Finite Groups of Derangements on the n-Cube II

Larry Cusick
Department of Mathematics
California State University, Fresno.
Fresno, California, USA
larryc@csufresno.edu

Oscar Vega *
Department of Mathematics
California State University, Fresno.
Fresno, California, USA
ovega@csufresno.edu

Submitted: Mar 23, 2011; Accepted: July 4, 2011; Published: XX
Mathematics Subject Classification: Primary 05E18; Secondary 05E10, 52C99, 20B25

Abstract

Given $k \in \mathbb{N}$ and a finite group G, it is shown that G is isomorphic to a subgroup of the group of symmetries of some n-cube in such a way that G acts freely on the set of k-faces, if and only if, $gcd(k, |G|) = 2^s$ for some non-negative integer s.

The proof of this result is existential but does give some ideas on what n could be.

1 Preliminaries

The n-dimensional cube, or simply n-cube, is denoted by Q_n and will be represented as having vertices the points of $\{1, -1\}^n \subset \mathbb{R}^n$, and edges joining any two vertices that differ in exactly one component. A *k-face* F of the n-cube is a k-subcube whose vertices have $n - k$ of the coordinates predetermined,

$$F = \{\mathbf{y} = (y_1, \dots, y_n) \in Q_n;\ y_{i_1} = a_{i_1}, \dots, y_{i_{n-k}} = a_{i_{n-k}}\},$$

where, of course, each $a_{i_j} = \pm 1$.

It is known that the automorphism group of the cube is $B_n = S_n \wr \mathbb{Z}_2$, the wreath product of S_n and $\mathbb{Z}_2$ (in this article we will use $\mathbb{Z}_2 = \{\pm 1\}$). This group is sometimes called the hyperoctahedral group, or the group of signed permutations; it is a Coxeter group of type $B_n = C_n$, and thus a Weyl group. We denote the elements in B_n by $(\sigma; \mathbf{x})$, where $\sigma \in S_n$ and $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in (\mathbb{Z}_2)^n$. The multiplication is given by

$$(\sigma; \mathbf{x})(\tau; \mathbf{y}) = (\sigma\tau; \mathbf{x}^\tau \mathbf{y})$$

where $\mathbf{x}^\tau = (x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(n)})$, and $\mathbf{x}^\tau \mathbf{y}$ is the standard component-to-component multiplication in $\mathbb{R}^n$. The (right) action of B_n on Q_n is given by $(\sigma, \mathbf{x})\mathbf{y} = \mathbf{y}^\sigma \mathbf{x}$.

*The authors would like to thank the referees for their helpful advice, which greatly improved the exposition.

Definition 1 *With the same notation as above.*

1. *Let G be a group acting on a set X. We say that $g \in G$ acts freely on X if and only if g does not fix any points in X.*
2. *A derangement of the k-faces of Q_n is an element of B_n that acts freely on the set of all k-faces of Q_n.*
3. *A subgroup H of B_n is said to be a* derangement *of the k-faces of Q_n if every non-identity element in H is a* derangement *of the k-faces of Q_n.*
4. *A group G will be called a* derangement *of the k-faces of Q_n if it is isomorphic to subgroup of B_n that is a derangement of the k-faces of Q_n. In such a case we introduce the notation*
$$G \vdash_k B_n.$$

We want to study conditions for a finite group G to be a derangement of the k-faces of some Q_n. The main tool we will use in this article is the Chen-Stanley criterion. In order to get to it we first need to set some notation.

Definition 2 *If $\sigma = (i_1, i_2, \ldots, i_s)$ is a cycle in S_n and $\mathbf{x} \in (\mathbb{Z}_2)^n$, then*

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

Theorem 1 (Chen-Stanley Criterion [2]) *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.*

Note that, in particular, $(\pi; \mathbf{x}) \in B_n$ is a vertex-derangement (i.e. $k = 0$) if, and only if, $x_\sigma = -1$ for some cycle σ in π. This is because there is one zero-element subset (the empty set), which is pi-invariant (vacuously) and every cycle is disjoint from the empty set.

