11-1990

Some Facts About CWAT-Sets

Martin Wattenburg

Advisors:
Gary Sherman

MSTR 90-09

SOME FACTS ABOUT CWAT-SETS

Martin Wattenberg

MS TR 90-09

November 1990

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 Phone: (812) 877-8391

Some Facts About CWAT-sets

Martin Wattenberg*
Brown University

November 25, 1990

1 Introduction

In [1] and [2], Sherman and Atkins, in connection with a problem in statistics, introduced a generalization of the concept of a subgroup of $\mathbf{Z}_2^n$. These generalized subgroups, which we call CWAT-sets (where "CWAT" is an acronym for "Closed With A Twist"), have a rich algebraic structure. In this paper we establish some simple combinatorial facts about CWAT-sets, as well as provide two construction methods, prove a divisibility theorem, and make a classification conjecture.

2 Notation

We will refer to elements of the group $\mathbf{Z}_2^n$ by strings of n binary digits. For instance, $\mathbf{Z}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$. Two such strings of binary digits are added by performing component-wise modulo 2 addition. For example, $1100 + 1010 = 0110$.

Suppose that $\mathbf{x} \in \mathbf{Z}_2^n$, $\mathbf{x} = x_1 x_2 ... x_n$, where each x_i is a binary digit, and $\sigma \in S_n$, where S_n is the symmetric group on n symbols. By $\sigma(\mathbf{x})$ we mean the element $x_{\sigma(1)} x_{\sigma(2)} ... x_{\sigma(n)}$. For instance, if $\mathbf{x} = 111000$, and σ is the transposition $(3, 4)$, then $\sigma(\mathbf{x}) = 110100$.

*Work supported by NSF grant DMS 8922674

If $T \subset \mathbf{Z}_2^n$, we will denote $\{\sigma(\mathbf{t}) | \mathbf{t} \in T\}$ by $\sigma(T)$. Notice that $\sigma^{-1}(\sigma(T)) = T$. If $\mathbf{x} \in \mathbf{Z}_2^n$, we will denote $\{\mathbf{t} + \mathbf{x} | \mathbf{t} \in T\}$ by $T + \mathbf{x}$.

3 Definitions and Facts

Definition. Let $T \subset \mathbf{Z}_2^n$. We say T is a CWAT-set if for all $\mathbf{t} \in T$, there exists a $\sigma \in S_n$ such that $T + \mathbf{t} = \sigma(T)$. We will denote the set of all CWAT-sets in $\mathbf{Z}_2^n$ by W_n.

Notice that a subgroup, G, of $\mathbf{Z}_2^n$ is a CWAT-set, since $G + g = G$ for each $g \in G$. However, not all CWAT-sets are subgroups. For instance, $\{000, 110, 101\}$ is a CWAT-set but not a subgroup.

Definition. Let $\mathbf{0}$ and $\mathbf{1}$ denote the vector $\overbrace{00...0}^{n \text{ times}}$ and the vector $\overbrace{11...1}^{n \text{ times}}$ respectively.

Fact 1. Every CWAT-set contains $\mathbf{0}$.

Proof. Let $T \in W_n$. For any $\mathbf{x} \in T, T + \mathbf{x} = \sigma(T)$ for some $\sigma \in S_n$. Since $\mathbf{x} \in T, T + \mathbf{x}$ includes $\mathbf{x} + \mathbf{x} = \mathbf{0}$. Hence $\mathbf{0} \in \sigma(T)$. Thus $\sigma^{-1}(\mathbf{0}) \in \sigma^{-1}(\sigma(T))$, so $\mathbf{0} \in T$.

Fact 2. Let $T \in W_n$. If $\mathbf{1} \in T$, then $|T|$ is even.

