Cwatset Isomorphism and its Consequences

Carolyn M. Girod, Matthew Lepinski,
Joseph R. Mileti, Jennifer R. Paulhus

MS TR 00-01

January 4, 2000

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/Class/ma/HTML/index.html

FAX: (812) 877-8883 Phone: (812) 877-8391

Cwatset Isomorphism and its Consequences

Carolyn M. Girod Matthew Lepinski Joseph R. Mileti
Jennifer R. Paulhus*

1 January 2000

Abstract

We explore the consequences of cwatset isomorphism (there are a finite number of non-isomorphic cwatsets of each order) and consider parallels between the theory of groups and the theory of cwatsets (cwatsets of prime order are cyclic but direct sums of isomorphic cwatsets aren't necessarily isomorphic).

*Work supported by NSF grant DMS-9619714

Contents

1 Introduction

Definition 1 *A subset, C, of $\mathbb{Z}_2^n$ is a cwatset if for each element,* $\mathbf{c}$*, of C, there exists a permutation, σ, of S_n such that $C + \mathbf{c} = C^\sigma$.*

Rose-Hulman students, Rose-Hulman NSF-REU participants, and Gary Sherman have developed the theory of cwatsets over the past ten years to include a basic understanding of cwatset structure and a complete listing of cwatsets up to degree seven ([1][4][5][7]). Our work, recorded in this technical report, continues this project. In particular we explore the consequences of cwatset isomorphism (there are a finite number of non-isomorphic cwatsets of each order)while searching for parallels between the theory of groups and the theory of cwatsets (cwatsets of prime order are cyclic but direct sums of isomorphic cwatsets aren't necessarily isomorphic).

2 Morphisms and Isomorphisms

2.1 Definitions

Recall that any cwatset is the natural projection of a subgroup of $S_n \wr \mathbb{Z}_2$ into $\mathbb{Z}_2^n$ ([7]).

Definition 2 *The Omega group, Ω_C, of a cwatset, C, is the group of all $(\sigma, \mathbf{b}) \in S_n \wr \mathbb{Z}_2$ such that $C + \mathbf{b} = C^\sigma$.*

Definition 3 *For any binary word $\mathbf{b}$, $\mathbf{b}_i$ is the i^{th} component of $\mathbf{b}$.*

Definition 4 $Aut_C = \{(\sigma, \mathbf{0}) | (\sigma, \mathbf{0}) \in \Omega_C\}$

Definition 5 *An element $(\sigma, \mathbf{b}) \in S_n \wr \mathbb{Z}_2$ is associated with the binary word $\mathbf{b}$.*

Definition 6 *A fiber in a quotient group is associated with a binary word, $\mathbf{b}$, if and only if all of the elements of the fiber are associated with $\mathbf{b}$.*

Definition 7 *We will say that a group homomorphism respects a mapping, f, of cwatsets if it maps elements associated with $\mathbf{b}$ to elements associated with $f(\mathbf{b})$.*

Lemma 1 *If ϕ respects f and ψ respects h, then $\psi \circ \phi$ respects $h \circ f$.*

Proof: Let g be an element in the domain of ϕ, associated with the binary word $\mathbf{b}$. Then $\phi(g)$ is associated with $f(\mathbf{b})$. Therefore, $\psi(\phi(g))$ is associated with $h(f(\mathbf{b}))$. Thus, by definition, $\psi \circ \phi$ respects $h \circ f$. □

In order to study isomorphisms of cwatsets, we first provide a definition of a morphism of cwatsets. The following definition was proposed by Daniel Biss [2].

Definition 8 *A map, f, between two cwatsets, C and D is a morphism if and only if there exists a group homomorphism $\phi : \Omega_C \to \Omega_D$ that respects f.*

Definition 9 *A bijective map, f, between two cwatsets is an isomorphism if and only if both f and f^{-1} are morphisms*

2.2 An Equivalent Condition

Theorem 1 (Biss[2]) *$C \cong D$ if and only if there exists a group isomorphism $\Psi : \Omega_C/I_C \to \Omega_D/I_D$ and a bijection $f : C \to D$ such that Ψ respects f.*

Theorem 1 was first proved in the context of category theory. Our proof will be made without the use of category theory.

Definition 10 *The isotropy group, I_C, of a cwatset, C, is the set of all $(\sigma, \mathbf{0}) \in \Omega_C$ such that $\mathbf{b}^\sigma = \mathbf{b}$ for all $\mathbf{b} \in C$.*

Lemma 2 *I_C is a normal subgroup of Ω_C.*

Proof: To see that I_C is closed, consider $(\alpha, \mathbf{0}), (\beta, \mathbf{0}) \in I_C$. For all $\mathbf{b} \in C$, $\mathbf{b}^{\alpha\beta} = \mathbf{b}^\beta$ since $(\alpha, \mathbf{0}) \in I_C$ and therefore $\mathbf{b}^{\alpha\beta} = \mathbf{b}$ since $(\beta, \mathbf{0}) \in I_C$. This implies, $(\alpha\beta, \mathbf{0}) \in I_C$. Hence $I_C \leq \Omega_C$.

