Automorphisms of the Cube n^d

Pavel Dvořák[1] ⋆ and Tomáš Valla[2] ⋆⋆

[1] Faculty of Mathematics and Physics,
Charles University in Prague, Czech Republic
koblich@iuuk.mff.cuni.cz

[2] Faculty of Information Technology,
Czech Technical University in Prague, Czech Republic
tomas.valla@fit.cvut.cz

Abstract. Consider a hypergraph H_n^d where the vertices are points of the d-dimensional combinatorial cube n^d and the edges are all sets of n points such that they are in one line. We study the structure of the group of automorphisms of H_n^d, i.e., permutations of points of n^d preserving the edges. In this paper we provide a complete characterization. Moreover, we consider the Colored Cube Isomorphism problem of deciding whether for two colorings of the vertices of H_n^d there exists an automorphism of H_n^d preserving the colors. We show that this problem is GI-complete.

1 Introduction

Combinatorial cube n^d (or simply a cube n^d) is a set of points $[n]^d$, where $[n] = \{0, \dots, n-1\}$. A *line* ℓ of a cube n^d is a set of n points of n^d which lie in a geometric line in the d-dimensional space where the cube n^d is embedded. We denote the set of all lines of the cube n^d by $\mathbb{L}(n^d)$. Thus, the hypergraph H_n^d is defined as $\big(n^d, \mathbb{L}(n^d)\big)$.

We denote the group of all permutations on n elements by $\mathbb{S}_n$. A permutation $P \in \mathbb{S}_{n^d}$ is an *automorphism* of the cube n^d if $\ell = \{v_1, \dots, v_n\} \in \mathbb{L}(n^d)$ implies $P(\ell) = \{P(v_1), \dots, P(v_n)\} \in \mathbb{L}(n^d)$. Informally, an automorphism of the cube n^d is a permutation of the cube points which preserves the lines. We denote the set of all automorphisms of n^d by T_n^d. Note that all automorphisms of n^d with a composition $\circ$ form a group $\mathbb{T}_n^d = (T_n^d, \circ, Id)$.

Our main result is the characterization of the generators of the group $\mathbb{T}_n^d$ and computing the order of $\mathbb{T}_n^d$. Surprisingly, the structure of $\mathbb{T}_n^d$ is richer than only the obvious rotations and symmetries. We use three groups of automorphisms for characterization of the group $\mathbb{T}_n^d$ as follows. The first one is a group $\mathbb{R}_d$ of rotations of the d-dimensional hypercube. Generators of $\mathbb{R}_d$ are the rotations

$$R_{ij}\big([x_1, \dots, x_i, \dots, x_j, \dots, x_d]\big) = [x_1, \dots, n - x_j - 1, \dots, x_i, \dots, x_d]$$

⋆ The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 616787.

⋆⋆ Supported by the Centre of Excellence – Inst. for Theor. Comp. Sci. 79 (project P202/12/G061 of GA ČR).

for every $i, j \in \{1, \dots, d\}$. The second group is a group of permutation automorphisms $\mathbb{F}_n$ contains mappings $F_\pi\big([x_1, \dots, x_d]\big) = [\pi(x_1), \dots, \pi(x_d)]$ where $\pi \in \mathbb{S}_n$ such that it has a *symmetry property*: if $\pi(p) = q$ then $\pi(n-p-1) = n-q-1$. The last one is a group of axial symmetry $\mathbb{X}$ which contains the automorphisms Id and $X\big([x_1, \dots, x_{d-1}, x_d]\big) = [x_1, \dots, x_d, x_{d-1}]$. Our main result is summarized in the following theorem. For the proof we use and generalize some ideas of Silver [11] who proved a same result for the cube 4^3.

Theorem 1. *The group* $\mathbb{T}_n^d$ *is generated by the elements of* $\mathbb{R}_d \cup \mathbb{F}_n \cup \mathbb{X}$. *The order of the group* $\mathbb{T}_n^d$ *is* $2^{d-1+k} d! k!$ *where* $k = \lfloor \frac{n}{2} \rfloor$.

