Z}_{2^n}$ of order 2^i, and there are $\Phi(2^i) = 2^{i-1}$ of them.
- (a^l, b^k) is of order 2^n as long as $o(b^k) = 2^n$ in $\mathbb{Z}_{2^n}$. There are $\Phi(2^n) = 2^{n-1}$ such y that satisfies this condition. So, there are $2^{n-1}p^m$ elements of order 2^n.
- Elements of order $p^i(1 \leq i \leq m)$ in G are exactly the ones in $\mathbb{Z}^{p^m}$ of order p^i, and there are $\Phi(p^i) = (p-1)p^{i-1}$ such elements.
- $o(a^l, b^k) = 2^i p^j(1 \leq i < n, 1 \leq j \leq m)$ if and only if $o(a^l) = p^j$ in $\mathbb{Z}_{p^m}$ and $o(b^k) = 2^i$ in $\mathbb{Z}_{2^n}$. So $|OS(2^i p^j)| = \Phi(p^j)\Phi(2^i) = 2^{i-1}p^{j-1}(p-1)$.

$\square$

Proof of Theorem 5.2.2. Suppose G is a *POS group* with the given action.

Lemma 5.2.3 has listed the cardinalities of every order subset. To make G a POS group, we want all cardinalities of order subsets to divide $|G|$. In particular, the number of elements of order $2^i p^j$ must divide $|G|$ when $i = n-1$ and $j = m$, that is, $2^{n-2}p^{m-1}(p-1)$ divides $2^n p^m$ and $p-1$ is a divisor of $2^2 = 4$. Since $p \neq 2$ by Theorem 5.1.3, $p = 3$ or 5. When $p = 3$, $|OS(p^m)| = 2 \cdot 3^{m-1}$, so we have $n \geq 1$. When $p = 5$, $|OS(p^m)| = 2^2 \cdot 5^{(m-1)}$. We then have $n \geq 2$.

Now suppose $G = \mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$ with $\phi_b(a) = a^{-1}$ and $p = 3$ or $p = 5$. When $p = 3, n \geq 1$; when $p = 5, n \geq 2$.

$\square$

Corollary 5.2.4 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_2 \times (\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n})$, where m, n are positive integers. Let a, b be generators of $\mathbb{Z}_{3^m}$ and $\mathbb{Z}_{2^n}$ respectively and $\phi_b(a) = a^{-1}$. Then G has perfect order subsets .*

Proof. According to the previous proofs, we know cardinalities of all order subsets of the subgroup $\{0\} \times (\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n})$. However, in $G \cong \mathbb{Z}_2 \times (\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n})$, the number of elements of 2^i $(1 < i < n)$is twice the cardinality of order subset of 2^i in $\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n}$, since for $g \in \mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n}$, if $o(g) = 2^i$ in $\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n}$, then $0 \times g$ and $1 \times g$ are both of order 2^i in G. The calculation of cardinalities of subsets of elements of order 2^n and $2^i 3^j$, where $1 \leq j \leq m$, is similar. In addition, different from $\mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n}$, we have elements of order $2 \cdot 3^j$, since if the order of $z \in \mathbb{Z}_{3^m} \rtimes_\phi \mathbb{Z}_{2^n}$ is 3^j, then $1 \times z$ has order $2 \cdot 3^j$. Furthermore, the number of elements of order 3^j equals the number of elements of order $2 \cdot 3^j$.

We then make the following table:

Orders of Elements	Cardinalities of Order Subsets
1	1
2	3
$2^i(2 \le i \le n-1)$	2^i
2^n	$2^n 3^m$
$3^i(1 \le i \le m)$	$2 \cdot 3^{i-1}$
$2 \cdot 3^i(1 \le i \le m)$	$2 \cdot 3^i$
$2^i 3^j(2 \le i \le n-1, 1 \le j \le m)$	$2^{i+1}3^{j-1}$

Table 5.2

With the sizes of every order subset being a divisor of $|G|$, we know G is a POS group. $\square$

Theorem 5.2.5 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$, and a, b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively. If $\phi_b(a) = a^{-1}$ and G is a POS group, then $n = 2^\alpha 3^\beta$, where α is a positive integer, and β is a non-negative integer.*

Proof. Since ϕ_b is of order 2 in $|Aut(\mathbb{Z}_m)|$ and $o(\phi_b)$ divides n, by the Uniqueness of Factorization, we have $n = 2^{\alpha_0} {p_1}^{\alpha_1} {p_2}^{\alpha_2} {p_3}^{\alpha_3} ... {p_k}^{\alpha_k}$, where $p_i(1 \le i \le k)$ are all odd primes and $1 \le \alpha_i$ for $0 \le i \le k$. .

Suppose n divides m. Then by a proof similar to the proof for Theorem 5.2.2, we have that the number of elements of order n is the sum of $m \cdot \Phi(n)$ and the number of elements of order n in $\mathbb{Z}_m$, where Φ is the Euler Phi Function and

$$\Phi(n) = 2^{\alpha_0 - 1}(p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} ... (p_k - 1)p_k^{\alpha_k - 1}.$$

In $\mathbb{Z}_m$, the number of elements of order n is also $\Phi(n)$. Thus, there are

$$(m+1)2^{\alpha_0 - 1}(p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} ... (p_k - 1)p_k^{\alpha_k - 1}$$

of elements of order n in G. Since G is a POS group, $(m+1)2^{\alpha_0-1}(p_1-1)p_1^{\alpha_1-1}(p_2-1)p_2^{\alpha_2-1}...(p_k-1)p_k^{\alpha_k-1}$ is a divisor of $|G|$. $mn = m2^{\alpha_0}{p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3}...{p_k}^{\alpha_k}$. This is equivalent to saying

$$(m+1)(p_1-1)(p_2-1)...(p_k-1)|2mp_1p_2...p_k.$$

Because $(m+1)$ and m are relatively prime, we should have $(m+1)$ divides $2p_1p_2...p_k$. It is not possible since m is a multiple of n, by assumption. Then $m+1$ is greater than n, and further greater than $2p_1p_2...p_k$. Therefore, n cannot be a divisor of m.

So in $\mathbb{Z}_m$, there is no element of order n, and the number of elements of order n is $m2^{\alpha_0-1}(p_1-1)p_1^{\alpha_1-1}(p_2-1)p_2^{\alpha_2-1}...(p_k-1)p_k^{\alpha_k-1}$. To make it a divisor of mn, we need $(p_1-1)(p_2-1)...(p_k-1) \mid 2p_1p_2...p_k$. As the p_i are odd numbers for all i, the p_i-1 are multiples of 2. So $(p_1-1)(p_2-1)...(p_k-1) = 2^k u$, where u is a positive integer and $2^k u \mid 2p_1p_2...p_k$. Thus $k=0$ or $k=1$.