Next we show that I_C is normal in Ω_C. Consider $(\alpha, \mathbf{0}) \in I_C$ and $(\sigma, \mathbf{b}) \in \Omega_C$. Then $(\sigma^{-1}, \mathbf{b}^{\sigma^{-1}})(\alpha, \mathbf{0})(\sigma, \mathbf{b}) = (\sigma^{-1}\alpha\sigma, \mathbf{b}^{\sigma^{-1}\alpha\sigma})$. Since $\mathbf{b}^{\sigma^{-1}} \in C$, We know that $(\mathbf{b}^{\sigma^{-1}})^\alpha = \mathbf{b}^{\sigma^{-1}}$. Therefore, $\mathbf{b}^{\sigma^{-1}\alpha\sigma} = \mathbf{b}^{\sigma^{-1}\sigma} = \mathbf{b}$. This implies, $(\sigma^{-1}, \mathbf{b}^{\sigma^{-1}})(\alpha, \mathbf{0})(\sigma, \mathbf{b}) = (\sigma^{-1}\alpha\sigma, \mathbf{0}) \in I_C$. Thus, $I_C \trianglelefteq \Omega_C$. □

Lemma 3 *$N \trianglelefteq \Omega_C$ and $N \leq Aut_C \Rightarrow N \leq I_C$.*

Proof: Consider an element $(\delta, \mathbf{0}) \in N$. Since $N \trianglelefteq \Omega_C$, $(\sigma, \mathbf{b})(\delta, \mathbf{0})(\sigma^{-1}, \mathbf{b}^{\sigma^{-1}}) \in \Omega_C$ for all $(\sigma, \mathbf{b}) \in N$. Therefore, $(\sigma\delta\sigma^{-1}, \mathbf{b}^{\delta\sigma^{-1}} + \mathbf{b}^{\sigma^{-1}}) \in Aut_C$ since $N \leq Aut_C$. This implies

$$(\mathbf{b}^\delta + \mathbf{b})^{\sigma^{-1}} = \mathbf{0} \Rightarrow \mathbf{b}^\delta + \mathbf{b} = \mathbf{0} \Rightarrow \mathbf{b}^\delta = \mathbf{b}.$$

Thus, $N \leq I_C$. □ .

It is often useful to think of a cwatset as a matrix where the rows of the matrix are the elements of the cwatsets. When we speak of the columns of a cwatset we are actually referring to the columns of the associated matrix. We now prove that a cwatset's isotropy group is non-trivial only if the cwatset has repeated columns.

Lemma 4 *Let $(\alpha, \mathbf{0}) \in I_C$ where $i^\alpha = j$. Then the i^{th} and j^{th} columns of C are identical.*

Proof: Since $(\alpha, \mathbf{0}) \in I_C, \mathbf{b}^\alpha = \mathbf{b}$ for each $\mathbf{b} \in C$. Therefore, $\mathbf{b}_j = \mathbf{b}_i$ for each $\mathbf{b} \in C$; i.e., the i^{th} and j^{th} columns of C are identical. □

It follows that the elements in a cwatset's isotropy group simply move columns within a block of identical columns.

Definition 11 *Let M be the matrix associated with the cwatset C and partition the columns of M into maximal subsets of identical columns. Denote the j^{th} column in the i^{th} component of this partition by M_{ij} denote the number of columns in the i^{th} component by $|M_i|$.*

Definition 12 *Let $P_C = \{(\pi, \mathbf{d}) \in \Omega_C |$for every i, j there exits an l such that $M_{ij}^\pi = M_{lj}\}$.*

Lemma 5 *P_C is a subgroup of Ω_C.*

Proof: Clearly $(id, \mathbf{0}) \in P_C$. To see that P_C is closed, consider $(\sigma, \mathbf{b}), (\pi, \mathbf{d}) \in P_C$ and an arbitrary column, M_{ij}, of C. Since $(\sigma, \mathbf{b}) \in P_C$, there exists an l such that $M_{ij}^\sigma = M_{lj}$. Since $(\pi, \mathbf{d}) \in P_C$, there exists a k such that $M_{lj}^\pi = M_{kj}$. Thus, there exists a k such that $M_{ij}^{\sigma\pi} = M_{kj}$. Hence, $(\sigma\pi, \mathbf{b}^\pi + \mathbf{d}) \in \Omega_C$ and therefore $P_C \leq \Omega_C$. □

We will now show that if a permutation in a cwatset's Omega group moves a column from component i to a column of component k then the permutation must move every column of component i to some column of component k.