An *isomorphism* of two hypergraphs $H_1 = (V_1, E_1), H_2 = (V_2, E_2)$ is a bijection $f : V_1 \to V_2$ such that for each $\{s_1, \dots, s_r\} \subseteq V_1$, $\{s_1, \dots, s_r\} \in E_1 \Leftrightarrow \{f(s_1), \dots, f(s_r)\} \in E_2$. A *coloring* of a hypergraph $H = (V, E)$ by k colors is a function $s : V \to [k]$. The following problem is well studied.

PROBLEM: Colored Hypergraph Isomorphism (CHI)
Instance: Hypergraphs $H_1 = (V_1, E_1), H_2 = (V_2, E_2)$, colorings $s_1 : V_1 \to [k], s_2 : V_2 \to [k]$.
Question: Is there an isomorphism $f : V_1 \to V_2$ of H_1 and H_2 such that it preserves the colors? I.e., it holds $s_1(v) = s_2(f(v))$ for every vertex v in V_1.

There are several FPT algorithms[3] for CHI—see Arvind et. al. [3, 2]. The problem Colored Cube Isomorphism is defined as the problem CHI where both $H_1, H_2 = H_n^d$. Since we know the structure of the group $\mathbb{T}_n^d$, it is natural to ask if Colored Cube Isomorphism is an easier problem than CHI. We prove that the answer is negative. The class of decisions problems GI contains all problems with a polynomial reduction to the problem Graph Isomorphism.

PROBLEM: Graph Isomorphism
Instance: Graphs G_1, G_2.
Question: Are the graphs G_1 and G_2 isomorphic?

It is well known that CHI is GI-complete, see Booth and Colbourn [6]. We prove the same result for Colored Cube Isomorphism.

Theorem 2. *The problem* Colored Cube Isomorphism *is* GI*-complete even if both input colorings has a form* $n^d \to [2]$.

The paper is organized as follows. First we count the order of the group $\mathbb{T}_2^d$, whose structure is different from other automorphism groups. Next, for clarity reasons we characterize the generators for $\mathbb{T}_n^3$, and then we generalize the results for the general group $\mathbb{T}_n^d$. In Section 5 we count the order of the group $\mathbb{T}_n^d$. In the last section we study the complexity of Colored Cube Isomorphism and show some idea of a prove of Theorem 2.

[3] The parameter is the maximum number of vertices colored by the same color.

1.1 Motivation

A natural motivation for this problem comes from the game of Tic-Tac-Toe. It is usually played on a 2-dimensional square grid and each player puts his tokens (usually crosses for the first player and rings for the second) at the points on the grid. A player wins if he occupies a line with his token vertically, horizontally or diagonally (with the same length as the grid size) faster than his opponent. Tic-Tac-Toe is a member of a large class of games called strong positional games. For an extraordinary reference see Beck [5]. The size of a basic Tic-Tac-Toe board is 3×3 and it is easy to show by case analysis that the game ends as a draw if both players play optimally. However, the game can be generalized to larger grid and more dimensions. The d-dimensional Tic-Tac-Toe is played on the points of a d-dimensional combinatorial cube and it is often called the game n^d. With larger boards the case analysis becomes unbearable even using computer search and clever algorithms have to be devised.

The only (as far as we know) non-trivial solved 3-dimensional Tic-Tac-Toe is the game 4^3, which is called Qubic. Qubic is a win for the first player, which was shown by Patashnik [10] in 1980. It was one of the first examples of computer-assisted proofs based on a brute-force algorithm, which utilized several clever techniques for pruning the game tree. Another remarkable approach for solving Qubic was made by Allis [1] in 1994, who introduced several new methods. However, one technique is common for both authors: the detection of isomorphisms of game configurations. As the game of Qubic is highly symmetric, this detection substantially reduces the size of the game tree.

For the game n^d, theoretical result are usually achieved for large n or large d. For example, by the famous Hales and Jewett theorem [8], for any n there is (an enormously large) d such that the hypergraph H_n^d is not 2-colorable, that means, the game n^d cannot end in a draw. Using the standard Strategy Stealing argument, n^d is thus a first player's win. In two dimensions, each game n^2, $n > 2$, is a draw (see Beck [5]). Also, several other small n^d are solved.

