Finite Groups of Derangements on the n-Cube

Larry W. Cusick
Department of Mathematics
California State University, Fresno
Fresno, CA 93740
larryc@csufresno.edu
tel: (559) 278-2462
fax: (559) 278-2872

Abstract

W. Y. C. Chen and R. P. Stanley have characterized the symmetries of the n-cube that act as derangements on the set of k-faces. In this paper we aim to use their result to characterize those finite subgroups of symmetries whose non-trivial members are derangements of the set of k-faces.

Key words: n-cube symmetries, n-cube face derangements, hyperoctahedral group

1 Introduction

In [3], W. Y. C. Chen and R. P. Stanley characterized the symmetries of the n-cube that act as derangements on the set of k-faces. Their elegant and simple criterion is easy to check, involving only permutation cycle decompositions and sign checking. In this paper we aim to use their result to explore finite subgroups of symmetries whose non-trivial members are derangements of the set of k-faces. Our main results are (1) a characterization of the cyclic subgroups that can act freely on the set of k-faces of some n-cube, (2) a necessary condition for any finite group to act freely on the set of k-faces of some n-cube and (3) that every finite 2-group acts freely on the set k-faces of some n-cube. The techniques used, beyond the Chen-Stanley condition, are elementary combinatorics, permutations and group theory.

The original motivation for this research was far removed from the combinatorics of k-faces on the n-cube. The so-called topological space problem asks which groups can act freely on an m-sphere, S^m. One can then ask which finite groups can act freely on a cartesian product of m-spheres, $(S^m)^n$. A consequence of the results in this paper is that the finite groups that can act freely on $(S^{2m})^n$ are precisely the finite 2-groups. Furthermore, a free action is homologically equivalent to a free action on $(S^0)^n$, the set of vertices on the n-cube. Thus we are motivated to ask which finite groups can act freely on the set of k-faces of the n-cube.

2 The Chen-Stanley Criterion

The n-cube, Q_n, will be represented as a graph. The vertices of Q_n are the elements of $(\mathbf{Z}_2)^n$, where $\mathbf{Z}_2 = \{1, -1\}$, and two vertices $\mathbf{x}$ and $\mathbf{y}$ are connected by a unique edge if, and only if, they differ in only one component. A symmetry of Q_n can be represented by a *signed permutation* $(\pi; x_1, \ldots, x_n)$ where π is an element of the symmetric group S_n and each x_i is either 1 or -1. Signed permutations act (on the right) of the vertices of the n-cube by

$$(y_1, \ldots, y_n)(\pi; x_1, \ldots, x_n) = (y_{\pi 1} x_1, \ldots, y_{\pi n} x_n).$$

The group of symmetries of the n-cube is denoted by B_n, the *hyperoctahedral group*, and has the structure of a wreath product $B_n = S_n \wr \mathbf{Z}_2 = S_n \times (\mathbf{Z}_2)^n$, with group multiplication given by

$$(\theta; y_1, \ldots, y_n)(\pi; x_1, \ldots, x_n) = (\theta \pi; y_{\pi 1} x_1, \ldots, y_{\pi n} x_n).$$

By a *k-face* of the n-cube, we mean a k-subcube whose vertices $\mathbf{y} = (y_1, \ldots, y_n) \in Q_n$ have $n - k$ of the coordinates predetermined,

$$F = F\{y_{i_1} = a_{i_1}, \ldots, y_{i_{n-k}} = a_{i_{n-k}}\},$$

where each $a_{i_j} = \pm 1$. It is easy to see that the cardinality of the set of k-faces on the n-cube is $2^{n-k} \binom{n}{k}$. A symmetry $(\pi; \mathbf{x}) \in B_n$ acts on the set of k-faces,

by

$$F\{y_{i_1} = a_{i_1}, \ldots, y_{i_{n-k}} = a_{i_{n-k}}\}(\pi; \mathbf{x}) = F\{y_{j_1} = a_{i_1}x_{j_1}, \ldots, y_{j_{n-k}} = a_{i_{n-k}}x_{j_{n-k}}\},$$

where $i_1 = \pi j_1, \ldots, i_{n-k} = \pi j_{n-k}$. In [3], Chen and Stanley provide a necessary and sufficient condition which is easy to check for a symmetry $(\pi; \mathbf{x}) \in B_n$ to be a derangement of the set of k-faces. To state the Chen-Stanley criterion, and for later applications, we will use the following notation: If $\sigma = (i_1, i_2, \ldots, i_s)$ is a cycle in S_n and $\mathbf{x} \in (\mathbf{Z}_2)^n$, then

$$x_\sigma = x_{i_1} x_{i_2} \cdots x_{i_s}.$$

Theorem 1 (Chen-Stanley Criterion) [3] *A symmetry $(\pi; \mathbf{x}) \in B_n$ is a derangement of the set of k-faces in Q_n if, and only if, for every k-element π-invariant subset $I \subset \{1, \ldots, n\}$, $x_\sigma = -1$ for some cycle σ in π disjoint from I.*

This leads naturally to the problem of computing the number k-faces left fixed by a given symmetry $(\pi; \mathbf{x}) \in B_n$. Towards a solution, we define a π-invariant subset $I \subset \{1, \ldots, n\}$ to be $(\pi; \mathbf{x})$-*good* if $x_\sigma = 1$ for every cycle σ in π that is disjoint from I. The Chen-Stanley criterion is equivalent to this: $(\pi; \mathbf{x})$ fixes some k-face if, and only if, there exists a $(\pi; \mathbf{x})$-good subset I.