In a previous article [3], the first author proved the following results.

Theorem 2 *Assume k and n are always non-negative integers, and that the notation is the same used before*

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

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

(iii) 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 $s \geq 0$.

(iv) If $|G| = 2^s$, then for all k there exists an n such that $G \vdash_k B_n$.

The main theorem in this article (theorem 6) is, essentially, the converse of theorem 2 (iii). We now move on to present concepts and results that will be needed in the proof of theorem 6.

2 Sufficiency

We can think of $G \vdash_k B_n$ as saying there is a faithful representation of G in the group of signed permutations, with an extra condition. Also, the hyperoctahedral group contains a copy of S_n, so any faithful representation of a group G into S_n can be easily 'extended' to an injective homomorphism $G \to B_n$.

Definition 3 *With the same notation used in the previous section we define:*

1. *An element* $(\pi;\mathbf{x}) \in B_n$ *is called* sufficient *if the following condition is satisfied.*
   (a) *If* $(\pi;\mathbf{x})$ *is of odd order, then* π *has no fixed points.*
   (b) *If* $(\pi;\mathbf{x})$ *is of even order, then there is a cycle* σ *in* π *for which* $x_\sigma = -1$.
2. *A representation of a group* G *into* B_n *is a homomorphism* $\rho : G \to B_n$.
3. *A representation* $\rho : G \to B_n$ *is called* sufficient *if* $\rho(g)$ *is sufficient for every non-identity element* $g \in G$.

Our idea is to consider a sufficient representation of a group G and then 'multiply' it with itself to create a representation for G that satisfies the conditions of the Chen-Stanley criterion. The way of multiplying representations we will use is defined next.

Definition 4 *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 given by*

$$\pi \times \theta = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & \cdots & n+m \\ \pi(1) & \pi(2) & \cdots & \pi(n) & n+\theta(1) & \cdots & n+\theta(m) \end{pmatrix}$$

The following *fundamental construction* will allow us to link the concepts of sufficient representation and derangements of k-faces.

Remark 1 (Fundamental Construction) Let $\Delta_t, \Delta_t^{(i)} : B_n \to B_{nt}$ be given by $\Delta_t(g) = \underbrace{g \times \cdots \times g}_{t \text{ times}}$ and $\Delta_t^{(i)}(g) = \underbrace{1 \times \cdots \times g \times \cdots \times 1}_{t \text{ factors}}$, where the element g appears only in the i-position. Note that $\Delta_t(g) = \Delta_t^{(1)}(g) \cdots \Delta_t^{(n)}(g)$.

For a cycle $\sigma = (i_1, \ldots, i_r)$, let $\tilde{\sigma}$ be the set $\{i_1, \ldots, i_r\}$, and for a permutation π of $\{1, \ldots, n\}$ with cycle decomposition $\pi = \sigma_1 \cdots \sigma_\ell$, let the *cycle set* of π be the set $\{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_\ell\}$.

Now notice that if we write $\Delta_t(g) = (\theta, \mathbf{y})$ and $\Delta_t^{(i)}(g) = (\theta^{(i)}, \mathbf{y}^{(i)})$, then the cycle set for θ is equal to the disjoint union $S = S_1 \cup \cdots \cup S_n$ where each S_i is the cycle set for $\theta^{(i)}$. It follows that for any fixed natural number k, and $g \in B_n$, there is a sufficiently large natural number t ($t > k$ will do) so that any k-element subset $I \subset \{1, \ldots, nt\}$ is disjoint from some cycle set S_i as derived from $\Delta_t^{(i)}(g)$ above.

Theorem 3 *Suppose* $\gcd(|G|, k) = 2^s$ *for some* s*, and there is a sufficient representation* $\rho : G \to B_r$*. Then* $G \vdash_k B_q$ *for some* q*.*

Proof. First, suppose $g = (\pi, \mathbf{x}) \in B_r$ is an even order element and $x_\sigma = -1$ for some cycle σ in π. Then, by the Fundamental Construction above, there is a sufficiently large outer product $\Delta_t(g) = (\theta, \mathbf{y})$ for which if $I \subset \{1, \ldots, rt\}$ (θ-invariant or not) then I is disjoint from some cycle set S_i. By assumption, $x_\sigma = -1$. The corresponding equivalent cycle σ' in $\theta^{(i)}$, hence in θ, then satisfies $y_{\sigma'} = x_\sigma = -1$.