All automorphisms for Qubic were characterized by Rolland Silver [11] in 1967. As in the field of positional games the game n^d is intensively studied and many open problems regarding n^d are posed, the characterization of the automorphism group of n^d is a natural task.

The need to characterize the automorphism group came from our real effort to devise an algorithm and computer program that would be able to solve the game 5^3, which is the smallest unsolved Tic-Tac-Toe game. While our effort of solving 5^3 is currently not yet successful, we were able to come up with the complete characterization of the automorphism group n^d, giving an algorithm for detection of isomorphic positions not only in the game 5^3, but also in n^d in general.

A game configuration can be viewed as a coloring s of n^d by crosses, rings and empty points, i.e., $s : n^d \to [3]$. Since we know the structure of the group $\mathbb{T}_n^d$, this characterization yields an algorithm for detecting isomorphic game positions by simply trying all combinations of the generators (the number of the combinations is given by the order of the group $\mathbb{T}_n^d$). A natural question arises: can one obtain a faster algorithm? Note that the hypergraph H_n^d has polynomially many edges in the number of vertices. Therefore, from a polynomial point of view it does not matter if there are hypergraphs H_d^n with colorings or only colorings on the input. Due to Theorem 2 we conclude that deciding if two game configurations are isomorphic is as hard as deciding if two graphs are isomorphic.

Although our primary motivation came from the game of Tic-Tac-Toe, we believe our result has much broader interest as it presents an analogy of automorphism characterization results of hypercubes (see e.g. [7, 9]).

2 Preliminaries

Beck [5] gives a different point of view on the lines of n^d. Let $s = (s^1, \dots, s^n)$ be a sequence of n distinctive points of a cube n^d. Let $s^i = [s^i_1, \dots, s^i_d]$ for every $1 \le i \le n$. We say that s is *linear* if for every $1 \le j \le d$ a sequence $\tilde{s}_j = (s^1_j, \dots, s^n_j)$ is strictly increasing, strictly decreasing or constant and at least one sequence $\tilde{s}_j$ has to be nonconstant. A set of points $\{p^1, p^2, \dots, p^n\} \subseteq n^d$ is a line if it can be ordered into a linear sequence $(q^1, q^2, \dots, q^n)$. Beck [5] worked with ordered lines (the linear sequences in our case). However, for us it is more convenient to have unordered lines because some automorphisms will change the order of points in the line.

Let ℓ be a line and $q = (q^1, \dots, q^n)$ be an ordering of ℓ into a linear sequence. Note that every line in $\mathbb{L}(n^d)$ has two such ordering. Another ordering of ℓ into a linear sequence is $(q^n, \dots, q^1)$. We define a *type* of a sequence $\tilde{q}_j = (q^1_j, \dots, q^n_j)$ as $+$ if $\tilde{q}_j$ is strictly increasing, $-$ if $\tilde{q}_j$ is strictly decreasing, c if $\tilde{q}_j$ is constant and $q^i_j = c$ for every $1 \le i \le n$. A type of q is $\mathit{type}(q) = (\mathit{type}(\tilde{q}_1), \dots, \mathit{type}(\tilde{q_n}))$.

Type of a line ℓ is a type of an ordering of ℓ into a linear sequence. Since every line has two such ordering, every line has also two types. However, the second type of ℓ can be obtained by switching $+$ and $-$ in the first type. For example, let $\ell = \big\{[0,0,3],[0,1,2],[0,2,1],[0,3,0]\big\} \in \mathbb{L}(4^3)$ then $\mathit{type}(\ell) = \big\{(0,+,-),(0,-,+)\big\}$. However, for better readability we write only $\mathit{type}(\ell) = (0,+,-)$. We denote the i-th entry in $\mathit{type}(\ell)$ by $\mathit{type}(\ell)_i$.

