Hypercube problems

Lecture 3

October 24, 2012

Lecturer: Petr Gregor Scribe by: Otakar Trunda Updated: November 8, 2012

1 Structure of the automorphism group

In this talk we take a closer look at the structure of $\Gamma = Aut(Q_n)$. We already know that

$$\forall g \in \Gamma\ \exists! \pi \in S_n\ \exists! a \in Z_2^n \text{ such that } g = r_\pi t_a \text{ where } r_\pi \in R_n,\ t_a \in T_n.$$

A subgroup N of a group G is *normal* (denoted by $N \lhd G$) if it is invariant under conjugation; that is, $gNg^{-1} = N$ for every $g \in G$. It is easy to see that $T_n \lhd \Gamma$ for every $n \geq 1$ and $R_n \not\lhd \Gamma$ for every $n \geq 2$.

Definition 1 *Let G, H be groups. The direct product of G and H (denoted by $G \times H$) is the group on $\{(g,h) \mid g \in G,\ h \in H\}$ with the operation defined by $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$.*

Note that Γ cannot be expressed as $R_n \times T_n$ since $(r_\pi, t_a)(r_\rho, t_b) \neq (r_\pi r_\rho, t_a t_b)$. However, we can use a conjugation to express the composition since

$$(r_\pi, t_a)(r_\rho, t_b) = (r_\pi(r_\rho r_{\rho^{-1}}), t_a)(r_\rho, t_b) = (r_\pi r_\rho, (r_{\rho^{-1}} t_a r_\rho) t_b).$$

Definition 2 *Let H, N be groups and let $\varphi : H \to Aut(N)$ be a homomorphism. The semidirect product (external) of H and N with respect to φ (we write $H \ltimes_\varphi N$) is the group on $\{(h,n),\ h \in H,\ n \in N\}$ with the operation defined by $(h_1,n_1)(h_2,n_2) = (h_1h_2, \varphi(h_2^{-1})(n_1)n_2)$.*

If H, N are subgroups of same group and N is normal then we can use the homomorphism φ defined by $\varphi(h) : n \mapsto hnh^{-1}$ (a conjugation by h). Then we write simply $H \ltimes N$.

Fact 3 *$Aut(Q_n) = R_n \ltimes T_n \simeq S_n \ltimes Z_2^n$ for every $n \geq 1$.*

To verify that $Aut(Q_n)$ can be expressed in this way, let us see the composition

$$(r_\pi, t_a)(r_\rho, t_b) = (r_\pi r_\rho,\ \varphi(r_\rho^{-1})(t_a)t_b) = (r_\pi r_\rho,\ r_\rho^{-1} t_a r_\rho t_b) = (r_\pi r_\rho, t_{a_\rho} t_b) = (r_{\pi\rho}, t_{a_\rho \oplus b})$$

since $r_\rho^{-1} t_a r_\rho : u \mapsto (u_{\rho^{-1}} \oplus a)_\rho = u \oplus a_\rho$. The neutral element is $(r_{id}, t_{\mathbf{0}})$ and the inverse is

$$(r_\pi, t_a)^{-1} = (r_\pi^{-1}, [\varphi(r_\pi)(t_a)]^{-1}) = (r_\pi^{-1}, [r_\pi t_a r_\pi^{-1}]^{-1}) = (r_\pi^{-1}, r_\pi t_a^{-1} r_\pi^{-1}) = (r_{\pi^{-1}}, t_{a_{\pi^{-1}}}).$$

$Aut(Q_n)$ is called the *hyperoctahedral* group and it is also the group of symmetries of a cross-polytope (a dual polytope to the hypercube). Alternatively, $Aut(Q_n)$ can be written as the *wreath product* $Aut(Q_n) \simeq S_2 \wr S_n$, see the following definition.

Definition 4 *Let A, H be groups, H acting on V. Let K be the direct product of copies of A indexed by elements of V (i.e. $K = \prod_{x \in V} A_x$, K is called a base.) The (unrestricted) wreath product of A and H (denoted by $A \wr_V H$) is $A \wr_V H = H \ltimes K$.*

If $H = S_n$ we take $V = [n]$ with the natural action of H on V and write simply $A \wr H$.

In the first lecture we defined the folded cube FQ_n and the augmented cube AQ_n. It is known that $Aut(FQ_n) \simeq S_{n+1} \ltimes Z_2^n$ [8] and $|Aut(AQ_n)| = 2^{n+3}$ [5].

Problem 1 *What is the structure of $Aut(AQ_n)$?*

2 Distance transitivity

In this section we inspect how $Aut(Q_n)$ acts on ordered pairs of vertices.

Definition 5 *Let Γ be a group acting on V and let $x, y \in V$. The orbital of (x, y) is a set*

$$\Gamma(x, y) = \{(g(x), g(y)) \mid g \in \Gamma\}.$$

In fact, it is an orbit in Γ with the action on $V \times V$ induced by the action on V.