If $k=0$, we are done, since this implies that $n=2^\alpha$. If $k=1$, from the above we know $(p-1)$ is a divisor of $2p$. So $p=3$.

□

Example 5.2.6. *The group $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_{12}$ has perfect order subsets.*

In the next theorem, we will further discuss what m can be when $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$ is a POS group and $n = 2^\alpha 3^\beta$.

Theorem 5.2.7 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_{2^l3^n} (l, n \geq 1)$, where a, b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively. Further, suppose that $\phi_b(a) = a^{-1}$. If* $\gcd(m, 2^l 3^n) = 1$ *and G is a POS-group, then m is a power of 7 and $l \geq 2$.*

Proof. We can factor m into ${q_1}^{c_1}{q_2}^{c_2}{q_3}^{c_3}...{q_k}^{c_k}$. Since m and $2^l 3^n$ are relatively prime, $q_i \neq 2$ or 3 for all $1 \leq i \leq k$. We count the number of elements of order

$m2^{l-1}3^n$. Since all elements of the form $b^{2^{l-1}3^n}$ in $\mathbb{Z}_{2^l3^n}$ are of order 2, they are in $\ker(\phi)$. We now consider two cases:

Case 1: $l \geq 2$. There are

$$2^{l-1}3^{n-1}(q_1-1)q_1^{c_1-1}(q_2-2)q_2^{c_2-1}...(q_k-1)q_k^{c_k-1}$$

elements of order $m2^{l-1}3^n$. Then $2^{l-1}3^{n-1}(q_1-1)q_1^{c_1-1}(q_2-2)q_2^{c_2-1}...(q_k-1)q_k^{c_k-1}$ divides $mn = 2^l3^n q_1{}^{c_1}q_2{}^{c_2}q_3{}^{c_3}...q_k{}^{c_k}$. This is equivalent to $(q_1-1)(q_2-1)...(q_k-1)$ being a divisor of $6q_1q_2...q_k$. Since $q_i - 1$ is an even number for all i, but $6q_1q_2...q_k = 2 \cdot w$, where w is odd, we have $k = 1$. Furthermore, $q-1|6q$, so $q = 7$.

Case 2: $l = 1$. There are

$$2 \cdot 3^{n-1}(q_1-1)q_1^{c_1-1}(q_2-2)q_2^{c_2-1}...(q_k-1)q_k^{c_k-1}$$

elements in G of order $m2 \cdot 3^n$. Since G is a POS group, we have $2 \cdot 3^{n-1}(q_1-1)q_1^{c_1-1}(q_2-2)q_2^{c_2-1}...(q_k-1)q_k^{c_k-1}$ must be a divisor of $mn = 2 \cdot 3^n q_1{}^{c_1}q_2{}^{c_2}q_3{}^{c_3}...q_k{}^{c_k}$, which is equivalent to $(q_1-1)(q_2-1)...(q_k-1)$ being a divisor of $3q_1q_2...q_k$. This is not possible, when $q_i \geq 5$ for $1 \leq i \leq k$.

Therefore, if $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_{2^l3^n} (l, n \geq 1)$ has perfect order subsets, m has to be a power of 7 and $l \geq 2$. So $G \cong \mathbb{Z}_{7^c} \rtimes_\phi \mathbb{Z}_{2^l3^n}$. We have a table summarizing these results on the next page.

Orders of Elements	Cardinalities of Order Subsets
1	1
$2^i((1 \leq i \leq l-1)$	2^{i-1}
$3^j(1 \leq j \leq n))$	$2 \cdot 3^{j-1}$
$7^k(1 \leq k \leq c)$	$6 \cdot 7^{k-1}$
$2^i 3^j(1 \leq i \leq l-1, 1 \leq j \leq n)$	$2^i 3^{j-1}$
$2^i 7^k(1 \leq i \leq l-1, 1 \leq k \leq c)$	$3 \cdot 2^i 7^{k-1}$
$3^j 7^k(1 \leq j \leq n, 1 \leq k \leq c)$	$4 \cdot 3^j 7^{k-1}$
$2^i 3^j 7^k(1 \leq i \leq l-1, 1 \leq j \leq n, 1 \leq k \leq c)$	$2^{i+1} 3^j 7^{k-1}$
2^l	$2^{l-1} 7^c$
$2^l 3^j(1 \leq j \leq n)$	$2^l 3^{j-1} 7^c$

Table 5.3

In this case, G always has perfect order subsets.

□

When m and $n = 2^a 3^b$ are not relatively prime, the case is more complicated. Before we consider, we need to see a new related definition and several lemmas.

Definition 5.2.8. *A group G is said to have **almost perfect order subsets** if the number of elements in each order subset of G is a divisor of $2|G|$.*

Lemma 5.2.9. *In $G \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}$, where p is a prime, there are $(p^2-1) \cdot p^{2i-2}$ elements of order p^i, where $i \leq m$ and $i \leq n$.*

Proof. We first count the number of elements (x, y), where x is of order p^i in $\mathbb{Z}_{p^m}$, and y is of order less than or equal to p^i in $\mathbb{Z}_{p^n}$. There are

$$\Phi(p^i) \cdot (1 + \Phi(p) + \Phi(p^2) ... + \Phi(p^i))$$

$$= (p-1)p^{i-1}[1 + (p-1) + (p-1)p + ... + (p-1)p^{i-1}] = (p-1)p^{2i-1}$$

choices.

Next, we count ordered pairs in $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$ with an element of order strictly less than p^i in the first position and an element of order exactly p^i in the second position. There are

$$[1 + \Phi(p) + \Phi(p^2) ... + \Phi(p^{i-1})] \cdot \Phi(p^i) = p^{i-1} \cdot (p-1)p^{i-1} = (p-1)p^{2i-2}$$

such elements. In sum, we have

$$(p-1)p^{2i-1} + (p-1)p^{2i-2} = (p^2-1) \cdot p^{2i-2}$$

elements of order p^i in $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$. □

The proofs of the following lemma is similar to the proof for the Going-Up Theorem in Finch and Jones' paper [1].