Theorem 2 *The number of k-faces left fixed by $(\pi; \mathbf{x}) \in B_n$ is equal to*

$$\sum_I 2^{c_I}$$

where the sum is taken over the set of $(\pi; \mathbf{x})$-good k-element subsets $I \subset \{1, \ldots, n\}$ and c_I is the number of cycles in π disjoint from I.

Proof. Suppose the k-face $F = F\{y_{i_1} = a_{i_1}, \ldots, y_{i_{n-k}} = a_{i_{n-k}}\}$ is left fixed by $(\pi; \mathbf{x}) \in B_n$,

$$F\{y_{i_1} = a_{i_1}, \ldots, y_{i_{n-k}} = a_{i_{n-k}}\} = F\{y_{j_1} = a_{i_1}x_{j_1}, \ldots, y_{j_{n-k}} = a_{i_{n-k}}x_{j_{n-k}}\},$$

where $i_1 = \pi j_1, \ldots, i_{n-k} = \pi j_{n-k}$. Let I be the complement of the set $\{i_1, \ldots, i_{n-k}\}$ in $\{1, \ldots, n\}$. Clearly $\{i_1, \ldots, i_{n-k}\}$, and hence I, is π-invariant. We claim that I is $(\pi; \mathbf{x})$-good. To see why this is true, let $\sigma = (i_{s_1}, \ldots, i_{s_t})$ by a cycle in π, disjoint from I (so its components are elements of $\{i_1, \ldots, i_{n-k}\}$). Then for $\mathbf{y} \in F$,

$$
\begin{aligned}
y_{i_{s_1}} &= a_{\pi i_{s_1}} x_{i_{s_1}} \\
&= y_{i_{s_2}} x_{i_{s_1}} \\
&= a_{\pi i_{s_2}} x_{i_{s_2}} x_{i_{s_1}} \\
&\vdots \\
&= a_{\pi i_{s_t}} x_{i_{s_t}} \cdots x_{i_{s_1}} \\
&= a_{i_{s_1}} x_\sigma \\
&= y_{i_{s_1}} x_\sigma.
\end{aligned}
$$

3

Thus $x_\sigma = 1$, and so I is $(\pi; \mathbf{x})$-good. Also note, from the above string of equalities, that we are free to choose the value of $a_{i_{s_1}} = \pm 1$, which then determines the remaining values $a_{i_{s_2}}, \ldots, a_{i_{s_t}}$ corresponding to the cycle σ. This gives a count of 2^{c_I} k-faces with the starting index set $\{i_1, \ldots, i_{n-k}\}$, where I is the complementary index set. The only contributing index sets would be those for which I is $(\pi; \mathbf{x})$-good, giving a total count of

$$\sum_I 2^{c_I}.$$

∎

3   Structure of the Hyperoctahedral Group

We will find the following notation, and resulting formulas, convenient. If $\mathbf{z} = (z_1, \ldots, z_n)$ and $\mathbf{x} = (x_1, \ldots, x_n)$ are vectors in $(\mathbf{Z}_2)^n$, we will write $\mathbf{zx}$ for the vector $(z_1 x_1, \ldots, z_n x_n)$. Also, we will write $\mathbf{y}^\pi$ for the vector $(y_{\pi 1}, \ldots, y_{\pi n})$. In this way, the group operation in B_n becomes

$$(\theta; \mathbf{y})(\pi; \mathbf{x}) = (\theta\pi; \mathbf{y}^\pi \mathbf{x}).$$

Similarly, the (right) action of B_n on the vertices of Q_n becomes $\mathbf{y}(\pi; \mathbf{x}) = \mathbf{y}^\pi \mathbf{x}$. And inductively, the t-th power of $(\pi; \mathbf{x})$ is given by the formula

$$(\pi; \mathbf{x})^t = (\pi^t; \mathbf{x}^{\pi^{t-1}} \mathbf{x}^{\pi^{t-2}} \cdots \mathbf{x}).$$

Theorem 3 *The order of $(\pi; \mathbf{x})$ is*

$$|(\pi; \mathbf{x})| = \begin{cases} 2|\pi|, & \text{if } x_\sigma = -1 \text{ and } |\pi|/|\sigma| \text{ is odd for some cycle } \sigma \text{ in } \pi; \\ |\pi|, & \text{otherwise.} \end{cases}$$

Proof. Suppose that t is the order of π. Pick $i = 1, \ldots, n$ and let σ be the cycle in π that contains i. The i-th component of $\mathbf{x}^{\pi^{t-1}} \mathbf{x}^{\pi^{t-2}} \cdots \mathbf{x}$ is then

$$
\begin{aligned}
x_{\pi^{t-1}i} x_{\pi^{t-2}i} \cdots x_i \;&=\; (x_\sigma)^{t/|\sigma|} \\[2ex]
&=\; \begin{cases} -1, & \text{if } x_\sigma = -1 \text{ and } t/|\sigma| \text{ is odd}; \\ 1, & \text{otherwise.} \end{cases}
\end{aligned}
$$

The theorem now follows. ∎

The following consequence will find employment later in the paper.