Proof. For any $\mathbf{x} \in T, T + \mathbf{x} = \sigma(T)$. Thus $\sigma(\mathbf{1}) \in T + \mathbf{x}$. But $\sigma(\mathbf{1}) = \mathbf{1}$. Therefore, $\mathbf{1} \in T + \mathbf{x}$. This implies that $\mathbf{1} + \mathbf{x} \in T$. So, for each $\mathbf{x} \in T, \mathbf{1} + \mathbf{x}$ is also in T. Since $\mathbf{1} + \mathbf{x} \neq \mathbf{x}, T$ must be the disjoint union of pairs of elements of the form $\{\mathbf{x}, \mathbf{1} + \mathbf{x}\}$. Therefore, $|T|$ is even.

Definition. Let $\mathbf{x} \in \mathbf{Z}_2^n$, and let $\mathbf{x} = x_1 x_2 ... x_n$, where each x_i is a binary digit. Define the weight of $\mathbf{x}$ to be the number of ones among its binary digits, so $w(\mathbf{x}) = \sum_{i=1}^{n} x_i$. Notice that (i) $w(\sigma(\mathbf{x})) = w(\mathbf{x})$ and (ii) that $w(\mathbf{x} + \mathbf{y}) \equiv w(\mathbf{x}) + w(\mathbf{y}) \pmod 2$.

Definition. For any $T \subset \mathbf{Z}_2^n$, let $E(T)$ be the set of elements in T of even weight, and $O(T)$ be the elements of T which have odd weight. Clearly, $T = E(T) \cup O(T)$, and $E(T) \cap O(T) = \emptyset$.

Fact 3. If T is a CWAT-set, then $E(T)$ is also a CWAT-set.

Proof. Let $\mathbf{t} \in E(T)$. Then for each $\mathbf{x} \in T, w(\mathbf{t} + \mathbf{x}) \equiv w(\mathbf{x}) \pmod 2$. Hence $E(T + \mathbf{t}) = E(T) + \mathbf{t}$. Now, $T + \mathbf{t} = \sigma(T)$ for some $\sigma \in S_n$. So $E(T) = E(\sigma(T))$. This implies that $E(T) + \mathbf{t} = E(\sigma(T))$, which in turns implies that $E(T) + \mathbf{t} = \sigma(E(T))$, since the weight function is unaffected

by permutations. This last equation is sufficient to show that $E(T)$ is a CWAT-set.

Fact 4. Let T be a CWAT-set. If $O(T) \neq \emptyset$, then $|T|$ is even.

Proof. We show that, in fact, $|O(T)| = |E(T)|$. Let $\mathbf{t} \in O(T)$, and choose $\sigma \in S_n$ so that $T + \mathbf{t} = \sigma(T)$. Now, $|E(T)| = |E(\sigma(T))| = |E(T + \mathbf{t})|$. Since $w(\mathbf{t}) \equiv 1 \pmod 2$, $E(T + \mathbf{t}) = O(T) + \mathbf{t}$, and $|O(T) + \mathbf{t}| = |O(T)|$, we have $|E(T)| = O(T)$.

Fact 5. If $T \in W_n$ and $|T| > 2^{n-1}$, then for any $0 \leq k \leq n$, there exists $\mathbf{x} \in T$ such that $w(\mathbf{x}) = k$.

Proof. We show that if T does not contain any element $\mathbf{x}$ of weight k, then $|T| \leq 2^{n-1}$.

Let $K = \{\mathbf{x} \in \mathbf{Z}_2^n | w(\mathbf{x}) = k\}$.Given any element $\mathbf{t} \in T$, T cannot contain any elements of $K + \mathbf{t}$. For, if it did contain such an element, say $\mathbf{x}_k + \mathbf{t}$, where $w(\mathbf{x}_k) = k$, then $T + \mathbf{t}$ would contain $\mathbf{x}_k + \mathbf{t} + \mathbf{t} = \mathbf{x}_k$, an element of weight k. Since $T + \mathbf{t} = \sigma(T)$ for some $\sigma \in S_n$, it has the same weight distribution as T, so this cannot occur.