Lemma 5.2.10 (Z.). *Let $G \cong (\mathbb{Z}_{p^a})^2 \times M$ and $\hat{G} \cong (\mathbb{Z}_{p^{a+1}})^2 \times M$, where a is a positive integer and p is a prime that does not divide $|M|$. If G has almost perfect order subsets, then $\hat{G}$ has almost perfect order subsets, i.e the Going-Up Theoren in [1] can be applied to almost POS groups.*

Proof. Let $(x, y) \in \hat{G}$, where x is an element of $(\mathbb{Z}_{p^{a+1}})^2$ and y is an element of M. Let d be the order of (x, y). We prove this lemma from two cases.

Case 1: We can assume that d is not divisible by p^{a+1}. Since G is almost POS, then by Lemma 2.0.3, the cardinality of the order subset of $\hat{G}$ determined by (x, y) divides $2 \cdot |\hat{G}|$.

Case 2: Suppose d is divisible by p^{a+1}. Then we have that the order of x in $(\mathbb{Z}_{p^{a+1}})^2$ is exactly p^{a+1}, and we can factor d as $p^{a+1}m$, where m is the order of y in M. Next, we let k be the number of elements in M that have order m. By Lemma 5.2.9, we know the total number of elements of order d is $(p^a)^2(p^2 -$

$1)k$. Lemma 5.2.9 tells us that the number of elements in G having order $p^a m$ is $(p^{a-1})^2(p^2-1)k$, which divides $2|G|$ since G is almost POS, Since $|\hat{G}| = p^2|G|$, it follows that $p^2(p^{a-1})^2(p^2-1)k = (p^a)^2(p^2-1)k$ divides $|\hat{G}|$.

□

Similarly, the Chopping-Off Theorem holds in the case of almost POS groups.

Lemma 5.2.11. *Suppose that G has almost perfect order subsets and that $G \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times ...\mathbb{Z}_{p^{a_{s-1}}} \times (\mathbb{Z}_{p^{a_s}})^2 \times M$, where p is a prime not dividing $|M|$ and $a_1 \leq a_2 \leq ... \leq a_{s-1} < a_s$ are positive integers. Then $\hat{G} \cong (\mathbb{Z}_{p^{a_s}})^2 \times M$ also has almost perfect order subsets.*

Proof. Let $(x, y) \in \hat{G}$, with x an element of $(\mathbb{Z}_{p^{a_s}})^2$ and y an element of M. So the order of (x, y) can be factored as $p^b m$ with $b \leq a_s$, where p^b is the order of x and m is the order of y. Also, suppose that $p^c k$, where p does not divide k, is the number of elements in M that have order m. Then by Lemma 5.2.9, the number of elements in $\hat{G}$ that have order $p^b m$ is $(p^2-1)(p^{b-1})^2 \cdot p^c k$.

Next, we intend to show $(p^2-1)(p^{b-1})^2 \cdot p^c k$ is a divisor of $2 \cdot |\hat{G}|$. We calculate the number of elements in $\hat{G}$ of order $p^{a_s} m$ to be $p^a(p^2-1)(p^{a_s-1})^2 \cdot p^c k$, where $a = \sum_{i=1}^{s-1} a_i$. This number divides $2 \cdot |G|$ since G is almost POS. We conclude that $(p^2-1)k$ is a divisor of $|M|$. Thus $(p^2-1)(p^{b-1})^2 \cdot p^c k$ divides $2 \cdot |\hat{G}|$, hence $\hat{G}$ has perfect order subsets. □

The Going-Down Theorem is also true for almost POS groups. This is a corollary of Lemma 5.2.11.

Lemma 5.2.12. *Suppose that G has almost perfect order subsets and that $G \cong (\mathbb{Z}_{p^a})^2 \times M$, where p is a prime not dividing $|M|$. Then $\hat{G} \cong (\mathbb{Z}_p)^2 \times M$ also has almost perfect order subsets.*

Theorem 5.2.13 (Z.). *Let G be a group such that* $G \cong \mathbb{Z}_{2^c 3^d m} \rtimes_\phi \mathbb{Z}_{2^e 3^f} (e, f \geq 1)$, *and* a, b *are generators of* $\mathbb{Z}_{2^c 3^d m}$ *and* $\mathbb{Z}_{2^e 3^f}$, *respectively.* $\phi_b(a) = a^{-1}$. *If G is a POS group, G has to be the following case:*

$$c < e - 1, d \neq f.$$

Further, in order to be ba POS group, G has to be in the form

$$\mathbb{Z}_{3^f} \times ((\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{7^n}) \rtimes \mathbb{Z}_{2^e})$$

Proof. Let $m = q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$, where $q_i \neq 2$ or 3 for all $1 \leq i \leq k$, and the q_i are primes. Then $G \cong \mathbb{Z}_{2^c 3^d m} \rtimes_\phi \mathbb{Z}_{2^e 3^f} \cong \mathbb{Z}_{3^f} \times ((\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}}) \rtimes \mathbb{Z}_{2^e})$.

Case 1: Suppose $c \geq e$. Then we count the number of elements of order 2^e, i.e. $|OS(2^e)|$. Let $G' \cong (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}}) \rtimes \mathbb{Z}_{2^e}$ and $(x, y) \in G'$. Then $o(x, y) = 2^e$ if $y \notin \ker(\phi)$. There are $2^{e-1} 2^c 3^d q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$ of such ordered pairs. If $y \in \ker(\phi)$, then $o(x, y) = 2^e$ if $o(x) = 2^e$ in $\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}}$. There are $2^{e-1} 2^{e-1} = 2^{2e-2}$ of them. Adding them together, we have $2^{e+c-1} 3^d m + 2^{2e-2}$ elements in G'. By the definition of POS-groups, we need to have $2^{e+c-1} 3^d m + 2^{2e-2}$ divide $|G| = 2^{e+c} 3^{f+d} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$, which is equivalent to having

$$2^{2e-2} (2^{c-e+1} 3^d q_1^{n_1} q_2^{n_2} ... q_k^{n_k} + 1) \mid 2^{e+c} 3^{f+d} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}.$$

It is true if $2^{c-e+1} 3^d q_1^{n_1} q_2^{n_2} ... q_k^{n_k} + 1$ divides $2^{c-e+2} 3^{f+d} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$. This is not possible since $2^{c-e+2} 3^{f+d} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$ is a multiple of 2^{c-e+2}, while 2^{c-e+2} cannot divide $2^{c-e+1} 3^d q_1^{n_1} q_2^{n_2} ... q_k^{n_k} + 1$. Therefore, G does not have perfect order subsets when $c \geq e$.

