GENERALIZED CWATSETS

Daniel Smith

Wabash College
Crawfordsville, IN 47933-0352 U.S.A.

Abstract. We define the gc-set, a generalization of the cwatset, and find some of its basic properties. Then some of the gc-set's group theoretic results are shown.

1. Introduction

In April of 1994, the Mathematics Magazine published an article[1] written by Gary Sherman and Martin Wattenberg which introduced cwatsets and was appropriately titled "Introducing... Cwatsets!" The following definition appeared in that article:

Definition 1.1. *A subset, C, of $\mathbb{Z}_2^n$ is a* ***cwatset*** *if for each element, c, of C, there exists a permutation, σ, of S_n such that $C+c=\sigma(C)$; i.e., C is* ***c****losed* ***w****ith* ***a t****wist.*

Example 1.2. $C=\{000,110,101\}$ is a cwatset since
$C+000=\{000,110,101\}=id(C)$
$C+110=\{110,000,011\}=\{000,110,011\}=(1,2)(C)$
$C+101=\{101,011,000\}=\{000,101,011\}=(1,3)(C)$

Cwatsets have the restriction that they can only be subsets of one kind of group, $\mathbb{Z}_2^n$. In generalizing the cwatset, we place them in a more general group setting.

Definition 1.3. *A subset, H, of a group, G, is a gc-set if for every $h\in H$, there exists $\phi_h : G\to G$, an automorphism, such that $\phi_h(h)\cdot H=\phi_h(H)$.*

The similarities between the definition of gc-sets and that of cwatsets is clear, and suggests that many of the cwatset properties should hold for gc-sets. The following theorem shows that gc-sets are truly a generalization of cwatsets.

Lemma 1.4. *All cwatsets are gc-sets.*

Proof. Let $C\subseteq\mathbb{Z}_2^n$ be a cwatset. Then for each $c\in C$, there exists a permutation π, such that $C+c=\pi(C)$. So $\pi^{-1}(C+c)=C$, and $\pi^{-1}(C)+\pi^{-1}(c)=C$. Since in $\mathbb{Z}_2^n$ each element is its own inverse, and since $\mathbb{Z}_2^n$ is abelian, $\pi^{-1}(c)+C=\pi^{-1}(C)$. Here π^{-1} is an automorphism on $\mathbb{Z}_2^n$, and thus Definition 1.3 is satisfied. □

The following example shows that not all gc-sets are cwatsets.

Example 1.5. Let $G = (\mathbb{Z}_{10}, +)$. Let $H = \{0, 2\}$. Let ϕ represent the identity automorphism and let θ represent the inverse automorphism. Then $\phi(0) \cdot H = \{0, 2\} = \phi(H)$, and $\theta(2) \cdot H = \{8, 0\} = \theta(H)$. Thus H is a gc-set; however, it is not a cwatset since $H \not\subseteq \mathbb{Z}_2^n$.

An important property of cwatsets is the containment of the identity. GC-sets also share this property.

Lemma 1.6. *All gc-sets contain the identity.*

Proof. Let H be a gc-set contained in the group G. Choose $h \in H$. By definition, there is an automorphism $\phi_h \in Aut(G)$ such that $\phi_h(h) \cdot H = \phi_h(H)$. Since $h \in H$, $\phi_h(h) \in \phi_h(H)$. Therefore, $\phi_h(h) \cdot h_1 = \phi_h(h)$ for some $h_1 \in H$. Thus $h_1 = e$, and H contains the identity. □

In 1996, Richard Mohr introduced in his paper, "CWATSETS: Weights, Cardinalities, and Generalizations"[4] a definition of a generalization of the cwatset similar to our definition. While his (H, ϕ) subsets do generalize the cwatset, Mr. Mohr's generalization fails to share several of the important defining properties of cwatsets. For instance, cwatsets always contain the identity, whereas (H, ϕ) subsets need not contain the identity. As a result, (H, ϕ) subsets aren't the projections of an "omega group" as are cwatsets, and thus they don't have the nice analogue of Lagrange's Theorem that we see in cwatsets. GC-sets, however, share all of these properties with cwatsets; therefore, gc-sets seem to be a quite satisfactory generalization.