Now, if we apply this argument to every element of T, we generate a list of $|K| \cdot |T|$ elements (counting repetitions) which T cannot contain. We will show that this list has at least $|T|$ distinct elements in it. To do so, we must determine how many times each element can appear in the list. We know that any element of the list, $\mathbf{x}$, is counted once for each $\mathbf{t} \in T$ such that $\mathbf{x} + \mathbf{t} \in K$. That is, once for each $\mathbf{t}$ such that $\mathbf{x} \in K + \mathbf{t}$. But $|K + \mathbf{t}| = |K|$. So no element is counted more than $|K|$ times in the list. Hence at least $(|K| \cdot |T|)/|K| = |T|$ elements of $\mathbf{Z}_2^n$ cannot be contained in T. So, there are at least as many elements of $\mathbf{Z}_2^n$ not in T as there are in T. This can only happen when $|T| \leq 2^{n-1}$.

Fact 6. If $T \in W_n$ and $|T| > 2^{n-1}$, then $|T|$ is even.

Proof. By Fact 5, T contains an element of odd weight. By Fact 4, $|T|$ is even.

Fact 7. If $T \in W_n$ and $|T| > 2^{n-1}$, then there exists a CWAT-set of size $|T|/2$ in W_n.

Proof. By Fact 5, T contains an element of odd weight. Hence, by Facts 3 and 4, $E(T)$ is a CWAT-set of size $|T|/2$.

4 Construction of CWAT-sets

Definition. Let $S \in \mathbf{Z}_2^n, T \in \mathbf{Z}_2^m$. We define their direct sum to be

$$S \oplus T = \{x_1 x_2 ... x_n y_1 y_2 ... y_m | x_1 ... x_n \in S, y_1 ... y_m \in T\}$$

.

Fact 8. If $S \in W_n, T \in W_m$, then $S \oplus T \in W_{n+m}$.

Proof. It is convenient to denote $\overbrace{00...0}^{n \text{ times}} x_1 x_2 ... x_n$ by $\mathbf{0}_n\mathbf{x}$, and $x_1 x_2 ... x_m \overbrace{00...0}^{m \text{ times}}$ by $\mathbf{x}\mathbf{0}_m$. Let $\mathbf{x} \in S \oplus T$. Then $\mathbf{x} = \mathbf{0}_n\mathbf{x}_t + \mathbf{x}_s\mathbf{0}_m$, where $\mathbf{x}_t \in T$ and $\mathbf{x}_s \in S$.

Note that $S \oplus T + \mathbf{x} = S \oplus T + \mathbf{0}_n\mathbf{x}_t + \mathbf{x}_s\mathbf{0}_m = (S + \mathbf{x}_s) \oplus (T + \mathbf{x}_t) = \sigma(S) \oplus \pi(T)$, for $\sigma \in S_n, \pi \in S_m$. Since in $\sigma(S) \oplus \pi(T), \sigma$ is acting on the first n digits while π is acting on the last m digits, $\sigma(S) \oplus \pi(T) = \tau(S \oplus T)$ for $\tau \in S_{n+m}$. Hence $S \oplus T + \mathbf{x} = \tau(S \oplus T)$, so $S \oplus T$ is a CWAT-set.

Definition. A cyclic CWAT-set set is defined as follows: (we will prove later that this definition does in fact produce a CWAT-set).

Choose $\sigma \in S_n$ and $\mathbf{x} \in \mathbf{Z}_2^n$ and consider the following sequence:

$$\mathbf{x}_0 = \mathbf{0}.$$

$$\mathbf{x}_{i+1} = \sigma(\mathbf{x}_i) + \mathbf{x}.$$

Since $\mathbf{Z}_2^n$ is finite, the set $\{\mathbf{x}_i\}$ of elements in this seequence is finite as well. We denote it as $C(\mathbf{x}, \sigma)$.

Fact 9. $C(\mathbf{x}, \sigma)$ is a CWAT-set.

Proof. First, we will need the following lemma.

Lemma. Let k be the least positive integer such that $\mathbf{x}_j = \mathbf{x}_k$ for some $j < k$. Then $j = 0$ and so $\mathbf{x}_j = \mathbf{x}_k = \mathbf{0}$.