Case 2: Suppose $c = e - 1$ and $f = d$. Then $G \cong \mathbb{Z}_{3^f} \times ((\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^f} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}}) \rtimes \mathbb{Z}_{2^{c+1}})$. In G, there are 8 elements of order 3, and by Lemma

5.2.9, there are $3 \cdot 2^{2c-2}$ elements of order 2^c and $q_1 - 1$ elements of order q_1. We then have that the number of elements of order $3 \cdot 2^c \cdot q_1$ is $8 \cdot 3 \cdot 2^{2c-2} \cdot (q_1 - 1) = 2^{2c+2} \cdot [(q_1 - 1)/2]$. But $2^{2c+2} \cdot [(q_1 - 1)/2]$ does not divide $|G| = 2^{2c+1} 3^{2f} q_1^{n_1} q_2^{n_2} ... q_k n_k$ since $2^{2c+2} > 2^{2c+1}$. Therefore, G does not have perfect order subsets in this case.

Case 3: Suppose $c < e - 1$ and $f = d$. We know $y \notin \ker(\phi)$ if and only if $o(y) = 2^e$ in $\mathbb{Z}_{2^e}$, and $o(x, y) = 2^e$ in G' when $y \notin \ker(\phi)$. Let $(z, x, y) \in G$, where z is an element in $\mathbb{Z}_{3^f}$, x is an element in $\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}}$, and y is an element in $\mathbb{Z}_{2^e}$. If $y \notin \ker(\phi)$, $o(z, x, y) = 3^i 2^e$ for some i, with $1 \leq i \leq d = f$. For each i, there are $2 \cdot 3^{i-1} \cdot 2^{e-1} \cdot 2^c \cdot 3^d \cdot q_1^{n_1} \cdot q_2^{n_2} \cdot ... \cdot q_k^{n_k}$ elements of order $3^i 2^e$. This number divides $|G|$, so we only need to consider (z, x, y) when $o(y) \neq 2^e$ in $\mathbb{Z}_{2^e}$. All elements of this property form an abelian subgroup of G:

$$\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}} \times \mathbb{Z}_{2^{e-1}}).$$

If G is a POS group, $\bar{G}$ has to be an almost POS group, as previously defined in this section.

By Lemma 5.2.10, Lemma 5.2.11 and Lemma 5.2.12, we know if $\bar{G}$ has almost perfect order subsets, then $\bar{G}' \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} ... \times \mathbb{Z}_{q_k}$ is almost POS too. However, $\bar{G}'$ has 8 elements of order 3, and 8 is not a divisor of $2|\bar{G}'|$. Therefore, $\bar{G}'$ is not an almost POS group, which comes to the conclusion that $\bar{G}$ cannot be almost POS. So G is not POS when $c < e - 1$ and $f = d$.

Case 4: Suppose $c = e - 1$ and $f \neq d$. We can first let $f < d$. Similar to Case 3, we want $\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}} \times \mathbb{Z}_{2^{e-1}})$ to be an almost POS group. In $\bar{G}$, the number of elements of order $2^c 3^{\max\{f,d\}} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$ is

$$2^{2c-1} 3^{f+d-1} (q_1 - 1) q_1^{n_1 - 1} (q_2 - 1) q_2^{n_2 - 1} ... (q_k - 1) q_k^{n_k - 1}.$$

If the number of elements of order $2^c 3^{\max\{f,d\}} q_1^{n_1} q_2^{n_2} ... q_k^{n_k}$ can divide $2|\bar{G}|$, k has to be equal to 1 and $q = 7$. So $\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{7^n} \times \mathbb{Z}_{2^c})$. By Lemma 5.2.9, we have that in $\bar{G}$, there are $(3 \cdot 2^{2c-2}$ elements of order 2^c and $8 \cdot 3^{2f-2}$ elements of order 3^f. Then, the number of elements of order $2^c \cdot 3^f \cdot 7^n$ equals $(3 \cdot 2^{2c-2})(8 \cdot 3^{2f-2})(6 \cdot 7^{n-1}) = 2^{2c+2} \cdot 3^{2f} \cdot 7^{n-1}$. But $2^{2c+2} \cdot 3^{2f} \cdot 7^{n-1}$ cannot divide $|G| = 2^{2c} \cdot 3^{f+d} \cdot 7^n$. Therefore, G is not POS in this case.

When $f > d$, the proof is similar since $\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}} \times \mathbb{Z}_{2^{e-1}})$ is an abelian direct product.

The only situation left is $c < e - 1$ and $f \neq d$. So, if $G \cong \mathbb{Z}_{2^c 3^d m} \rtimes_\phi \mathbb{Z}_{2^e 3^f}$ has perfect only subset, it has to be this case. Next we discuss the form of G if G is a POS group.

Case 5: Suppose $c < e - 1$ and $f \neq d$. Without loss of generality, we can assume that $f < d$. By Lemma 5.2.11, we have if $\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} ... \times \mathbb{Z}_{q_k^{n_k}} \times \mathbb{Z}_{2^{e-1}})$ is almost POS, $\bar{G}' \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} ... \times \mathbb{Z}_{q_k}$ is almost POS too. In $\bar{G}\prime$, there are $2 \cdot (q_1 - 1)(q_2 - 1)...(q_k - 1)$ elements of order $2 \cdot 3 \cdot q_1 q_2 ... q_k$, and so $2 \cdot (q_1 - 1)(q_2 - 1)...(q_k - 1)$ divides $2|\bar{G}'| = 12 \cdot q_1 q_2 ... q_k$. So $k = 1$ and $q = 7$ and $\bar{G} \cong \mathbb{Z}_{3^f} \times (\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{7^n} \times \mathbb{Z}_{2^{e-1}})$. By Lemma 5.2.9, we have that in $\bar{G}$, there are $3 \cdot 2^{2c-2}$ elements of order 2^c and $8 \cdot 3^{2f-2}$ elements of order 3^f, and the number of elements of order $2^c \cdot 3^f \cdot 7^m$ is $(3 \cdot 2^{2c-2})(8 \cdot 3^{2f-2})(6 \cdot 7^{n-1})$. Then $\bar{G}$ is almost POS if

$$(3 \cdot 2^{2c-2})(8 \cdot 3^{2f-2})(6 \cdot 7^{n-1}) \mid 2 \cdot |\bar{G}| = 2^{e+c} \cdot 3^{f+d} \cdot 7^n.$$

This is always true whenever $c < e - 1$ and $f \neq d$. Therefore, in order for $\bar{G}$ to be almost POS and G to be POS, $G \cong \mathbb{Z}_{3^f} \times ((\mathbb{Z}_{2^c} \times \mathbb{Z}_{3^d} \times \mathbb{Z}_{7^n}) \rtimes \mathbb{Z}_{2^e})$.