2. Group Theoretic Analysis of the GC-set.

Since gc-sets are a generalization of cwatsets, it is often useful to look at cwatsets to provide counterexamples and generate ideas for the properties to look for in gc-sets. One useful way to study cwatsets is by looking at the wreath product of S_n and $\mathbb{Z}_2^n$. GC-sets have a nice analogue.

Definition 2.1. *For two elements (ϕ, h), and (θ, g) in $Aut(G) : G$, their* ***product*** *is defined by $(\phi, h)(\theta, g) = (\theta \circ \phi, h\phi^{-1}(g))$.*

The set $Aut(G) \times G$, combined with the binary operation from Definition 2.1 form a group. This group, in conjunction with the following definition, is a quite useful tool for studying gc-sets.

Definition 2.2. *A projection in G of a subgroup P of $Aut(G) : G$ is $\{h | (\phi, h) \in P\}$.*

Lemma 2.3. *Let G be a finite group. Let $P \leq Aut(G) : G$ with projection H. Then $\phi(h) \cdot H = \phi(H)$ for all $(\phi, h) \in P$.*

Proof. Fix an arbitrary $h_0 \in H$ and $\phi_{h_0} \in Aut(G)$ such that $(\phi_{h_0}, h_0) \in P$, and now for each $h \in H$ choose some $\phi_h \in Aut(G)$ such that $(\phi_h, h) \in P$. Since P is a subgroup, $P \supseteq \{(\phi_{h_0}, h_0)(\phi_h, h) | h \in H\} = \{(\phi_h \circ \phi_{h_0}, h_0\phi_{h_0}^{-1}(h)) | h \in H\}$. Since the projection of P is H, $\{h_0\phi_{h_0}^{-1}(h) | h \in H\} \subseteq H$. But $|\{h_0\phi_{h_0}^{-1}(h) | h \in H\}| = |H|$, therefore $\{h_0\phi_{h_0}^{-1}(h) | h \in H\} = H$ for all fixed but arbitrary $h_0 \in H$. Now $\{h_0\phi_{h_0}^{-1}(h) | h \in H\} = h_0\phi_{h_0}^{-1}(H)$. Thus $h_0\phi_{h_0}^{-1}(H) = H$, and $\phi_{h_0}(h_0) \cdot H = \phi_{h_0}(H)$ for all $(\phi_{h_0}, h_0) \in P$. □

Theorem 2.4. *A subset, H, of a finite group G is a gc-set if and only if it is the projection of a subgroup of $Aut(G) : G$.*

Proof. (⇒)Let $H \subseteq G$ be a gc-set, and define a subset $P(H)$ of $Aut(G):G$ by $P(H) = \{(\phi, h) | \phi(h) \cdot H = \phi(H)$ for some $\phi \in Aut(G)$ and some $h \in H\}$. Claim: $P(H)$ is a subgroup of $Aut(G):G$. Since G is finite, it suffices to show that $P(H)$ is closed. Let (ϕ, h),$(\theta, g) \in P(H)$. Recall that $(\phi, h)(\theta, g) = (\theta \circ \phi, h\phi^{-1}(g))$. Then $\theta \circ \phi(h\phi^{-1}(g))H = \theta(\phi(h)\phi(\phi^{-1}(g))) \cdot H = \theta(\phi(h)g) \cdot H = \theta \circ \phi(h)\theta(g) \cdot H$. Since $(\theta, g) \in P(H)$, $\theta(g) \cdot H = \theta(H)$. Therefore, $\theta \circ \phi(h\phi^{-1}(g)) \cdot H = \theta \circ \phi(h)\theta(H) = \theta(\phi(h) \cdot H)$. But $(\phi, h) \in P(H)$ as well, so $\phi(h) \cdot H = \phi(H)$. Now, $\theta \circ \phi(h\phi^{-1}(g)) \cdot H = \theta \circ \phi(H)$, and thus $(\theta \circ \phi, h\phi^{-1}(g)) \in P(H)$, and $P(H)$ is a subgroup of $Aut(G):G$. By the definition of gc-set, for each $h \in H$, there exists an automorphism $\phi \in Aut(G)$ such that $\phi(h) \cdot H = \phi(H)$. Since $P(H)$ contains all ϕ such that $\phi(h) \cdot H = \phi(H)$ for each $h \in H$, $P(H)$ projects onto H.