Corollary 1 *If the order of $(\pi; \mathbf{x}) \in B_n$ is odd, then $x_\sigma = 1$ for every cycle in π.*

We will use *bicycle decompositions* of symmetries in B_n. This is similar to cycle decompositions for permutations. Any element $(\sigma; \mathbf{x}) \in B_n$ in which σ is a cycle and $x_j = 1$ if $\sigma(j) = j$ will be called a *bicycle*. Two bicycles are called *disjoint* if their respective permutation parts are disjoint in the usual sense. If $\pi = \sigma_1 \cdots \sigma_t$ is a disjoint cycle decomposition of the permutation π (we include cycles of length 1), and $g = (\pi; \mathbf{x}) \in B_n$, we let $\mathbf{x}^i = (x_1^i, \ldots, x_n^i)$ where

$$x_j^i = \begin{cases} 1, & \text{if } \sigma_i(j) = j; \\ x_j, & \text{otherwise.} \end{cases}$$

We then have the *disjoint bicycle decomposition* $g = g_1 \cdots g_t$ where $g_i = (\sigma_i; \mathbf{x}^i)$ for $i = 1, \ldots, t$. From this discussion, we can see that every element of B_n has a disjoint bicycle decomposition. The proof of the following theorem is elementary and will be omitted.

Theorem 4 (Uniqueness of Disjoint Bicycle Decompositions) *If $\pi = \sigma_1 \cdots \sigma_t$ is a disjoint cycle decomposition of the permutation π, and if $g_i = (\sigma_i; \mathbf{x}^i)$ and $h_i = (\sigma_i; \mathbf{y}^i)$ are bicycles for each $i = 1, \ldots, t$ and if $g = g_1 \cdots g_t = h_1 \cdots h_t$, then $g_i = h_i$ for each $i = 1, \ldots, t$.*

∎

When $k = 0$, the Chen-Stanley criterion says this: A symmetry $(\pi; \mathbf{x}) \in B_n$ fixes a vertex on the n-cube if, and only if, $x_\sigma = 1$ for every cycle σ in π. Furthermore, we can use Theorem 2 to see that if $(\pi; \mathbf{x})$ fixes a vertex, it fixes 2^t vertices where t is the number of cycles in π. One consequence is a way to recognize conjugates in B_n.

Theorem 5 *Two symmetries $(\theta; \mathbf{y}), (\pi; \mathbf{x}) \in B_n$ are conjugate if, and only if, (1) θ and π have the same cycle structure and (2) for some pairing of respectively equal length cycles in the two permutations $\tau_1 \longleftrightarrow \sigma_1, \ldots, \tau_s \longleftrightarrow \sigma_s$, we have $y_{\tau_j} = x_{\sigma_j}$ for all $j = 1, \ldots, s$.*

Proof. Since part (1) of the theorem follows from the well known property of conjugate permutations, we need only prove part (2). Suppose $(\pi; \mathbf{x}) = (\psi; \mathbf{z})^{-1}(\theta; \mathbf{y})(\psi; \mathbf{z})$ where $(\psi; \mathbf{z}) \in B_n$. Then

$$(\pi; \mathbf{x}) = (\psi^{-1}\theta\psi; \mathbf{z}^{\psi^{-1}\theta\psi}\mathbf{y}^\psi\mathbf{z}).$$

Let $\mathbf{w} = \mathbf{y}^\psi\mathbf{x}$. Then a straightforward calculation establishes that $\mathbf{z}$ is a vertex left fixed by $(\pi; \mathbf{w})$.

Thus, per the discussion in the paragraph above the theorem, $w_\sigma = 1$ for every cycle σ in π. If we write $\sigma = (i_1, \ldots, i_m)$, and let $\tau = \psi^{-1}\sigma\psi = (\psi(i_1), \ldots, \psi(i_m))$, then

$$\begin{aligned} w_\sigma &= w_{i_1} \cdots w_{i_m} \\ &= (y_{\psi(i_1)} \cdots y_{\psi(i_m)})(x_{i_1} \cdots x_{i_m}) \\ &= y_\tau x_\sigma. \end{aligned}$$

This, with $w_\sigma = 1$, implies $y_\tau = x_\sigma$.