$\square$

CHAPTER 6

OPEN QUESTIONS

Though this research has been fruitful in terms of results, many interesting questions remain unsolved. These investigations mainly focused on the constructions of semidirect products with perfect order subsets. But we know little about the relationship of the two groups that are factors in semidirect product POS groups or the existence of actions other than inversion that can make groups such as $\mathbb{Z}_{p^m} \rtimes_\phi \mathbb{Z}_{2^n}$ POS.

I conclude with a brief list of open questions:

- Let G be a group such that $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_n$, and a, b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively. If $\phi_b(a) = a^{-1}$ and m is a multiple of n, is it possible for G to be a POS group?
- Let G be a group such that $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_{2^n}$, and a, b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_{2^n}$, respectively. If $\phi_b(a) \neq a^{-1}$ and $\phi_b(a) \neq a$, is it possible for G to have perfect order subsets?
- Let G be a group such that $G \cong \mathbb{Z}_m \rtimes_\phi \mathbb{Z}_{2^n}$, and a, b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_{2^n}$, respectively. If $o(\phi_b(a)) \neq 2$, can G have perfect order subsets?
- Let G be a group such that $G \cong \mathbb{Z}_{2^m} \times (\mathbb{Z}_{7^n} \rtimes_\phi \mathbb{Z}_{3^l}$. a, b are generators of $\mathbb{Z}_{7^n}$ and $\mathbb{Z}_{3^l}$, respectively. If $\phi_b(a) \neq a^2$, is G POS?

APPENDIX A

SEMIDIRECT PRODUCTS WITH NON-INVERSIONS

When semidirect products have non-inversion actions, perfect order subsets can still occur. We can support this by examining the following cases.

Theorem A.0.14 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_{3^p} \times (\mathbb{Z}_{2^m} \rtimes_\phi \mathbb{Z}_{2^n})$. a,b are generators of $\mathbb{Z}_2^m$ and $\mathbb{Z}_2^n$, and $\phi_b(a) = a^{1+2^{m-1}}$. Then G is a POS-group.*

Before we start to verify it, I would like to introduce a theorem that will be useful to the proof:

Theorem A.0.15. *Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements, where d is the greatest common divisor of n and s.* *[64, Fraileigh]*

Proof of Theorem A.0.14. Let $(a^l, b^k) \in \mathbb{Z}_{2^m} \rtimes_\phi \mathbb{Z}_{2^n}$. We may write $l = 2^r\alpha$, $k = 2^s\beta$, where $0 \le r \le m$, $0 \le s \le n$, $2 \nmid \alpha$, and $2 \nmid \beta$. Then the order of b^k in $\mathbb{Z}_{2^n}$ is 2^{n-s}. By calculation, we have

$$\phi_{b^k}(a^l) = a^{l(1+2^{m-1})^k} \qquad \textbf{(1.1)}$$

. Repeated application of **(1.1)** indicates $(a^l, b^k)^{2^{n-s}} = (a^\gamma, e_b)$, where

$$\gamma = l[1 + (1+2^{m-1})^k + (1+2^{m-1})^{2k} + ... + (1+2^{m-1})^{2^{n-s}k-1}]$$

This is a geometric series and equal to

$$\gamma = l\frac{(1+2^{m-1})^{2^n\beta}-1}{(1+2^{m-1})^{2^s\beta}-1} = 2^r\alpha\,\frac{(1+2^{m-1})^{2^n\beta}-1}{(1+2^{m-1})^{2^s\beta}-1}.$$

We have $(1+2^{m-1})^{2^n\beta}-1 = [1+\binom{2^n\beta}{1}2^{m-1}+\binom{2^n\beta}{2}(2^{m-1})^2+...+\binom{2^n\beta}{2^n}(2^{m-1})^{2^n\beta}] - 1 = \sum_{i=1}^{2^n\beta}\binom{2^n\beta}{i}(2^{m-1})^i = 2^{m-1}2^n\beta u$, where u is an odd positive integer. Similarly, $(1+2^{m-1})^{2^s\beta}-1 = 2^{m-1}2^s\beta v$ and v is an odd positive integer. Since $2^s\beta$ is a divisor of $2^n\beta$, $(1+2^{m-1})^{2^s\beta}-1$ divides $(1+2^{m-1})^{2^n\beta}-1$. Hence $\gamma = 2^r2^{n-s}w$, where w is a positive odd integer.

If $m-r \le n-s$, that is, $m \le n+r-s$, $\gamma = 2^r2^{n-s}w \equiv 0\,(mod\,2^m)$. Therefore $o(a^l,b^k) = 2^{n-s}$.

If $m-r > n-s$, $\gamma = 2^r2^{n-s}w \not\equiv 0,(mod\,2^m)$. Then $o(a^\gamma,e_b) = 2^{m-r-n+s}$. So $o(a^l,b^k) = 2^{n-s}2^{m-r-n+s} = 2^{m-r}$.

Let's compare this situation to the corresponding direct product: $(a^l,b^k) \in \mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n}$. By Theorem A.0.15 and the fact that $\max\{\frac{2^m}{gcd(l,2^m)},\frac{2^n}{gcd(k,2^n)}\} = 2^s$, $o(a^l,b^k) = 2^{n-s}$ if $m-r \le n-s$. Similarly, $o(a^l,b^k) = 2^{m-r}$ if $m-r > n-s$. So the orders of element in $\mathbb{Z}_{2^m}\rtimes_\phi\mathbb{Z}_{2^n}$ correspond to the orders of elements in $\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n}$. Therefore, instead of counting the number of elements of a given order in G, we can count them in $G' \cong \mathbb{Z}_{3^p}\times(\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n})$.

Without loss of generality, we assume $n \ge m$. In $G' \cong \mathbb{Z}_{3^p}\times(\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n})$, when $0 \le i \le p, 1 \le j \le m$, $|OS(3^i2^j)|$ is equal to the multiplication of $\Phi(3^i)$ and the number of elements of order 2^j in $\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n}$. By Lemma 5.2.9, there are $3\cdot 2^{2j-2}$ ordered pairs of order 2^j in $\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n}$. Therefore, there are $\Phi(3^i)\cdot 3\cdot 2^{2j-2} = 3^i2^{2j-1}$ elements of order 3^i2^j in G.

Next we count the number of ordered triples of order 3^i2^j when $0 \le i \le p$ and $m < j \le n$. There are $\Phi(3^i) = 2\cdot 3^{i-1}$ elements of order 3^i in $\mathbb{Z}_{3^p}$. In $\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n}$, we count ordered pairs with elements of order 2^j in the second position and any element in the first position since $j > m$. There are $2^m\Phi(2^j)$ such choices. So, there are $3^{i-1}2^{m+j}$ elements of order 3^i2^j.