Lemma 6 *If $(\sigma, \mathbf{b}) \in \Omega_C$ and $M_{ij}^\sigma = M_{lk}$ then for each $y \leq |M_l|$ there exists an $x \leq |M_i|$ such that $M_{ix}^\sigma = M_{ly}$.*

Proof: $C + b = C^\sigma$, since $(\sigma, \mathbf{b}) \in \Omega_C$. By assumption, $M_{ij}^\sigma = M_{lk}$. Since all of the M_l columns are identical and all of the entries in $\mathbf{b}$ corresponding to M_l columns are identical, all of the M_l columns in C^σ must be identical. Thus, every M_{ly} in M_l is the image under σ of something identical to M_{ij}. But by definition the only columns identical to M_{ij} are M_{ix} for some x. From this it follows that for each $y \leq |M_l|$ there exists an $x \leq |M_i|$ such that $M_{ix}^\sigma = M_{ly}$. □

Corollary 1 *If $(\sigma, \mathbf{b}) \in \Omega_C$ and $M_{ij}^\sigma = M_{lk}$ then $|M_i| = |M_l|$.*

Proof: Note that the $x's$ guaranteed by the previous lemma are distinct since σ induces an injective mapping from the columns of C to the columns of C^σ. Thus, $|M_i| \geq |M_l|$. However, $(\sigma, \mathbf{b}) \in \Omega_C \Rightarrow (\sigma^{-1}, \mathbf{b}^{\sigma^{-1}}) \in \Omega_C$. Since $M_{lk}^{\sigma^{-1}} = M_{ij}$ then by the previous lemma, $|M_i| \leq |M_l|$. Hence, $|M_i| = |M_l|$. □

Lemma 4 states that any permutation associated with an element of the isotropy group only moves columns within sets of identical columns. We will now show the converse to be true.

Lemma 7 *If for every i and j there exists k such that $M_{ij}^\alpha = M_{ik}$, then $(\alpha, \mathbf{0}) \in I_C$.*

Proof: Since α moves columns within sets of identical columns, then $\mathbf{b}^\alpha = \mathbf{b}$ for each $\mathbf{b} \in C$. It remains only to show that $(\alpha, \mathbf{0}) \in \Omega_C$. To do this we must demonstrate that $C^\alpha + \mathbf{0} = C$; i.e., for each $\mathbf{x} \in C$ there exists a $\mathbf{y} \in C$ such that $\mathbf{x}^\alpha = \mathbf{y}$. But this is true for $\mathbf{x} = \mathbf{y}$. Thus, $(\alpha, \mathbf{0}) \in I_C$. □

We are now in a position to prove that every cwatset's Omega group is isomorphic to a semidirect product of P_C and I_C.

Lemma 8 *For each $(\sigma, \mathbf{b}) \in \Omega_C$ there exists $(\pi, \mathbf{d}) \in P_C$ and $(\alpha, \mathbf{0}) \in I_C$ such that $(\sigma, \mathbf{b}) = (\pi, \mathbf{d})(\alpha, \mathbf{0})$.*

Proof: Consider $(\sigma, \mathbf{b}) \in \Omega_C$. For each column M_{ij} of C, there exists l and k such that $M_{ij}^\sigma = M_{lk}$. From Lemma 6, we know π can be chosen such that $M_{ij}^\pi = M_{lj}$. We choose α such that $\pi\alpha = \sigma$. This implies $M_{lj}^\alpha = M_{lk}$, so by the previous lemma, $(\alpha, \mathbf{0}) \in \Omega_C$. By assumption, $(\sigma, \mathbf{b}) \in \Omega_C$. Since Ω_C is closed, $(\pi, \mathbf{b}) \in \Omega_C$. Since $(\pi, \mathbf{b}) \in \Omega_C$ and $M_{ij}^\pi = M_{lj}$ for all i and j, then $(\pi, \mathbf{b}) \in P_C$. □

Theorem 2 *For every cwatset, C, Ω_C is isomorphic to a semidirect product of P_C and I_C.*

Proof: From the previous lemma, $\Omega_C = P_C I_C$. Additionally, $P_C \cap I_C = (id, \mathbf{0})$ and I_C is normal in Ω_C. Therefore, Ω_C is isomorphic to a semi-direct product of P_C and I_C. □

Corollary 2 *For any cwatset, C, there exists a homomorphism from Ω_C to Ω_C/I_C and an isomorphism from Ω_C/I_C to P_C such that both mappings respect the identity bijection.*