Proof. Suppose $j \neq 0$. Then $\mathbf{x}_j = \mathbf{x}_k$ implies that $\sigma(\mathbf{x}_k) + \mathbf{x} = \sigma(\mathbf{x}_j) + \mathbf{x}$, which in turn implies that $\mathbf{x}_{j-1} = \mathbf{x}_{k-1}$, which is a contradiction. Hence $j = 0$ and $\mathbf{x}_j = \mathbf{x}_k = \mathbf{0}$.

With the aid of our lemma, we now know that $C(\mathbf{x}, \sigma)$ looks like this: $\{\mathbf{x}_0, \mathbf{x}_1, ..., \mathbf{x}_{k-1}\}$ where $\sigma(\mathbf{x}_{k-1}) + \mathbf{x} = \mathbf{x}_0 = \mathbf{0}$. In particular, we have shown that in the sequence $\{\mathbf{x}_i\}, \mathbf{x}_a = \mathbf{x}_b$ if, and only if, $a \equiv b \pmod{k}$.

For convenience in notation, let $T = C(\mathbf{x}, \sigma)$. To prove the fact, we will use induction to show that $T + \mathbf{x}_i = \sigma^i(T)$.

Clearly, $T + \mathbf{x}_0 = T + \mathbf{0} = T = \sigma^0(T)$. Now, note that $T + \mathbf{x} = \sigma(T)$, since

$$\begin{aligned} T + \mathbf{x} &= \{\mathbf{x}_0 + \mathbf{x}, \mathbf{x}_1 + \mathbf{x}, ..., \mathbf{x}_{k-1} + \mathbf{x}\} \\ &= \{(\sigma(\mathbf{x}_{k-1}) + \mathbf{x}) + \mathbf{x}, (\sigma(\mathbf{x}_0 + \mathbf{x}) + \mathbf{x}, ..., (\sigma(\mathbf{x}_{k-2}) + \mathbf{x}) + \mathbf{x}\} \\ &= \{\sigma(\mathbf{x}_{k-1}), \sigma(\mathbf{x}_0), ..., \sigma(\mathbf{x}_{k-2})\} \\ &= \sigma(T). \end{aligned}$$

Now, assume that $T + \mathbf{x}_i = \sigma^i(T)$.

Then $\sigma(T + \mathbf{x}_i) = \sigma^{i+1}(T)$, which means that $\sigma(T) + \sigma(\mathbf{x}_i) = \sigma^{i+1}(T)$, since σ acts as a homomorphism. This last equation tells us that $T + \sigma(\mathbf{x}_i) + \mathbf{x} = \sigma^{i+1}(T)$. But this means that $T + \mathbf{x}_{i+1} = \sigma^{i+1}(T)$.

So, we've shown that in general $T + \mathbf{x}_i = \sigma^i(T)$, which means that T is a CWAT-set.

Fact 10. Let $\mathbf{x} \in \mathbf{Z}_2^n, \sigma \in S_n, m$ be the order of σ in S_n. Then $|C(\mathbf{x}, \sigma)|$ divides $2m$.

Proof. Consider the sequence $\{\mathbf{x}_i\}$ whose members are $\{\mathbf{x}_0, \sigma(\mathbf{x}_0)+\mathbf{x}, ...\}$. Let $k = |C(\mathbf{x}, \sigma)|$. From the proof of the previous fact, we know that $\mathbf{x}_a = \mathbf{x}_b$ if, and only if, $a \equiv b \pmod{k}$. We now show that $\mathbf{x}_{2m} = \mathbf{0}$.

Note that

$$\begin{aligned} \mathbf{x}_{2m} &= \mathbf{x} + \sigma(\mathbf{x} + \sigma(\mathbf{x} + ...))...) \\ &= \sum_{i=0}^{2m-1} \sigma^i(\mathbf{x}) \\ &= \sum_{i=0}^{m-1} \sigma^i(\mathbf{x}) + \sum_{i=m}^{2m-1} \sigma^i(\mathbf{x}). \end{aligned}$$

However, since the order of σ is m, $\sum_{i=0}^{m-1} \sigma^i(\mathbf{x}) = \sum_{i=m}^{2m-1} \sigma^i(\mathbf{x})$. Therefore, $\mathbf{x}_{2m} = \mathbf{0}$. By the lemma, this means that $\mathbf{x}_{2m} = \mathbf{x}_0$, and therefore $2m \equiv 0 \pmod{k}$. Thus $|C(\mathbf{x}, \sigma)|$ divides $2m$.