We can now make the following table:

Orders of Elements	Cardinalities of Order Subsets
1	1
$2^j(1 \le j \le \min\{m,n\})$	$3 \cdot 2^{2j-2}$
$2^j(\min\{m,n\}+1 \le j \le \max\{m,n\})$	$2^{\min\{m,n\}} \cdot 2^{j-1}$
$3^i(1 \le i \le p)$	$2 \cdot 3^{i-1}$
$3^i 2^j(1 \le i \le p, 1 \le j \le \min\{m,n\})$	$3^i 2^{2j-1}$
$3^i 2^j(1 \le i \le p, \min\{m,n\}+1 \le j \le \max\{m,n\})$	$3^{i-1} 2^{\min\{m,n\}+j}$

Table A.1

It is easy to see that $G\prime \cong \mathbb{Z}_{3^p} \times (\mathbb{Z}_{2^m} \rtimes_\phi \mathbb{Z}_{2^n})$ is a POS-Group. Therefore,$G \cong \mathbb{Z}_{3^p} \times (\mathbb{Z}_{2^m} \rtimes_\phi \mathbb{Z}_{2^n})$ is a POS-group.

□

The above theorem can be further generalized.

Theorem A.0.16 (Z.). *Let G be a group such that $G \cong \mathbb{Z}_{3^p} \times (\mathbb{Z}_{2^m} \rtimes_\phi \mathbb{Z}_{2^n})$. a,b are generators of $\mathbb{Z}_{2^m}$ and $\mathbb{Z}_{2^n}$, respectively; and $\phi(b) = a^{1+2^{m-1}+2^{m-2}+...+2^{m-i}}$, where $0 \le i \le \min\{m-1, n-1\}$. Then G is a POS-group.*

Proof. Let $(a^l, b^k) \in \mathbb{Z}_{2^m} \times_\phi \mathbb{Z}_{2^n}$. We may write $l = 2^r\alpha$, $k = 2^s\beta$, where $0 \le r \le m$, $0 \le s \le n$, $2 \nmid \alpha$, and $2 \nmid \beta$. Similar to the previous proof, we have $(a^l, b^k)^{2^{n-s}} = (a^\gamma, e_b)$, where

$$\gamma = l\,\frac{(1+2^{m-1}+...+2^{m-i})^{2^n\beta}-1}{(1+2^{m-1}+...+2^{m-i})^{2^s\beta}-1} = 2^r\alpha\,\frac{(1+2^{m-1}+...+2^{m-i})^{2^n\beta}-1}{(1+2^{m-1}+...+2^{m-i})^{2^s\beta}-1}.$$

Then $(1+2^{m-1}+...+2^{m-i})^{2^n\beta}-1 = 2^{m-i}2^n u$ and $(1+2^{m-1}+...+2^{m-i})^{2^s\beta}-1 = 2^{m-i}2^s v$, where u and v are two positive odd integers. We can have $\gamma = 2^r 2^{n-s} w$, where w is a positive odd integer.

The rest is the same as in Theorem A.0.14. So G in this case has perfect order subsets.

$\square$

APPENDIX B

SEMIDIRECT PRODUCTS WITH THE QUATERNION GROUP

First, I will consider the definition of the quaternion group as well as its important properties that will be used in the theorems in this secion.

The quaternion group is a non-abelian group of order eight, isomorphic to a certain eight-element subset of the quaternions under multiplication. It is often denoted by Q or Q_8, and is given by the group presentation: $Q = \langle -1, i, j, k | (-1)^2 = 1, i^2 = j^2 = k^2 = -1 \rangle$, where 1 is the identity element and -1 commutes with the other elements of the group.[8]

Property B.0.17. *The elements i,j,k are all of order 4 and any two of them can generate Q_8. So another notation for Q_8 is $Q_8 = \langle i, j | i^2 = j^2, j^{-1}ij = i^{-1} \rangle$.* [9]

Property B.0.18. *Every element in Q_8 can be uniquely written as $i^\alpha j^\beta$, where $0 \leq \alpha \leq 3$ and $\beta \in \{0, 1\}$.* [10]

With the help of properties above, we can invesitigate POS of semidirect products with the quaternion group.

Theorem B.0.19 (Z.). *Let $G \cong Q_8 \rtimes_\phi \mathbb{Z}_{3^n}$, and c is the generator of $\mathbb{Z}_{3^n}$. If $\phi(c) = \psi_c$, where $\psi_c(i) = j$, and $\psi_c(j) = ij$, then G has perfect order subsets.*

Proof. First, we show that for $x \in \mathbb{Z}_{3^n}$, $o(x) \neq 3^n$ if and only if $x \in \ker(\phi)$.

If $o(x) = 3^n$, then $\mathbb{Z}_{3^n} = \langle x \rangle = \langle 1 \rangle$. So $\phi(1) \in \ker(\phi)$ and therefore $y \in \ker(\phi)$ for all $y \in \mathbb{Z}_{3^n}$. This is not possible.

If $o(x) \neq 3^n$, then $x = c^{3^\alpha y}$, where $1 \leq \alpha < n$ and $3 \nmid y$. Then $\phi(c^3) = \psi_{c^3}$, and $\psi_{c^3}(i) = \psi_c(\psi_c(\psi_c(i))) = \psi_c(\psi_c(j)) = \psi_c(ij) = \psi_c(i)\psi_c(j)$, since ψ_c is an automorphism. Further $\psi_c(i)\psi_c(j) = jij = i$. For a similar reason, $\psi_{c^3}(j) = j$. So $c^3 \in \ker(\phi)$. Also, we have $x = c^{3^\alpha y} \in \langle c^3 \rangle$, and therefore $x \in \ker(\phi)$.

From $c^3 \in \ker(\phi)$, we know $o(\psi_c) = 3$. Therefore $\langle \psi_c \rangle \cong \mathbb{Z}_3$. For c^k such that $3 \nmid k$, $\psi_{c^k}(i)$ is $\psi_c(i)$ or $\psi_c^{-1}(i)$. Similarly, $\psi_{c^k}(j)$ is $\psi_c(j)$ or $\psi_c^{-1}(j)$.