Now suppose $g = (\pi, \mathbf{x})$ is non-trivial and has odd order, π has no fixed points, and $\gcd(|g|, k) = 2^s$ for some s. Then, by necessity, $\gcd(|g|, k) = 1$. Let $\Delta_t(g) = (\theta, \mathbf{y})$. It also follows that θ is an odd order permutation, and so for any t there is no k-element θ-invariant subset $I \subset \{1, \ldots, rt\}$.

Now, we may assume $G < B_r$ and $\gcd(|G|, k) = 2^s$ for some s. By choosing t to be sufficiently large for all even order elements, we have a representation $\rho : G \to B_{rt}$ that satisfies the Chen-Stanley condition. $\square$

What is now left to be proved is that every group G such that $\gcd(|G|, k) = 2^s$, for some s, admits a sufficient representation in some B_n. We will prove this in the next section by inducing a representation for G from its 2-Sylow subgroup (recall that the case $|G|$ odd has already been discussed in theorem 2). The following theorem justifies us wanting to induce from the 2-Sylow subgroup of G.

Theorem 4 (See [3]) *Every finite* 2*-group has a sufficient representation.*

3 Induced Representations

Suppose H is a subgroup of a finite group G of index m and $\rho_0 : H \to B_n$ is a faithful representation. There is a representation $\rho : G \to B_{nm}$, *induced up from* ρ_0 whose construction we will now describe.

First choose a complete set of coset representatives $\{g_1, \ldots, g_m\}$ of the subgroup H,

$$G = g_1 H \cup \cdots \cup g_m H.$$

Pick $g \in G$. For each $i = 1, \ldots, m$, the product gg_i is in one of the cosets, and so $gg_i = g_{\theta(i)} h_i$ for some permutation θ of $\{1, \ldots, m\}$ and $h_i \in H$. We can write each $\rho_0(h_i) = (\pi_i; \mathbf{x}_i)$. Then

$$\rho(g) = (\pi; \mathbf{x_1}, \ldots, \mathbf{x}_m)$$

where π is the permutation on $\{1, \ldots, nm\}$ that permutes the successive m-blocks via θ, while the block interiors are permuted via the corresponding π_i. Specifically, for $j \in \{1, \ldots, nm\}$, write $j = an + b$ where $0 \leq a < m$ and $0 < b \leq n$, then

$$\pi(j) = \pi_{\theta(a+1)}(b) + (\theta(a+1) - 1)n.$$

Remark 2 Note that if we restrict the induced representation ρ back to the subgroup H, then $\rho|_H$ is the direct sum of m copies of ρ_0 (see, for example, [5]). Thus, for $h \in H$,

$$\rho(h) = \rho_0(h) \times \cdots \times \rho_0(h) \quad (m \text{ times}).$$

It follows immediately that if ρ_0 is sufficient, then so is $\rho|_H$.

Lemma 1 *If H is a finite 2-group, $g \in G$ is an odd order element and $\rho(g) = (\pi; \mathbf{x})$, then π has no 1-cycle. That is, $\rho(g)$ is sufficient.*

Proof. Suppose π has a 1-cycle. Then θ must fix one block, that is θ has a 1-cycle. So, $gg_j = g_j h$ for some $j = 1, \ldots, m$ and $h \in H$. Thus, $g_j^{-1} g g_j \in H$, that is g cannot be of odd order. □

Theorem 5 (See [3]) *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 $j = 1, \ldots, s$.