Fact 11. W_n contains CWAT-sets of order $2n$ and order n.

Proof. Let $\mathbf{x} = 1\ \overbrace{00...0}^{n-1 \text{ times}}$, $\mathbf{y} = 11\ \overbrace{00...0}^{n-2 \text{ times}}$ and $\sigma =$ the n-cycle $(1, 2, ..., n)$. It is easily checked that $|C(\mathbf{x}, \sigma)| = 2n$, and that $|C(\mathbf{y}, \sigma)| = n$.

5 A Lagrange-type theorem for CWAT-sets

The results proved in this section will lead to an interesting divisibility fact about the order of a CWAT-set.

Definition. Let $T \in W_n$. Let $\Sigma(T) = \{\sigma \in S_n | \sigma(T) = T + \mathbf{t} \text{ for some } \mathbf{t} \in T\}$.

We will refer to this set simply as Σ when there is no chance of confusion.

Fact 12. $\Sigma(T)$ is a subgroup of S_n.

Proof. Choose any $\sigma, \tau \in \Sigma$.

There exist $\mathbf{x}, \mathbf{y} \in T$ such that: (i) $T + \mathbf{x} = \sigma(T)$. and (ii) $T + \mathbf{y} = \tau(T)$. From (ii) we have that $T = \tau(T) + \mathbf{y}$. In particular, this means that $\mathbf{y} + \tau(\mathbf{x}) \in T$.

Now, from (i), $T + \mathbf{x} = \sigma(T)$, so $\tau(T) + \tau(\mathbf{x}) = \tau(\sigma(T))$. Thus $T + \mathbf{y} + \tau(\mathbf{x}) = \tau(\sigma(T))$. But $\mathbf{y} + \tau(\mathbf{x}) \in T$ as shown above. Hence $\tau \circ \sigma \in \Sigma$. That is, Σ is a subgroup of S_n.

Definition. Let $\Sigma_{\mathbf{t}} = \{\sigma \in S_n | \sigma(T) = T + \mathbf{t}\}$.

Fact 13. $\Sigma_{\mathbf{0}}$ is a subgroup of Σ.

Proof. $\sigma_{\mathbf{0}}$ is just the stabilizer of T in S_n.

Note that $\Sigma_{\mathbf{0}}$ is not necessarily a normal subgroup of Σ. Consider the CWAT-set $\{000, 1000, 110, 111, 011, 001\}$. Here $\Sigma = S_3$ and $\Sigma_{\mathbf{0}} = \mathbf{Z_2}$.

Fact 14. $\Sigma_{\mathbf{t}}$ is a left coset of $\Sigma_{\mathbf{0}}$.

Proof. Suppose that $T + \mathbf{t} = \pi_1(T)$. Then for each $\sigma \in \Sigma_{\mathbf{0}}, T + \mathbf{t} = \pi(\sigma(T))$. Thus $\pi \circ \sigma \in \Sigma_{\mathbf{t}}$. Hence $\Sigma_{\mathbf{t}}$ is the union of left cosets of $\Sigma_{\mathbf{0}}$.

Now we will show that $\Sigma_{\mathbf{t}}$ consists of only one left coset. Suppose that $\pi, \tau \in \Sigma_{\mathbf{t}}$. Then $\pi(T) = T + \mathbf{t} = \tau(T)$. Hence $\pi(T) = \tau(T)$, which implies that $\pi^{-1}(\tau(T)) = T$. Thus $\pi^{-1} \circ \tau = \sigma$, for some $\sigma \in \Sigma_{\mathbf{0}}$. So $\tau = \pi \circ \sigma$; i.e. π and τ are in the same coset of $\Sigma_{\mathbf{0}}$.

Definition. Let $F(T) = \{\mathbf{t} \in T | T + \mathbf{t} = T\}$. That is, $F(T)$ consists of those elements of T which fix T under addition.