Every element in Q_8 can be expressed as $i^p j^q$, where $p = 0, 1, 2, 3$ and $q = 0, 1$. Let $(i^p j^q, c^k) \in G \cong Q_8 \rtimes_\phi \mathbb{Z}_{3^n}$. Since if $c^k \in \ker(\phi)$, the order of $(i^p j^q, c^k)$ would be easy to calculate, here we only consider the case when $o(c^k) = 3^n$. There are $\Phi(|\mathbb{Z}_{3^n}|) = \Phi(3^n) = 2 \cdot 3^{n-1}$ such c^k, where Φ is the Euler Phi Function. We separate it into four cases, depending on ψ_{c^k} and q:

Case 1: When $\psi_{c^k} = \psi_c$ and $q = 0$.Then $\psi_{c^k}(i) = \psi_c(i) = j$ and $\psi_{c^k}(j) = \psi_c(j) = ij$. We have

$$(i^p, c^k)^{3^n} = (i^p \psi_{c^k}(i^p) \psi_{c^{2k}}(i^p)..\psi_{c^{(3^n-1)k}}(i)^p, 0)$$

$$= (i^p j^p (ij)^p i^p j^p (ij)^p ... i^p j^p (ij)^p, 0) = ((i^p j^p (ij)^p)^{3^{n-1}}, 0).$$

We consider four subcases:

- If $p = 0$, then $i^p = j^p = (ij)^p = 1$ and $i^p j^p (ij)^p = 1$. So $((i^p j^p (ij)^p)^{3^{n-1}}, 0) = (1, 0)$, which is the identity of $Q_8 \rtimes_\phi \mathbb{Z}_{3^n}$. So $o(i^p, c^k) = 3^n$, since $o(c^k) = 3^n$.

- If $p = 1$, we have $i^p = i$, $j^p = j$ and $(ij)^p = ij$. So $i^p j^p (ij)^p = ij(ij) = -1$. Then $((i^p j^p (ij)^p)^{3^{n-1}}, 0) = (-1, 0)$. We further have $o(i^p, c^k) = 2 \cdot 3^n$.

- If $p = 2$, then $i^p = -1$, $j^p = -1$ and $(ij)^p = -1$. $i^p j^p (ij)^p = ij(ij) - 1$. Hence $((i^p j^p (ij)^p)^{3^{n-1}}, 0) = (-1, 0)$, and $o(i^p, c^k) = 2 \cdot 3^n$.

- If $p = 3$, $i^p = -i$, $j^p = -j$ and $(ij)^p = -(ij)$. $i^p j^p (ij)^p = -ij(ij) = 1$. We have $((i^p j^p (ij)^p)^{3^{n-1}}, 0) = (1, 0)$ and $o(i^p, c^k) = 3^n$.

Case 2: When $\psi_{c^k} = \psi_c$ and $q = 1$.

$$(i^p j, c^k)^{3^n} = (i^p j \psi_{c^k}(i^p j) \psi_{c^{2k}}(i^p j) .. \psi_{c^{(3^n-1)k}}(i^p j), 0)$$

$$= (i^p(j) \cdot j^p(ij) \cdot (ij)^p(i) \cdot i^p(j) \cdot (j)^p(ij) \cdot (ij)^p(i) ... i^p(j) \cdot j^p(ij) \cdot (ij)^p(i), 0)$$

$$= ((i^p(j) \cdot j^p(ij) \cdot (ij)^p(i))^{3^{n-1}}, 0).$$

Similar to Case 1, we also divide it into four small cases:

- When $p = 0$, $i^p = j^p = (ij)^p = 1$. So $i^p(j) \cdot j^p(ij) \cdot (ij)^p(i) = -1$, which indicates $((i^p(j) \cdot j^p(ij) \cdot (ij)^p(i))^{3^{n-1}}, 0) = (-1, 0)$. We have $o(i^p(j), c^k) = 2 \cdot 3^n$.

- When $p = 1$, $i^p(j) = ij$, $j^p(ij) = j(ij) = i$ and $(ij)^p(i) = ij(i) = j$. We have $i^p(j) \cdot j^p(ij) \cdot (ij)^p(i) = (ij)ij = -1$. Then $((i^p(j) \cdot j^p(ij) \cdot (ij)^p(i))^{3^{n-1}}, 0) = (-1, 0)$.We have $o(i^p, c^k) = 2 \cdot 3^n$.

- When $p = 2$, $i^p(j) = -j$, $j^p(ij) = -ij$ and $(ij)^p(i) = -i$. $i^p(j) \cdot j^p(ij) \cdot (ij)^p(i) = -j(ij)i = 1$. Then $((i^p(j) \cdot j^p(ij) \cdot (ij)^p(i))^{3^{n-1}}, 0) = (1, 0)$. $o(i^p, c^k) = 3^n$.

- When $p = 3$, $i^p(j) = -ij$, $j^p(ij) = -jij = -i$ and $(ij)^p(i) = -iji = -j$. $i^p(j) \cdot j^p(ij) \cdot (ij)^p(i) = 1$. We have $((i^p(j) \cdot j^p(ij) \cdot (ij)^p(i))^{3^{n-1}}, 0) = (1, 0)$ and $o(i^p, c^k) = 3^n$.

So when $\psi_{c^k} = \psi_c$, $(1, c^k)$, (i^3, c^k), $(i^2 j, c^k)$, and $(i^3 j, c^k)$ are of order 3^n, while (i, c^k), (i^2, c^k), (j, c^k), and (ij, c^k) are of order $2 \cdot 3^n$. So we have $4 \cdot 3^{n-1}$ elements of order 3^n and $4 \cdot 3^{n-1}$ elements of order $2 \cdot 3^n$.

We can use the similar reasoning to calculate the order of (i^p, c^k) when $\psi_{c^k} = (\psi_c)^{-1}$:

Case 3: When $\psi_{c^k} = (\psi_c)^{-1}$ and $q = 0$. Then $\psi_{c^k}(i) = \psi_{c^2}(i) = ij$ and $\psi_{c^k}(j) = \psi_{c^2}(j) = i$. We have

$$(i^p, c^k)^{3^n} = (i^p \psi_{c^k}(i^p) \psi_{c^{2k}}(i^p)..\psi_{c^{(3^n-1)k}}(i^p), 0)$$

$$= (i^p (ij)^p (j)^p (i)^p (ij)^p (j)^p ...(i)^p (ij)^p (j)^p, 0) = ((i^p (ij)^p (j)^p)^{3^{n-1}}, 0)$$

.