Proof: Let ϕ be the natural homomorphism from Ω_C to Ω_C/I_C and consider $(\sigma, \mathbf{b}) \in \Omega_C$. Since ϕ is the natural projection, $(\sigma, \mathbf{b}) \in \phi(\sigma, \mathbf{b})$. Consider an arbitrary $(\pi, \mathbf{d}) \in \phi(\sigma, \mathbf{b})$. Then by definition of a fiber in Ω_C/I_C, $(\pi, \mathbf{d})(\sigma^{-1}, \mathbf{b}^{\sigma^{-1}}) \in I_C$. Therefore,

$$\mathbf{d}^{\sigma^{-1}} + \mathbf{b}^{\sigma^{-1}} = \mathbf{0} \Rightarrow (\mathbf{d} + \mathbf{b})^{\sigma^{-1}} = \mathbf{0} \Rightarrow \mathbf{b} = \mathbf{d}$$

Hence, all of the elements of $\phi(\sigma, \mathbf{b})$ are associated with the binary word, $\mathbf{b}$. Thus, ϕ respects the identity bijection.

Now let ζ be the mapping ϕ with domain restricted to P_C. We know that ζ respects the identity bijection because ϕ respects the identity bijection. Consider $(\pi, \mathbf{d}), (\rho, \mathbf{x}) \in P_C$ such that $\phi(\pi, d) = \phi(\rho, \mathbf{x})$. This implies that $(\pi, \mathbf{d})(\rho, \mathbf{x})^{-1} \in I_C$. But P_C is closed, thus $(\pi, \mathbf{d})(\rho, \mathbf{x})^{-1} \in P_C$. Therefore, $(\pi, \mathbf{d})(\rho, \mathbf{x})^{-1} \in P_C \cup I_C$. Thus, $(\pi, \mathbf{d})(\rho, \mathbf{x})^{-1} = (id, \mathbf{0})$, which implies $(\pi, \mathbf{d}) = (\rho, \mathbf{x})$. Therefore, ζ is injective which implies ζ is an isomorphism. $\square$

We know present a proof of Theorem 1. *Proof:* First we will show that the existence of Ψ and f imply that $C \cong D$. Let ϕ be the natural projection from Ω_C to Ω_C/I_C and let ϕ' be the natural projection from Ω_D to Ω_D/I_D. Similarly, let ζ be the isomorphism from P_C to Ω_C/I_C and ζ' be the isomorphism from P_D to Ω_D/I_D. Note that Ψ respects f and $\phi, \phi', \zeta, \zeta'$ each respect the identity bijection (as per the previous corollary). By Lemma 1, $\phi\Psi\zeta'$ is a group homomorphism from Ω_C to Ω_D that respects f and $\phi'\Psi^{-1}\zeta$ is a group homomorphism from Ω_D to Ω_C that respects f^{-1}. Hence, f is an isomorphism of cwatsets, i.e., $C \cong D$.

Next, we must show that $C \cong D$ implies the existence of Ψ and f. Since, $C \cong D$, there exists a morphism of cwatsets, $h : C \to D$, and an associated group homomorphism, $\Phi : \Omega_C \to \Omega_D$. We know that $\Omega_C/ker(\Phi) \cong Im(\Phi) \leq \Omega_D$. Since Φ respects a bijection between C and D, $\ker(\Phi) \leq Aut_C$ which implies $\ker(\Phi) \leq I_C$. By the third isomorphism theorem for groups, $I_C/\ker(\Phi) \trianglelefteq \Omega_C/\ker(\Phi)$ and $\frac{\Omega_C/\ker(\Phi)}{I_C/\ker(\Phi)} \cong \Omega_C/I_C$. Additionally, since Ω_D is a semidirect product there exists a natural projection from Ω_D to P_D. Since $Im(\Phi) \leq \Omega_D$, then there exists a natural projection, Υ from $Im(\Phi)$ to some $N_D \leq P_D$. Note that this implies that there does not exist a non-trivial $K \trianglelefteq N_D$ such that $K \leq Aut_D$. Similarily, there does not exist a non-trivial $K \trianglelefteq \frac{Im(\Phi)}{I_C/\ker(\Phi)}$ such that $K \leq Im(Aut_D)$, because there is no non-trivial $K \trianglelefteq \Omega_C/I_C$ such that $K \leq Im(Aut_C)$. Thus, $ker(\Upsilon) = I_C/\ker(\Phi)$, because if this were not true then either $\frac{ker(\Upsilon)}{I_C/\ker(\Phi)} \trianglelefteq Aut_D$ or $\frac{I_C/\ker(\Phi)}{\ker(\Upsilon)} \trianglelefteq Im(Aut_D)$.