On the other hand, suppose θ and π have the same cycle structure, $\theta = \tau_1 \cdots \tau_m$ and $\pi = \sigma_1 \cdots \sigma_m$ where each cycle pair τ_j and σ_j have the same length, and $y_{\tau_j} = x_{\sigma_j}$ for every $j = 1, \ldots, m$. Then, θ and π are necessarily conjugate. So there is a permutation $\psi \in S_n$ such that $\tau_j = \psi^{-1}\sigma_j\psi$ for every $j = 1, \ldots, m$. Again, if we let $\mathbf{w} = \mathbf{y}^\psi\mathbf{x}$,

$$
\begin{aligned}
w_{\sigma_j} &= y_{\tau_j} x_{\sigma_j} \\
&= 1,
\end{aligned}
$$

for every $j = 1, \ldots, m$. So we conclude $(\pi; \mathbf{w})$ fixes some vertex $\mathbf{z}$, $\mathbf{z}^\pi\mathbf{w} = \mathbf{z}$. Thus

$$
\begin{aligned}
(\psi; \mathbf{z})^{-1}(\theta; \mathbf{y})(\psi; \mathbf{z}) &= (\psi^{-1}\theta\psi; \mathbf{z}^{\psi^{-1}\theta\psi}\mathbf{y}^\psi\mathbf{z}) \\
&= (\pi; \mathbf{z}^\pi\mathbf{y}^\psi\mathbf{z}) \\
&= (\pi; \mathbf{z}^\pi(\mathbf{y}^\psi\mathbf{x})(\mathbf{x}\mathbf{z})) \\
&= (\pi; (\mathbf{z}^\pi\mathbf{w})(\mathbf{x}\mathbf{z})) \\
&= (\pi; \mathbf{z}\mathbf{x}\mathbf{z}) \\
&= (\pi; \mathbf{x}).
\end{aligned}
$$

∎

3.1 A Combinatorial Identity

In [3], it is proved that the number of symmetries in B_n that fix a vertex is $(2n-1)!! = 1 \cdot 3 \cdot 5 \cdots (2n-1)$. By using Theorem 5 and counting conjugacy classes, we obtain another formula, and consequently a combinatorial identity that may be of independent interest.

We start with the set of partitions of n, denoted by $\mathcal{P}_n$. The elements of $\mathcal{P}_n$ are parameterized by the symbols $\lambda = (1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n})$ where $n = 1 \cdot m_1 + \ldots + n \cdot m_n$. The partitions $\mathcal{P}_n$ are in one-to-one correspondence with the conjugacy classes in S_n, where the symbol λ above corresponds to the class of a permutation $\pi = \sigma_1\sigma_2\cdots\sigma_t$ where $t = \sum_j m_j$ is the number of cycles in π and the lengths of the cycles are equal to the integers in the partition. So, for example, the partition $8 = 2+3+3$ corresponds to the cycle type $(12)(345)(678)$.

It follows from the above paragraph and Theorem 5 that the conjugacy class of $(\pi; \mathbf{x})$ is uniquely determined by an ordered pair $(\lambda; \mathbf{z})$ where λ is the symbol in $\mathcal{P}_n$ described above and $\mathbf{z} \in (\mathbf{Z}_2)^t$ equals to the vector $(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_t})$. As the conjugate of a vertex fixing symmetry is vertex fixing, the Chen-Stanley condition ($k = 0$) tells us that a vertex fixing symmetry conjugacy class $(\lambda; \mathbf{z})$ is characterized by $\mathbf{z} = (1, 1, \ldots, 1)$.

We will organize our count of vertex fixing symmetries in B_n according to the conjugacy classes. Let's begin with a particularly easy class, that represented by the pair $((j); 1)$. This corresponds to the bicycles $(\sigma; \mathbf{x})$ where σ is a

cycle of length j and $\mathbf{x}$ has an even number of minus ones in the components corresponding to σ. There are 2^{j-1} vectors $\mathbf{x}$ that satisfy this requirement and so if $f(j)$ is the number of permutations in the class represented by (j), then the number of symmetries in the class $((j); 1)$ is $f(j)2^{j-1}$. Now, consider a class $(\lambda; 1, 1, \ldots, 1)$ where λ is the symbol $(1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n})$. Using a similar argument as above, and by letting $f(\lambda)$ be the number of permutations in the class represented by λ, the number of symmetries in the class $(\lambda; 1, 1, \ldots, 1)$ is

$$
\begin{aligned}
f(\lambda)\prod_j^n 2^{(j-1)m_j} &= f(\lambda)2^{\left(\sum_j (j-1)m_j\right)} \\
&= f(\lambda)2^{n-t(\lambda)},
\end{aligned}
$$

where $n = \sum_j jm_j$ and $t(\lambda) = \sum_j m_j$. To go any further we will need to know how to compute $f(\lambda)$. This formula is easy to derive and appears to be well known. You start with the $k!$ ways of placing 1 through n in sequence with parentheses appropriately placed for the given cycle structure. Now for each cycle of length i divide by the number of ways to write the cycle, which is i. Finally divide by the $m_i!$ ways you can permute the cycles of length i. The resulting formula is

$$
f(1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n}) = \frac{n!}{1^{m_1}m_1!2^{m_2}m_2!\cdots n^{m_n}m_n!}.
$$

Putting this together gives us a count of the set B_n^*, the vertex fixing symmetries in B_n,

$$
\begin{aligned}
|B_n^*| &= \sum_{\lambda=(1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n})} \frac{2^{n-t(\lambda)}n!}{1^{m_1}m_1!2^{m_2}m_2!\cdots n^{m_n}m_n!} \\
&= \sum_{\lambda=(1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n})} \frac{2^n n!}{(2\cdot 1)^{m_1}m_1!(2\cdot 2)^{m_2}m_2!\cdots (2\cdot n)^{m_n}m_n!},
\end{aligned}
$$

where the sum is taken over the partitions $\lambda \in \mathcal{P}_n$.