(⇐) For the converse, let P be a subgroup of $Aut(G):G$. Let H be the projection of P in G. By Lemma 2.3, $\phi(h) \cdot H = \phi(H)$ for all $(\phi, h) \in P$, thus for all h there is a $\phi \in Aut(G)$ such that $\phi(h) \cdot H = \phi(H)$, and H is a gc-set. Now armed with a new way of looking at gc-sets, we begin to attack Lagrange's Theorem. Theorem 2.6 gives us an analogue of Lagrange as a corollary. □

An immediate result of Theorem 2.4 is the fact that the direct product of gc-sets is itself a gc-set.

Corollary 2.5. *Let H_1 and H_2 be gc-sets contained in the groups G_1 and G_2 respectively. Then the direct product, $H_1 \times H_2$, is a gc-set as a subset of the group $G_1 \times G_2$.*

Proof. Since $H_1 \leq G_1$ and $H_2 \leq G_1$ are gc-sets, by Theorem 2.4, there exist subgroups P_1 and P_2 of $Aut(G_1)$:G_1 and $Aut(G_2)$:G_2 such that H_1 is the projection of P_1 and H_2 is the projection of P_2. Now let P be the subgroup of $Aut(G_1 \times G_2)$:$(G_1 \times G_2)$ such that $((\phi, \theta), (h_1, h_2)) \in P$ if and only if $(\phi, h_1) \in P_1$ and $(\theta, h_2) \in P_2$. Then $H_1 \times H_2$ is the projection of P. Thus by Theorem 2.4, $H_1 \times H_2$ is a gc-set as a subset of the group $G_1 \times G_2$. □

Theorem 2.6. *Let G be a finite group. If $P \leq Aut(G):G$, and H is the projection of P in G, then $|H|$ divides $|P|$.*

Proof. Let $P(h) = \{(\phi, h) | \phi(h) \cdot H = \phi(H)$ for some $(\phi, h) \in P\}$. By Lemma 2.3, $P(h) = \{(\phi, h) \in P\}$. Clearly, $P = \cup_{h \in H} P(h)$. Claim: $P(e)$ is a subgroup of P. Let (ϕ, e),$(\theta, e) \in P(e)$. Then $H = \phi(H) = \theta(H)$. Therefore, $\theta \circ \phi(H) = H = e\phi^{-1}(e) \cdot H$. Thus $(\theta \circ \phi, e) \in P(e)$, and $P(e)$, a closed subset of the finite group P, is a subgroup. Claim: $P(h)$ is a left coset of $P(e)$ for each $h \in H$. Fix $(\theta, h) \in P(h)$. Let $(\phi, e) \in P(e)$. $H = \phi(e) \cdot H = \phi(H)$, so $H = \phi(H) = \phi^{-1}(H)$. Now look at $(\theta, h)(\phi, e) = (\phi \circ \theta, h)$. We know that $\theta(h) \cdot H = \theta(H)$, and since $H = \phi^{-1}(H)$, $\theta(h)\phi^{-1}(H) = \theta(H)$. Therefore, $\phi \circ \theta(h) \cdot H = \phi \circ \theta(H)$. Thus $(\phi \circ \theta, h) \in P(h)$. Now let (π, h),$(\sigma, h) \in P(h)$. $(\sigma^{-1}, \sigma(h^{-1}))(\pi, h) = (\pi \circ \sigma^{-1}, \sigma(h^{-1})\sigma(h)) = (\pi \circ \sigma^{-1}, e) \in P(e)$. Assume that two elements in $P(h)$ form different cosets with $P(e)$, i.e. $(\theta, h)P(e) \neq (\sigma, h)P(e)$. Then $(\sigma^{-1}, \sigma(h^{-1}))(\theta, h)P(e) \neq P(e)$, but $(\sigma^{-1}, \sigma(h^{-1}))(\theta, h) \in P(e)$, and therefore $(\sigma^{-1}, \sigma(h^{-1}))(\theta, h)P(e) = P(e)$, a contradiction. Thus any two elements in $P(h)$ form the same left cosets of $P(e)$. Since $P = \cup_{h \in H} P(h)$, $|P : P(e)| = |H|$, and now we have $|P| = |P : P(e)| \cdot |P(e)| = |H| \cdot |P(e)|$. Thus $|H|$ divides $|P|$. □