Let $n \geq 1$ be fixed, $\Gamma = Aut(Q_n)$ with the action on $V = V(Q_n)$. For $0 \leq d \leq n$ let

$$D_d = \{(u, v) \in V \times V \mid d_H(u, v) = d\}.$$

Since every vertex u in Q_n has exactly $\binom{n}{d}$ vertices at distance d and there are 2^n choices for u, we obtain $|D_d| = \binom{n}{d}2^n$. Moreover, as every automorphism preserves the distances, it is clear that $\Gamma(x, y) \subseteq D_d$ for every $x, y \in V$ where $d = d_H(x, y)$. The following lemma shows that actually the equality holds.

Lemma 6 *For every $x, y \in V$ it holds $|\Gamma(x, y)| = \binom{n}{d}2^n$ where $d = d_H(x, y)$.*

Proof From the orbit-stabilizer theorem for the group Γ_x we have

$$|\Gamma_{x,y}|.|\Gamma_x y| = |\Gamma_x| \tag{1}$$

where $\Gamma_{x,y} = \Gamma_{(x,y)} = \Gamma_x \cap \Gamma_y$. From a study of stabilizers in the last lecture

$$|\Gamma_x| = n! \text{ and } \Gamma_x y = \{z \mid d_H(x, z) = d_H(x, y)\}, \text{ so } |\Gamma_x y| = \binom{n}{d}. \tag{2}$$

From (1) and (2) it follows that

$$|\Gamma_{(x,y)}| = (n - d)!n!. \tag{3}$$

By another use of the orbit-stabilizer theorem,

$$|\Gamma_{(x,y)}|.|\Gamma(x, y)| = |\Gamma|. \tag{4}$$

From (3), (4) and the fact that $|\Gamma| = n!2^n$ we obtain $|\Gamma(x, y)| = \binom{n}{d}2^n$. ■

Before we state the result let us put another definition.

Definition 7 *A graph $G = (V, E)$ is*

- *distance-transitive if for every $x, y, u, v \in V$ with $d_G(x, y) = d_G(u, v)$ there is $g \in Aut(G)$ such that $g(x) = u$ and $g(y) = v$,*
- *arc-transitive if for every $x, y, u, v \in V$ with $xy, uv \in E$ there is $g \in Aut(G)$ such that $g(x) = u$ and $g(y) = v$ (we also say that G is symmetric),*
- *edge-transitive if for every $xy, uv \in E$ there is $g \in Aut(G)$ such that $g(xy) = uv$,*
- *vertex-transitive if for every $x, y \in V$ there is $g \in Aut(G)$ such that $g(x) = y$.*

Clearly, distance-transitivity implies arc-transitivity which implies both edge-transitivity and vertex-transitivity. There are graphs that are edge-transitive but not vertex-transitive.

Theorem 8 *For every $n \geq 1$ the hypercube Q_n is distance-transitive.*

Proof From Lemma 6 it directly follows that $\Gamma(x, y) = D_d$ for every $x, y \in V(Q_n)$ where $d = d_H(x, y)$. ■

A problem on hypercube automorphisms

A d-th level in Q_n is the set $L_d = \{u \in Z_2^n \mid |u| = d\}$. Let n be even and $A \subseteq L_{n/2}$ be a basis of $\mathbb{F}_2^n$. For $a \in L_{n/2}$ let $R(a) = \{r \in R_n \mid r(a) = a \oplus \mathbf{1}\}$. Then $C \subseteq Z_2^n$ is called *A-compatible* if for every $a \in A$ there is $r_a \in R(a)$ such that $r_a(C) = C$.

Examples of trivial A-compatible sets are unions of some levels.

Problem 2 (the weakest form) *For some basis A in $L_{n/2}$ where n is even, find a nontrivial A-compatible set in some level L_d.*

Problem 3 (the strongest form) *For every $n \equiv 2 \pmod 4$, every basis $A \in L_{n/2}$ find all (nontrivial) A-compatible sets in each level L_d.*

3 Symmetry breaking

In this section we inspect how to break all the symmetries of Q_n. A first approach is by labeling the vertices. Let $G = (V, E)$ be a graph.

A mapping $\Phi : V \to \{1, 2, ..., r\}$ is called an *r-labeling* of G. Then (G, Φ) is called a *labeled graph*. Its automorphisms must preserve the labeling; that is, $Aut(G, \Phi) = \{g \in Aut(G) \mid \Phi(u) = \Phi(g(u)) \text{ for every } u \in V\}$. A labeling Φ of G is called *distinguishing* if $Aut(G, \Phi) = \{id\}$; that is, (G, Φ) is *rigid*. The *distinguishing number* $D(G)$ of G is the minimal number of labels in a distinguishing labeling of G.