Reconciling our two counts gives us the advertised identity.

Theorem 6 *Summing over the partitions of n,*

$$
\sum_{\lambda=(1^{m_1}\ 2^{m_2}\ \ldots\ n^{m_n})} \frac{2^n n!}{(2\cdot 1)^{m_1}m_1!(2\cdot 2)^{m_2}m_2!\cdots (2\cdot n)^{m_n}m_n!} = (2n-1)!!.
$$

4 Finite Groups of Derangements

The fundamental question we address is this: Which finite groups G are isomorphic to subgroups of B_n, for some n, in such a way that G acts freely on the set of k-faces of the n-cube?

Definition 1 If a finite group G is isomorphic to a subgroup of B_n in which every non-identity element acts as a derangement of the set of k-faces, then we write

$$G \vdash_k B_n.$$

The number of k-faces in the n-cube is $2^{n-k} \binom{n}{k}$. And so, if $G \vdash_k B_n$, then the order of G divides $2^{n-k} \binom{n}{k}$. For example, if $k = 0$, then a necessary condition for $G \vdash_0 B_n$ is that G is a finite 2-group. We will see later that this condition is sufficient.

If G is a finite group, then it is possible to embed G into an arbitrarily large symmetric group $G \to S_n$ so that for every non-identity element $g \in G$, $\rho(g)$ is a permutation whose cycle structure is $|g|$-cycles only. (Use the diagonal of the Cayley representation.) We can then compose this representation with the natural embedding $S_n \to B_n$ given by $\pi \mapsto (\pi; 1, 1, \ldots, 1)$. It follows that if $\gcd(|g|, k) = 1$, there are no $\rho(g)$-invariant k-element subsets of $\{1, 2, \ldots, n\}$, and hence, by the Chen-Stanley condition, $G \vdash_k B_n$.

If $(\pi; \mathbf{x}) \in B_n$ is an odd order element, then by Corollary 1, $x_\sigma = 1$ for every cycle σ in π. Consequently, if $(\pi; \mathbf{x})$ was a derangement of the set of k-faces, then by the Chen-Stanley condition, there can be no π-invariant k-element subset $I \subseteq \{1, 2, \ldots, n\}$. It follows that k must be relatively prime to the order of π (which is equal to the order of $(\pi; \mathbf{x})$).

We summarize the above discussion in the following theorem.

Theorem 7

1. If G is a finite group and $\gcd(|G|, k) = 1$, then $G \vdash_k B_n$ for some n.

2. If G is a group of odd order, then $G \vdash_k B_n$ for some n if, and only if, $\gcd(k, |G|) = 1$.

We will next characterize those cyclic groups that are k-face derangements on some cube. One convenient means of building symmetries out of old ones is the *outer product*.

Definition 2 The *outer product* $\times : B_n \times B_m \to B_{n+m}$ is defined by

$$(\pi; \mathbf{x}) \times (\theta; \mathbf{y}) = (\pi \times \theta; \mathbf{x}, \mathbf{y})$$

where $\pi \times \theta$ is the permutation $[\pi_1, \ldots, \pi_n, n + \theta_1, \ldots, n + \theta_n]$.

Theorem 8 *For any $m \geq 2$ and $k \geq 0$, $\mathbf{Z}_m \vdash_k B_n$ for some n if, and only if, $\gcd(k, m) = 2^s$ for some $s \geq 0$.*

Proof. Because of Theorem 7, we may assume m is even, and so we'll replace m by $2m$. We assume $\gcd(k, 2m) = 2^s$ for some $s \geq 0$. We wish to construct an element $g \in B_n$, for some n, so that g generates a cyclic group $\mathbf{Z}_{2m} \vdash_k B_n$. Pick $q \geq 0$ so that $mq \leq k < m(q+1)$. Let σ be the cycle $\sigma = (1, 2, 3, \ldots, m)$, $\mathbf{y} = (1, 1, 1, \ldots, 1, -1) \in (\mathbf{Z}_2)^m$, $h = (\sigma; \mathbf{y}) \in B_t$ and

$$g = \underbrace{h \times h \times \cdots \times h}_{(q+1) \text{ times}} \in B_n$$

where $n = m(q+1)$. It is easy to see that the order of g is $2m$, and we wish to show that g^i is a derangement of the set of k-faces in Q_n for every $i = 1, 2, \ldots, 2m - 1$. We have $g^i = h^i \times \cdots \times h^i$ where each h^i is a product of bicycles $(\psi; \mathbf{z})$ and ψ is a $m/\gcd(m, i)$-cycle. We have exactly $i/\gcd(m, i)$ of the entries in $\mathbf{z}$ are equal to -1 if $0 < i \leq m$ and $(2m - i)/\gcd(m, i)$ entries are equal to -1 if $m < i < 2m$. In either case, $z_\psi = (-1)^{i/\gcd(m, i)}$. In summary, if we write $g^i = (\pi; \mathbf{x})$ then every cycle σ in π has length equal to $m/\gcd(m, i)$ and

$$x_\sigma = (-1)^{i/\gcd(m, i)}.$$

Suppose π leaves a k-element set invariant. Then, k must be a multiple of $m/\gcd(m, i)$. We will be done with the "if" case if we can show that $x_\sigma = -1$. This is accomplished by the following lemma.