Corollary 2.7. *Let G be a finite group. Let $H \subseteq G$ be a gc-set. Then $|H|$ divides $|Aut(G)| \cdot |G|$.*

Proof. By theorem 2.6, $|H|$ divides $|P|$ where P is a subgroup of $Aut(G){:}G$ such that H is the projection of P in G. By Lagrange's Theorem, $|P|$ divides $|Aut(G) : G| = |Aut(G)| \cdot |G|$. Thus $|H|$ divides $|Aut(G)| \cdot |G|$. □

We now have an analogue of Lagrange's theorem in finite group theory. The result isn't quite as strong as its group theoretical counterpart, but that should come as no surprise since a subgroup is only a special case of a gc-set. The reader should note the similarities between the Lagrange analogue for gc-sets and that of cwatsets given in "Introducing... Cwatsets!"[1] These similarities help show that the gc-set is a nice generalization of the cwatset.

Example 2.8. Recall that $H = \{000, 110, 101\}$, a subset of $\mathbb{Z}_2^3$, is a gc-set. Now $|H| = 3$, but $|\mathbb{Z}_2^3| = 8$. Now we know from Corollary 2.7 that $|H|$ divides $|Aut(G)| \cdot |G|$, and since $\gcd(|H|, |\mathbb{Z}_2^3|) = 1$, $|H|$ must divide $|Aut(\mathbb{Z}_2^3)|$. In fact, $|Aut(\mathbb{Z}_2^3)| = 6$.

After Lagrange, the next results in finite group theory to assault are the Sylow Theorems. Below, a result similar to Sylow's First Theorem is given for a type of gc-set.

Definition 2.9. *A **minimally spanning group**, P, of a gc-set H, is a subgroup of $Aut(G) : G$ such that H is the projection of P in G, and $|P| = |H|$.*

It is not known whether all gc-sets have minimally spanning groups. If all gc-sets do have minimally spanning groups, then the following analogue of Sylow's First Theorem is universally true.

Example 2.10. Let $G = \mathbb{Z}_7$. Let $H = \{0, 2\}$. Let ϕ be the inverse automorphism, and φ be the identity automorphism. Clearly, $P = \{(\varphi, 0), (\phi, 2)\}$ is a subgroup of $Aut(G) : G$. Also H is the projection of P and $|P| = |H|$. Thus H is a gc-set with a minimally spanning group.

Theorem 2.11. *Let G be a finite group. Let $H \subseteq G$ be a gc-set with a minimally spanning group P. Let p be a prime such that p^k divides $|H|$. Then H contains gc-sets of order $p, p^2, ..., p^k$.*

Proof. $|H| = p^k m$, so $|P| = p^k m$. By Sylow's First Theorem, P contains subgroups of order $p, p^2, ..., p^k$. Since P is a subgroup of $Aut(G) : G$, these subgroups are also subgroups of $Aut(G) : G$. Since $|P| = |H|$, and H is the projection of P in G, we know by theorem 2.4 that for each subgroup P_i of P, there is a subset H_i of H such that H_i is the projection of P_i, and $|P_i| = |H_i|$. Thus H contains gc-sets of order $p, p^2, ..., p^k$. □

The following theorem gives us a technique for finding gc-sets with minimally spanning groups.