Fact 15. $F(T)$ is a subgroup of T.

Proof. Suppose that $\mathbf{x}, \mathbf{y} \in F(T)$; i.e. $T + \mathbf{x} = T = T + \mathbf{y}$.

Then $T + \mathbf{x} + \mathbf{y} = T + \mathbf{y} = T$. Hence $\mathbf{x} + \mathbf{y} \in F(T)$.

Fact 16. T is the union of cosets of $F(T)$.

Proof. Suppose that $\mathbf{x} \in T$ and $\mathbf{z} \in F(T)$. Then $T + \mathbf{x} = T + \mathbf{z} = T$. In particular, $\mathbf{x} + F(T) \in T$ for each $\mathbf{x} \in T$.

Fact 17. $\Sigma_{\mathbf{x}} = \Sigma_{\mathbf{y}}$ if, and only if, $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of $F(T)$.

Proof. Suppose that $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of $F(T)$. Then $\mathbf{x} = \mathbf{y} + \mathbf{z}$ for some $\mathbf{z} \in F(T)$. $T + \mathbf{x} = T + \mathbf{z} + \mathbf{y} = T + \mathbf{y}$. Therefore, $\Sigma_{\mathbf{x}} = \Sigma_{\mathbf{y}}$.

Now suppose that $\Sigma_{\mathbf{x}} = \Sigma_{\mathbf{y}}$. Then $T + \mathbf{x} = T + \mathbf{y}$. So $T = T + \mathbf{x} + \mathbf{y}$, and $\mathbf{x} + \mathbf{y} = \mathbf{z}$, for some $\mathbf{z} \in F(T)$. Thus $\mathbf{x} = \mathbf{y} + \mathbf{z}$, which means that $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of $F(T)$.

Fact 18. $|T| = |F(T)| \cdot [\Sigma: \Sigma_{\mathbf{0}}]$.

Proof. $|T| = |F(T)|\cdot$ (number of cosets of $F(T)$ in T) Since Fact 17 establishes a one-to-one correspondence between the cosets of $F(T)$ in T and the cosets of $\Sigma_{\mathbf{0}}$ in Σ, the number of cosets of $F(T)$ in T is just $[\Sigma: \Sigma_{\mathbf{0}}]$. Hence $|T| = |F(T)| \cdot [\Sigma: \Sigma_{\mathbf{0}}]$.

Fact 19. If $T \in W_n$, then $|T|$ divides $2^n n!$.

Proof. From Fact 18, $|T| = 2^k [\Sigma: \Sigma_{\mathbf{0}}]$, since $F(T)$ is a subgroup of $\mathbf{Z}_2^n$. Since Σ is a subgroup of S_n, $[\Sigma: \Sigma_{\mathbf{0}}]$ divides $n!$. Hence $|T|$ divides $2^n n!$.

Notice that if T is a subgroup, then $[T: F(T)] = [\Sigma: \Sigma_{\mathbf{0}}]$, so that $|T|$ divides $2^n = |\mathbf{Z}_2^n|$. Thus Lagrange's Theorem, in the context of $\mathbf{Z}_2^n$, is a special case of Fact 19.

6 A Classification Conjecture for CWAT-sets

Conjecture. Let $T \in W_n$. Then T can be written as

$$T = \sigma(G \oplus C_1 \oplus C_2 \oplus ... \oplus C_k),$$

where G is a subgroup of $\mathbf{Z}_2^n$, the $\{C_i\}$ are cyclic CWAT-sets, and $\sigma \in S_n$. That is, every CWAT-set is either the direct sum of a subgroup of $\mathbf{Z}_2^n$ and several other CWAT-sets, or some permutation of such a direct sum.

If the conjecture is true, it will provide a great deal of information about CWAT-sets, since the structure of subgroups of $\mathbf{Z}_2^n$ is known, and the structure of cyclic CWAT-sets is easily accessible. For instance, with the help of the conjecture it might be possible to determine the size of W_n. Whether or not the conjecture is true, further investigation of the properties of CWAT-sets should prove fruitful.