Lemma 1 *If $\gcd(k, 2m) = 2^s$ for some $s \geq 0$, $0 < i < 2m$, and $m/\gcd(m, i)$ divides k, then $i/\gcd(m, i)$ is odd.*

Proof of Lemma. Since $\gcd(k, 2m)$ is a power of 2 and $m/\gcd(m, i)$ divides k, we may conclude that $m/\gcd(m, i)$ is a power of 2, $m/\gcd(m, i) = 2^a$ for some $a \geq 0$. Thus,

$$\gcd(m, i) = \frac{m}{2^a}.$$

It follows that $i = rm/2^a$ for some r that is relatively prime to 2^a. Thus,

$$\frac{i}{\gcd(m, i)} = \frac{rm/2^a}{m/2^a}$$
$$= r.$$

If $a > 0$, then clearly r is odd since it is relatively prime to 2^a. If, however, $a = 0$, then $\gcd(m, i) = 1$. Since $i < 2m$, we may conclude that $i = m$ and so $r = 1$, also odd. This completes the proof of the lemma.

Finally, assume $\mathbf{Z}_{2m} \vdash_k B_n$ for some n. We want to show that $\gcd(k, 2m) = 2^s$ for some $s \geq 0$. Suppose p is an odd prime that divides m. Then $\mathbf{Z}_p$ is a subgroup of $\mathbf{Z}_{2m}$, and so $\mathbf{Z}_p \vdash_k B_n$. By the above, we have $\gcd(p, k) = 1$, that is

9

p does not divide k. So the only prime $2m$ and k can possibly have in common is 2, $\gcd(2m, k) = 2^s$, for some $s \geq 0$.

∎

Corollary 2 *If G is a finite group and $G \vdash_k B_n$ for some $n \geq 1$, then $\gcd(k, |G|) = 2^s$ for some $s \geq 0$.*

5 Finite 2-Groups

Since there are 2^n vertices on the n-cube, any subgroup of B_n that acts freely on the vertices (i.e. is a derangement of the vertices) is necessarily a 2-group. We will first look at cyclic groups. To generate a cyclic subgroup of vertex derangements, a symmetry's order must be a power of 2. This is not a sufficient condition however.

Theorem 9 *A vertex derangement $g \in B_n$ whose order is a power of 2 will generate a cyclic subgroup of vertex derangements if, and only if, g contains a bicycle that is a vertex derangment and whose order is equal to the order of g.*

Proof. Suppose $g = (\pi; \mathbf{x})$ is a vertex derangement whose order is a power of 2. Then the order of every bicycle in g is also a power of 2, and since the order of g is the least common multiple of the orders of its bicycles, there is one bicycle $h = (\sigma; \mathbf{y})$ in g whose order is that of g. Let's suppose h is also a vertex derangement, so $y_\sigma = -1$ by the Chen-Stanley criterion. Then since the bicycle decomposition of any power of g contains the bicycle decomposition of the same power of h, we can see that g will generate a cyclic subgroup of vertex derangments if, and only if, h will. Assume $h^2 \neq 1$. If we write $\sigma = (i_1, i_2, \ldots, i_{2^t})$, then $\sigma^2 = (i_1, i_3, \ldots, i_{2^t-1})(i_2, i_4, \ldots, i_{2^t})$, and so h^2 is in the form $h^2 = ((i_1, i_3, \ldots, i_{2^t-1}); \mathbf{u})((i_2, i_4, \ldots, i_{2^t}); \mathbf{v})$ for appropriate vectors $\mathbf{u}$ and $\mathbf{v}$ fashioned from $\mathbf{y}^\sigma \mathbf{y}$. To see that h^2 is a vertex derangement, we need only check,

$$
\begin{aligned}
u_{(i_1, i_3, \ldots, i_{2^t-1})} &= (\mathbf{y}^\sigma \mathbf{y})_{(i_1, i_3, \ldots, i_{2^t-1})} \\
&= y_{\sigma i_1} y_{i_1} y_{\sigma i_3} y_{i_3} \cdots y_{\sigma i_{2^t-1}} y_{i_{2^t-1}} \\
&= y_{i_2} y_{i_1} y_{i_4} y_{i_3} \cdots y_{i_{2^t}} y_{i_{2^t-1}} \\
&= y_\sigma \\
&= -1.
\end{aligned}
$$

Inductively then, all powers h^{2^k} are vertex derangements (except if equal to the identity). For a general power h^m, write $m = 2^t(2k+1)$. Then since the order of h is a power of 2, h^{2k+1} generates the same group as h. This implies h is a power of h^{2k+1} and going back to the original definition of vertex derangement (free action on vertices of the hypercube), we may conclude that h^{2k+1} is a

vertex derangement. So by the same induction argument as above h^m is a vertex derangement.