Theorem 2.12. *The finite product of gc-sets contained in finite groups where each gc-set has a minimally spanning group is itself a gc-set with a minimally spanning group.*

Proof. It suffices to show that the product of two gc-sets with minimally spanning groups is a gc-set a with minimally spanning group. Let H_1 and H_2 be gc-sets contained in the groups G_1 and G_2, respectively. Let H_1 and H_2 have minimally spanning groups P_1 and P_2. Since $|H_1 \times H_2| = |H_1| \cdot |H_2| = |P_1| \cdot |P_2| = |P_1 \times P_2|$, we need only show that $H_1 \times H_2$ is the projection of the subgroup $P_1 \times P_2$.

Claim: $H_1 \times H_2$ is the projection of $P_1 \times P_2$ in $G_1 \times G_2$.

For each $h_i \in H_i$, there is a $\phi_i \in Aut(G_i)$ such that $(\phi_i, h_i) \in P_i$. Therefore for each $(h_1, h_2) \in H_1 \times H_2$ there is a $(\phi_1, \phi_2) \in Aut(G_1 \times G_2)$ such that $(\phi_1, h_1) \in P_1$ and $(\phi_2, h_2) \in P_2$, and $((\phi_1, \phi_2), (h_1 h_2)) \in P_1 \times P_2$. Therefore $H_1 \times H_2$ is contained in the projection of $P_1 \times P_2$, but $|H_1 \times H_2| = |P_1 \times P_2|$, so $H_1 \times H_2$ is the projection of $P_1 \times P_2$ in $G_1 \times G_2$. Thus the finite product of gc-sets contained in finite groups where each gc-set has a minimally spanning group is itself a gc-set with minimally spanning group. □

Since we can now produce infinitely many gc-sets with minimally spanning groups, we now know that Theorem 2.11 is true for a large class of gc-sets.

2.1. **Cyclic GC-sets.** Another type of gc-set we are now studying is the cyclic gc-set. Just as cyclic groups are better behaved than other groups, cyclic gc-sets seem to have a simpler structure than other gc-sets. Also the ease with which an idea from cwatset theory is adapted to gc-set theory suggests the existence of the deep similarities we desire in a generalization.

Definition 2.13. *Let G be a group. Let $H \subseteq G$ be a gc-set. We say H is a* ***cyclic gc-set*** *if there exists an $h \in H$, and an automorphism $\phi \in Aut(G)$ such that $\phi(h) \cdot H = \phi(H)$, and $H = \{h_1, h_2, ...\}$ where $h_1 = h$, and $h_n = h_1\phi(h_{n-1})$ for all $n > 1$.*

Example 2.14. Let $H = \{0000, 1101, 1010, 0001, 1100, 1011\}$ once again under the usual group. Now let $h = 1101$, and let $\phi = (1, 2, 3)$. Clearly, $h_1 = 1101$. $h_2 = h_1\phi(h_1) = 1010$. Now $h_3 = h_1\phi(h_2) = 0001$, $h_4 = h_1\phi(h_3) = 1100$, $h_5 = h_1\phi(h_4) = 1011$, $h_6 = h_1\phi(h_5) = 0000$, $h_7 = 1101$, and now the elements are repeated. Thus H is a cyclic gc-set.