Corollary 1 *If H is a Sylow 2-subgroup of G, ρ_0 is sufficient, and $g \in G$ is an element whose order is a power of 2, then $\rho(g)$ is sufficient.*

Proof. Since Sylow subgroups are conjugate, some conjugate of g is an element of H. The corollary now follows from theorem 5, the assumptions and remark 2. □

4 Main Theorem

It is our aim in this section to prove:

Theorem 6 (Main Theorem) *Suppose G is a finite group and k is a non-negative integer with $\gcd(|G|, k) = 2^s$ for some non-negative integer s, then there is positive integer q for which $G \vdash_k B_q$.*

According to theorem 3, the Main Theorem will follow from the assumptions if we can prove the existence of a sufficient representation $\rho : G \to B_r$ for some r.

Theorem 7 *Every finite group has a sufficient representation.*

We begin with a few lemmas.

Lemma 2 *In B_m, Suppose $\alpha = (\sigma; \mathbf{x})$ where $\sigma = (12 \ldots m)$ and $\alpha^t = (\sigma^t; \mathbf{y})$. Then $y_\sigma = (x_\sigma)^{t/\gcd(m,t)}$.*

Proof. The permutation σ^t is a product of $(m/\gcd(m,t))$-cycles in the form $(i, i+t, \ldots, i+(m/\gcd(m,t)-1)t)$ for $i = 1, \ldots, \gcd(m,t)$ where terms are mod m. And, the jth component of $\mathbf{y}$ is $y_j = x_j x_{j+1} \cdots x_{j+t-1}$ (indices computed mod m). Thus,

$$\begin{aligned} y_\sigma &= (x_1 \cdots x_{i+t-1}) \cdots (x_{i+(m/\gcd(m,t)-1)t}, \ldots x_{i+mt/\gcd(m,t)-1}) \\ &= x_1 x_2 \ldots x_{mt/\gcd(m,t)} \quad \text{(indices mod } m) \\ &= (x_\sigma)^{t/\gcd(m,t)}. \end{aligned}$$

□

Remark 3 It is known that any element $\alpha \in B_m$ is a product of disjoint *bicycles*. A bicycle is any element $(\sigma; \mathbf{x}) \in B_m$ in which σ is a cycle and $x_j = 1$ if $\sigma(j) = j$. Two bicycles are called disjoint if their respective permutation parts are disjoint in the usual sense. See [3] for more details.

Lemma 3 *Suppose* $\alpha = (\pi; \mathbf{x}) \in B_m$ *and* $x_\sigma = 1$ *for every cycle* σ *in* π. *If* $\alpha^t = (\pi^t; \mathbf{y})$, *then* $y_\psi = 1$ *for every cycle* ψ *in* π^t.

Proof. By factoring α as a product of disjoint *bicycles*, it is enough to prove the lemma for $\pi =$ cycle. And, in fact, we may assume $\alpha = (\sigma; \mathbf{x}) \in B_m$ where σ is the cycle $(12\ldots m)$, as external products will allow us to 'paste' these cycles. Lemma 3 now follows from lemma 2. □

We can now prove the Main Theorem.

Proof.[Proof of Theorem 7] Let H be a Sylow 2-subgroup of G, of index m. By corollary 4, there is a sufficient representation $\rho_0 : H \to B_n$ for some n. Let $\rho : G \to B_{nm}$ be the representation induced up from ρ_0. We will prove ρ is sufficient.

Pick $g \in G$, a non-identity element. If the order of g is odd or a power of 2, then $\rho(g)$ is sufficient by lemma 1 and corollary 1. Now assume the order of g to be $2^a(2b+1)$ with $a > 0$. Notre that $g' = g^{2b+1}$ has order 2^a, and so $\rho(g')$ is sufficient. It follows that if we write $\rho(g') = (\pi; \mathbf{x})$, then $x_\sigma = -1$ for some cycle σ in π. It follows from lemma 3, that if $\rho(g) = (\theta; \mathbf{y})$, then $y_\psi = -1$ for some cycle ψ in θ. That is, $\rho(g)$ is sufficient. □

References

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

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

[3] L. W. Cusick. *Finite Groups of Derangements on the n-Cube*, To Appear in Ars Combinatoria.

[4] 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.

[5] J. P. Serre. *Linear Representations of Finite Groups*, Springer-Verlag (1977).