Now suppose that every bicycle h in g whose order is that of g fixes a vertex. Let the order of g be 2^t. Any power of a vertex fixing symmetry is vertex fixing. It follows that all of the bicycles in $g^{2^{t-1}}$ fix a vertex, and so the non-identity element $g^{2^{t-1}}$ fixes a vertex.

∎

A cyclic subgroup of vertex derangements of order 2^t is generated by $g = ((1, 2, 3, \ldots, 2^{t-1}); -1, 1, \ldots, 1) \in B_{2^{t-1}}$. And by Theorem 9 and Theorem 3, if $\mathbf{Z}_{2^t} \vdash_0 B_n$, then $n \geq 2^{t-1}$.

One consequence of Theorem 9 is that any $\mathbf{Z}_{2^m} \vdash_0 B_n$ has a "squareroot" $\mathbf{Z}_{2^{m+1}} \vdash_0 B_{2n}$. To this end, define the "squaring map" $\nu : B_n \longrightarrow B_{2n}$ by

$$\nu(g) = g \times g.$$

It is straightforward to verify that $\nu(g) = h^2$ where $h = (\theta; \mathbf{y})$ and

$$\theta(j) = \begin{cases} j + n & \text{if } 1 \leq j \leq n; \\ \pi(j - n) & \text{if } n + 1 \leq j \leq 2n \end{cases}$$

and

$$y_j = \begin{cases} 1 & \text{if } 1 \leq j \leq n; \\ x_{j-n} & \text{if } n + 1 \leq j \leq 2n. \end{cases}$$

Also, using the Chen-Stanley criterion $(k = 0)$, one can easily verify that if g is a vertex derangement, then so is $\nu(g)$.

Corollary 3 *If $G < B_n$ is a cyclic subgroup of vertex derangements of order 2^m, then there is a cyclic subgroup of vertex derangements $H < B_{2n}$ of order 2^{m+1} for which $\nu(G) < H$.*

Proof. If $\sigma = (i_1, \ldots, i_s)$ is a cycle in S_n, let σ' be the cycle in S_{2n} given by $\sigma' = (i_1, i_1 + n, \ldots, i_s, i_s + n)$. For a permutation written as a product of cycles $\pi = \sigma_1 \cdots \sigma_t$, we can let $\pi' = \sigma_1' \cdots \sigma_t'$. Then, letting θ be as in the paragraph above, $\theta = \pi'$ and we get the identity $y_{\sigma'} = x_\sigma$ for any cycle σ in π. So it follows from the Chen-Stanley criterion $(k = 0)$ that h is a vertex derangement if g is.

For a bicycle $g_i = (\sigma_i, \mathbf{x}^i)$, we let $g_i' = (\sigma_i', \mathbf{1}, \mathbf{x}^i)$ where $\mathbf{1} = (1, \ldots, 1)$ a string of n 1's. We do this so that if $g = g_1 \cdots g_t$ is a bicycle decomposition, then $h = g_1' \cdots g_t'$ is also a bicycle decomposition. By Theorem 9 we may assume g_1 is a vertex derangment whose order is equal to the order of g. Since $(g_1')^2 = \nu(g_1)$, we know that the order of g_1' is equal to twice the order of g, i.e. the order of h. Thus, again by Theorem 9, h generates a group of vertex derangements.

∎

We now wish to prove that every finite 2-group G acts as a group of vertex derangements on some cube.

Let's begin with the Sylow 2-subgroups of symmetric groups, $\Gamma_n < S_{2^n}$. Their construction is well known, see for example [5]. We begin with $\Gamma_1 = S_2$. Inductively define $\Gamma_n = S_2 \wr \Gamma_{n-1}$. This means that the elements of Γ_n are the triples $(\tau; \phi_1, \phi_2) \in S_2 \times (\Gamma_{n-1})^2$ with multiplication

$$(\tau; \phi_1, \phi_2)(\rho; \psi_1, \psi_2) = (\tau\rho; \phi_{\rho 1}\psi_1, \phi_{\rho 2}\psi_2).$$

This group, Γ_n, can be viewed naturally as a subgroup of S_{2^n} in the following way. Since $\phi_1, \phi_2 \in S_{2^{n-1}}$, the pair (ϕ_1, ϕ_2) can be thought of as a permutation of a 2^n-tuple where ϕ_1 permutes the first 2^{n-1} components and ϕ_2 permutes the second 2^{n-1} components. The non-trivial transposition τ simply flips the two halves. The order of Γ_n is easily seen to be $2^{2^n - 1}$, which is the largest power of 2 that divides $2^n!$, thus Γ_n is a Sylow 2-subgroup of S_{2^n}. Given the above construction, the motive for the following lemma should be apparent.