Example 2.15. Here is a non-cwatset example. Let $G = D_4$, the dihedral group on four vertices. Let $H = \{R_0, R_{90}\}$. Choose $h = R_{90}$, and $\phi : G \to G$ by $\phi(g) = F_h g F_h$ whereF_h is a flip around a horizontal axis. Since $\phi(R_0) \cdot H = \phi(H)$ and $\phi(R_{90}) \cdot H = \phi(H)$, H is a gc-set. Now, $h_1 = R_{90}$, and $h_2 = h_1\phi(h_1) = R_0$. $h_3 = R_{90}$, and we cycle through the list of elements continuously. Therefore H is a cyclic gc-set.

There is one major result so far in the research of cyclic gc-sets, and it allows us to get more out of the relationship between the subgroup of $Aut(G) : G$, and the gc-set into which it projects.

Theorem 2.16. *$H \subseteq G$ is a cyclic gc-set if and only if it is the projection of P, a cyclic subgroup of $Aut(G) : G$.*

Proof. Let H be a cyclic gc-set. By Definition 2.13, there is an automorphism $\phi \in Aut(G)$ such that $H = \{h_1, h_2, ...\}$ where $h_n = h_1\phi(h_{n-1})$. Look at $P = \langle(\phi^{-1}, h_1)\rangle$ a cyclic subgroup of $Aut(G) : G$. Now, $(\phi^{-1}, h_1)(\phi^{-1}, h_1) = (\phi^{-1} \circ \phi^{-1}, h_1\phi(h_1))$, and $h_2 = h_1\phi(h_1)$. In general, $(\phi^{-1}, h_1)(\theta, h_{n-1}) = (\theta \circ \phi^{-1}, h_1\phi(h_{n-1}))$, and $h_n = h_1\phi(h_{n-1})$. Thus the projection of P is H. For the converse, let $P = \langle(\phi, h_1)\rangle$, a cyclic subgroup of $Aut(G) : G$. Now $(\phi, h_1)(\phi, h_1) = (\phi \circ \phi, h_1\phi^{-1}(h_1))$, $(\phi, h_1)(\phi \circ \phi, h_1\phi^{-1}(h_1)) = (\phi \circ \phi \circ \phi, h_1\phi^{-1}(h_1\phi^{-1}(h_1)))$, etc. Let H be the projection of P in G. $H = \{h_1, h_1\phi^{-1}(h_1), h_1\phi^{-1}(h_1\phi^{-1}(h_1)), ...\}$. Clearly $h_n = h_1\phi^{-1}(h_{n-1})$, and since $\phi \in Aut(G)$, $\phi^{-1} \in Aut(G)$. Thus, by Definition 2.13, H is a cyclic gc-set. □

3. Conclusion

Currently, the gc-set shows promise as a generalization of the cwatset since many of the significant theorems from cwatset theory can be extended to gc-set theory in a natural way. The study of gc-sets can continue in several directions, with many generalizations from cwatset theory just over the horizon, and many more analogues to group theoretical ideas waiting to be found. An analogue to the cwatset isomorphism is still needed, and Theorem 2.16 may perhaps be used to prove an analogue of the Fundamental Theorem of Cyclic Groups for the gc-set. Also, the question of which gc-sets have minimally spanning groups is still open, and although we know that many cyclic gc-sets do have minimally spanning groups, it is not known whether all cyclic gc-sets have a minimally spanning group. Questions such as these help to insure that GC-set theory will continue to provide many great opportunities for future research.

References

[1] Gary J. Sherman and Martin Wattenberg, Introducing...Cwatsets!, *Mathematics Magazine*, vol. 67 No. 2, Mathematical Association of America, Washington D.C., 1994.

[2] Cary Girod, Matthew Lepinski, Joseph Mileti and Jennifer Paulhus,Cwatset Isomorphism and Its Consequences, Rose-Hulman MS TR 00-01.

[3] J.A. Gallian, *Contemporary Abstract Algebra, ed. 4*, Houghton Mifflin Company, New York, 1998.

[4] Richard Mohr, "CWATSETS: Weights, Cardinalities, and Generalizations". Rose-Hulman Institute of Technology Technical Report Series, MS TR 96-03, 1996.