- If $p = 0$, then $i^p = j^p = (ij)^p = 1$. So $j^p (ij)^p (i)^p = 1$ and $o(i^p, c^k) = 3^n$.
- If $p = 1$, we have $i^p = i$, $j^p = j$ and $(ij)^p = ij$. Therefore, $j^p (ij)^p (i)^p = ij(ij) = -1$. So $o(i^p, c^k) = 2 \cdot 3^n$.
- If $p = 2$, we have $j^p = -1$, $(ij)^p = -1$ and $i^p = -1$. It follows that $j^p (ij)^p i^p = -1$. $o(i^p, c^k) = 2 \cdot 3^n$.
- If $p = 3$, then $i^p = -i$, $j^p = -j$ and $(ij)^p = -ij$. $j^p (ij)^p i^p = 1$. We have $o(i^p, c^k) = 3^n$.

Case 4: When $\psi_{c^k} = (\psi_c)^{-1}$ and $q = 1$.

$$(i^p j, c^k)^{3^n} = (i^p j \psi_{c^k}(i^p j) \psi_{c^{2k}}(i^p j)..\psi_{c^{(3^n-1)k}}(i^p j), 0)$$

$$= (i^p (j) \cdot (ij)^p (i) \cdot (j)^p (ij) \cdot i^p (j) \cdot (ij)^p (i) \cdot (j)^p (ji)...i^p (j) \cdot (ij)^p (i) \cdot (j)^p (ij), 0)$$

$$= ((i^p (j) \cdot (ij)^p (i) \cdot j^p (ij))^{3^{n-1}}, 0).$$

- If $p = 0$, $i^p = j^p = (ij)^p = 1$. We have $o(i^p(j), c^k) = 2 \cdot 3^n$.
- If $p = 1$, then $i^p(j) = ij$, $(ij)^p i = iji = j$ and $j^p(ij) = jij = i$. $i^p(j) \cdot (ij)^p (i) \cdot (j)^p (ij) = 1$. We have $o(i^p, c^k) = 3^n$.

- If $p = 2$, then $i^p(j) = -j$, $(ij)^p(i) = -i$ and $(j)^p(ij) = -ij$. Hence $o(i^p, c^k) = 3^n$.

- If $p = 3$, then $i^p(j) = -ij$, $(ij)^p(i) = -j$ and $(j)^p(ij) = -i$. Therefore, we have $(-ij)(-j)(-i) = -1$ and $o(i^p, c^k) = 2 \cdot 3^n$.

When $\psi_{c^k} = (\psi_c)^{-1}$, $(1, c^k)$, (i^3, c^k), $(i^2 j, c^k)$, and $(i^3 j, c^k)$ are of order 3^n. (i, c^k), (i^2, c^k), (j, c^k), and (ij, c^k) are of order $2 \cdot 3^n$. Therefore, $4 \cdot 3^{n-1}$ elements are of order 3^n and $4 \cdot 3^{n-1}$ elements of order $2 \cdot 3^n$.

Considering all cases, in $G \cong Q_8 \rtimes_\phi \mathbb{Z}_{3^n}$, there are always $8 \cdot 3^{n-1}$ elements of order 3^n and $8 \cdot 3^{n-1}$ of order $2 \cdot 3^n$.

Now, we calculate orders of elements $(i^p j^q, c^k)$, when $3 \nmid k$. When $3|k$, $c^k \in \ker(\phi)$. Then $(i^p j^q, c^k)$ acts the same way as in the direct product $Q_8 \times_\phi \mathbb{Z}_{3^n}$. In Q_8, there is one element of order 1, one element of order 2 and six elements of order 4. In $\mathbb{Z}_{3^n}$, the order of every element, other than the identity and those of order 3^n is in form 3^i, with $1 \leq i \leq n-1$. And there are $\Phi(3^i) = 2 \cdot 3^{i-1}$ elements of order 3^i.

From the above information, we have the table on the next page:

Orders of Elements	Cardinalities of Order Subsets
1	1
2	1
4	6
$3^i(1 \leq i \leq n-1)$	$2 \cdot 3^{i-1}$
$2 \cdot 3^i(1 \leq i \leq n-1)$	$2 \cdot 3^{i-1}$
$4 \cdot 3^i \ (1 \leq i \leq n-1)$	$4 \cdot 3^i$
3^n	$8 \cdot 3^{n-1}$
$2 \cdot 3^n$	$8 \cdot 3^{n-1}$

Table B.1

Every number in the right column can divide $|G| = 8 \cdot 3^n$, i.e. the number of elements of every given order can divide the size of the whole group. Therefore, $G \cong Q_8 \rtimes_\phi \mathbb{Z}_{3^n}$ is POS. $\square$

APPENDIX C

GAP CODE

```
OrderFrequency:=function(g)
local h,w;
w := [ ];
w := h-> Collected(List(Elements(h), Order));
return w(g);
end;


POS:=function(n)
  local i, j, p, x, Small;
    for i in [1..n] do
      Small:=AllSmallGroups(i);
        for j in Small do
          if not IsAbelian(j) then
            p:=OrderFrequency(j);
            if ForAll(p, x-> i mod x[2] = 0) then
            Print(StructureDescription(j)," (", IdGroup(j),") is non abelian POS
\ n");
```

```
            fi;
          fi;
        od;
    od;
end;
```

References

[1] Carrie E. Finch and Lenny Jones, A Curious Connection Between Fermat Numbers and Finite Groups, *The American Mathemaical Monthly*, June-July 2002, 517-523

[2] Carrie E. Finch and Lenny Jones, Non-abelian Groups with Perfect Order Subsets, *The JP Journal of Algebra, Number Theory, and Applications*, 3(1)(2003), 13-26

[3] GAP software, http://www.gap-system.org/

[4] Ashish Kumar Das, On Finite Groups Having Perfect Order Subsets, *International Journal of Algebra*, Vol.3(2009), NO.13, 629-637

[5] Gallian, Joseph A., *Contemporary Abstract Algebra*, Houghton Mifflin Company, 2002

[6] Nathanson, Melvyn B., *Elementary Methods in Number Theory*, Springer, 2000

[7] Fraleigh, John B., and Victor J. Katz., *A First Course in Abstract Algebra*, Pearson Education, 2003

[8] Quaternion Group, *Wikipedia, the Free Encyclopedia*, http://en.wikipedia.org/wiki/Quaternion_group

[9] Scott, W.R., *Group Theory*, Dover Publication,Inc., 1987

[10] Dicyclic Group, *Wikipedia, the Free Encyclopedia*, http://en.wikipedia.org/wiki/Dicyclic_group

[11] Nguyen Trong Tuan and Bui Xuan Hai, On Perfect Order Subsets in Finite Groups, June 2010

[12] Ashish Kumar Das, POS Groups Revisited, March 2009