Lemma 2 *If $G \vdash_0 B_n$, then $S_2 \wr G \vdash_0 B_{2n+1}$.*

Proof. We may replace G by its isomorphic image in B_n. Then we define a function

$$\epsilon : S_2 \wr B_n \longrightarrow B_{2n+1}$$

by

$$\epsilon(1; (\pi, \mathbf{x}), (\theta, \mathbf{y})) = ([\pi_1, \ldots, \pi_n, \theta_1 + n, \ldots, \theta_n + n, 2n+1]; \mathbf{x}, \mathbf{y}, 1)$$

and

$$\epsilon(\tau; (\pi, \mathbf{x}), (\theta, \mathbf{y})) = ([\pi_1 + n, \ldots, \pi_n + n, \theta_1, \ldots, \theta_n, 2n+1]; \mathbf{x}, \mathbf{y}, -1)$$

where τ is the non-identity element in S_2. Clearly ϵ is one-to-one, and it is straightforward to prove that ϵ is a homomorphism. It is an equally straightforward deduction, using the Chen-Stanley criterion with $k = 0$, that $\epsilon(1; g_1, g_2)$ and $\epsilon(\tau; g_1, g_2)$ are vertex derangements if g_1 and g_2 are. Thus if G is a subgroup of vertex derangements in B_n, $S_2 \wr G$ is isomorphic via ϵ to a subgroup of vertex derangements in B_{2n+1}.

■

Theorem 10 $\Gamma_n \vdash_0 B_{2^n - 1}$.

Proof. The group Γ_1 is isomorphic to B_1, which starts our induction. Using Lemma 2 and the induction hypothesis gives us that $\Gamma_n = S_2 \wr S_{n-1}$ is isomorphic to a subgroup of vertex derangements in $B_{2(2^{n-1}-1)+1} = B_{2^n - 1}$.

■

Corollary 4 *If G is a finite group of order 2^n, then G is isomorphic to a subgroup of symmetries of the (2^n-1)-cube so that all of its non-trivial elements are vertex derangements.*

Proof. Any finite group is isomorphic to a subgroup of $S_{|G|}$. Under the hypothesis, G is isomorphic to a Sylow2- subgroup Γ_n of the symmetric group S_{2^n}. Apply Theorem 10.

∎

Finding free actions by specific 2-groups can be a challenge however. The generalized quaternions

$$Q_n = <\alpha, \beta \mid \alpha^{2^{n-1}} = 1, \ \alpha^{2^{n-2}} = \beta^2 = (\alpha\beta)^2 >$$

of order 2^n is predicted by the above Corollary to be isomorphic to a subgroup of vertex derangements in B_{2^n-1}. The proof of the theorem however is not helpful in finding the embedding. But by assigning

$$\alpha \mapsto ((1,2,\ldots,2^{n-2})(2^{n-2}+1, 2^{n-2}+2, \ldots, 2^{n-1}); -1, \underbrace{1, \ldots, 1}_{2^{n-2}-1}, -1, \underbrace{1, \ldots, 1}_{2^{n-2}-1})$$

and

$$\beta \mapsto ((1, 2^{n-1})(2, 2^{n-1}-1)\ldots(2^{n-2}, 2^{n-2}+1); -1, \underbrace{1, \ldots, 1}_{2^{n-2}-2}, -1, 1, \underbrace{-1, \ldots, -1}_{2^{n-2}-2}, 1),$$

we can see that Q_n is isomorphic to a subgroup of vertex derangments in B_{2^n-1}.

Corollary 5 *If G is a finite 2-group and $k \geq 0$, then there exists $n \geq 0$ such that G is isomorphic to a group of symmetries on the n-cube in such a way that it acts as derangements on the set of k'-faces for every $k' \leq k$.*

Proof. By Corollary 4, we may assume $G < B_m$ and G acts as a group of derangements on the set of vertices. So, every non-identity $g = (\pi; \mathbf{x}) \in G$ satisfies $x_\sigma = -1$ for some cycle σ in π. Fix $k \geq 0$ and suppose $k' \leq k$. The there exists a sufficiently large t (with respect to k) such that $h = \underbrace{g \times g \times \cdots \times g}_{t} = (\theta, \mathbf{y})$ satisfies the following: If $I \subseteq \{1, 2, \ldots, mt\}$ is a k'-element subset, then one of the cycles, σ', of $\underbrace{\sigma \times \sigma \times \cdots \times \sigma}_{t}$ (in θ) is disjoint from I. Furthermore, $y_{\sigma'} = x_\sigma = -1$. Hence, $h \in B_{mt}$ is a derangement of the set of k'-faces.

We may now choose one t sufficiently large that the above argument will apply to all $g \in G$. Thus, G is isomorphic, via a diagonal mapping, to a subgroup of B_{mt}, acting as derangements on the set of k'-faces.

∎

References

[1] M. Baake. *Structure and Representations of the Hyperoctahedral Group*, J. Math. Phys. **25**, (1984), 3171-3182.

[2] W. Y. C. Chen. *Induced Cycle Structures of the Hyperoctahedral Group*, SIAM J. Disc. Math. 6 (1993) 353-362.

[3] W. Y. C. Chen & R. P. Stanley. *Derangements of the n-cube*, Discrete Mathematics 115 (1993) 65-75.

[4] L. W. Cusick & P. Tannenbaum. *Fixed Points of the Twisted Cyclic Shift Operator*, Am. Math. Month. **96**, (1989), 713-717.

[5] M. H. Hall. *The Theory of Groups*, The Macmillan Co.(1959).

[6] N. Metropolis & G-C. Rota. *Combinatorial Structure of the Faces of the n-Cube*, SIAM J. Appl. Math Vol. 35, No. 4 (1978), 689-694.