Theorem 9 (Bogstad, Cowen [1]) *$D(Q_1) = 2$, $D(Q_2) = D(Q_3) = 3$, and $D(Q_n) = 2$ for every $n \geq 4$.*

Proof Clearly $D(Q_n) \geq 2$ since Q_n is not rigid for every $n \geq 1$. It is easy to see that $D(Q_1) = 2$, $D(Q_2) = 3$. We leave as a homework to verify $D(Q_3) = 3$.

Let $n \geq 4$. We define $S = \{s_i = \sum_{j=1}^{i} e_j \mid 0 \leq i \leq n\}$ and $t = e_1 \oplus e_n$. Furthermore, for $u \in V(Q_n)$ let $\Phi(u) = 1$ if $u \in S \cup \{t\}$, and $\Phi(u) = 2$ otherwise. Then Φ is distinguishing 2-labeling since every automorphism of (Q_n, Φ) has to map the set S to itself and cannot revert the order of vertices in S as $s_1 t \in E(Q_n)$ and $s_{n-1} t \notin E(Q_n)$. ■

We may require, in addition, that the distinguishing labeling is proper. The *distinguishing chromatic number* $\chi_D(G)$ of a graph G is the minimal number of labels in a distinguishing *proper* labeling of G; that is, adjacent vertices have distinct labels.

Theorem 10 (Choi et al. [4], Klöckl [7]) *$\chi_D(Q_1) = 2$, $\chi_D(Q_2) = \chi_D(Q_3) = \chi_D(Q_4) = 4$, and $\chi_D(Q_n) = 3$ if $n \geq 5$.*

Another approach to the symmetry breaking is by finding a set of vertices that every automorphism has to preserve point-wise. Let $G = (V, E)$ be a graph.

A set $S \subseteq V$ is *point-wise preserved* by $g \in Aut(G)$ if $g(s) = s$ for every $s \in S$. If S is point-wise preserved only by the trivial automorphism, the we call S a *symmetry breaking set*. Let $br(G)$ be the minimal size of a symmetry breaking set of G.

Theorem 11 (Boutin [3]) *$br(Q_n) = \lceil \log_2 n \rceil + 1$ for every $n \geq 1$.*

Proof Let M be some binary $(m \times n)$-matrix with distinct columns where $m = \lceil \log_2 n \rceil$. Then the rows of M together with the vector $\mathbf{0}$ form a symmetry breaking set since every automorphism maps columns to columns or its complements in M, which is possible on by the identity.

On the other hand, if R is a symmetry breaking set with $|R| < \lceil \log_2 n \rceil + 1$, let M be the $(|R| \times n)$ - matrix with R in rows. There are at most $2^{|R|}$ distinct columns in M, hence $c_i = c_j$ or $c_i = \overline{c_j}$ for some distinct columns i, j. Then $r_{(ij)}$ or $r_{(ij)} t_{e_i}$ is a nontrivial automorphism point-wise preserving R. ■

Let $r(G)$ be the minimal size of a set-wise symmetry breaking set S in a graph G. That is, $g(S) = S$ only by the trivial automorphism g.

Problem 4 *Determine the value of $r(Q_n)$.*

By Theorem 9, $r(Q_n)$ is defined if and only if $n = 1$ or $n \geq 4$. Moreover, from the above results we obtain $\lceil \log_2 n \rceil + 1 \leq r(Q_n) \leq n + 2$ for every $n \geq 4$.

4 Notes

For more on distance transitivity the reader is referred to [6]. The value $\chi_D(Q_4) = 4$ in Theorem 10 is due to Klöckl [7]. According to [2], Problem 4 was already posed by W. Imrich. Boutin [2] showed that $r(Q_n) \leq 2\lceil \log_2 n \rceil - 1$ for every $n \geq 5$.

References

[1] B. Bogstad, L. J. Cowen, *The distinguishing number of the hypercube*, Discrete Mathematics 283 (2004), 29–35.

[2] D. L. Boutin, *Small label classes in 2-distinguishing labelings*, Ars Mathematica Contemporanea 1 (2008), 154–164.

[3] D. L. Boutin, *The determining number of a Cartesian product*, Journal of Graph Theory 61 (2009), 77–87.

[4] J. O. Choi, S. G. Hartke, H. Kaul, *Distinguishing chromatic number of Cartesian products of graphs*, SIAM J. Discrete Math. 24 (2010), 82–100.

[5] S. A. Choudum, V. Sunitha, *Automorphisms of augmented cubes*, International Journal of Computer Mathematics 85 (2008), 1621–1627.

[6] C. Godsil, G. Royle, *Algebraic Graph Theory*, Springer-Verlag, New York, 2004.

[7] W. Klöckl, *On distinquishing numbers*, Discussiones Mathematicae Graph Theory 28 (2008), 419–429.

[8] S. M. Mirafzal, *Some other algebraic properties of folded hypercubes*, arXiv:1103.4351v1.