Let us now define several terms we use in the rest of the paper. A *dimension* $\dim(\ell)$ of a line $\ell \in \mathbb{L}(n^d)$ is $\dim(\ell) = \big|\big\{i \in \{1,\dots,d\} | \mathit{type}(\ell)_i \in \{+,-\}\big\}\big|$. A *degree* $\deg(p)$ of a point $p \in n^d$ is a number of incident lines, formally $\deg(p) = \big|\{\ell \in \mathbb{L}(n^d) | p \in \ell\}\big|$. Two points $p_1, p_2 \in n^d$ are *collinear*, if there exists a line $\ell \in \mathbb{L}(n^d)$, such that $p_1 \in \ell$ and $p_2 \in \ell$. A point $p \in n^d$ is called a *corner* if p has coordinates only 0 and $n-1$. A point $p = [x_1, \dots, x_d] \in n^d$ is an *outer point* if there exists at least one $i \in \{1, \dots, d\}$ such that $x_i \in \{0, n-1\}$. If a point $p \in n^d$ is not an outer point then p is called an *inner point*.

A line $\ell \in \mathbb{L}(n^d)$ is called an *edge* if $\dim(\ell) = 1$ and ℓ contains two corners. Two corners are *neighbors* if they are connected by an edge. A line $\ell \in \mathbb{L}(n^d)$ with $\dim(\ell) = d$ is called *main diagonal*. We denote the set of all main diagonals by $\mathbb{L}_m(n^d)$. For better understanding the notions see Figure 1 with some examples in the cube 4^3.

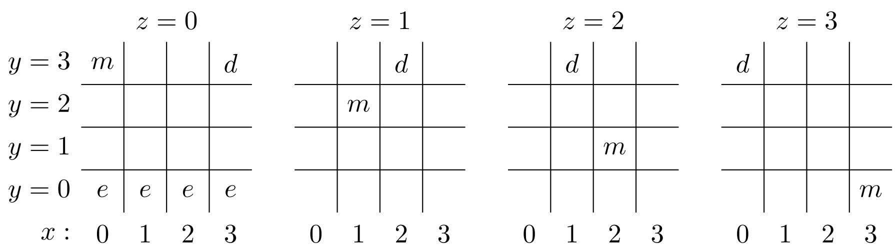

Fig. 1. A cube 4^3 with some examples of lines. An edge e has a type $(+, 0, 0)$, a line d has a dimension 2 and a type $(+, 3, -)$ and a main diagonal m has a type $(+, -, +)$.

A k-dimensional *face* F of the cube n^d is a maximal set of points of n^d, such that there exist two index sets $I, J \subseteq \{1, \ldots, d\}, I \cap J = \emptyset, |I| + |J| = d - k$ and for each point $[x_1, \ldots, x_d]$ in F holds that $x_i = 0$ for each $i \in I$ and, $x_j = n - 1$ for each $j \in J$. For example, $\{[x, y, 0, n-1] | x, y \in [n]\}$ is a 2-dimensional face of the cube n^4.

A point $p \in n^d$ is *fixed* by an automorphism T if $T(p) = p$. A set of points $\{p_1, \ldots, p_k\}$ is fixed by an automorphism T if $\{p_1, \ldots, p_k\} = \{T(p_1), \ldots, T(p_k)\}$. Note that if a set S is fixed it does not necessarily mean every point of S is fixed.

2.1 Order of $\mathbb{T}_2^d$

The cube 2^d is different from other cubes because every two points are collinear. Thus, we have the following proposition.

Proposition 1. *Order of the group* $\mathbb{T}_2^d$ *is* $(2^d)!$.

Proof. Every permutation of the points of the cube 2^d is an automorphism, as the graph H_2^d is the complete graph on 2^d vertices. □

We further assume that $n > 2$.

3 Automorphisms of n^3

For better understanding of our technique, we first show the result for the 3-dimensional case of the group $\mathbb{T}_n^3$. Here we state several general lemmas how an arbitrary automorphism maps main diagonals, edges and corners. The proofs are technical and are omitted from this conference paper.

Lemma 1. *Let* $F = \{[x, y, 0, \ldots, 0] | x, y \in [n]\}$ *be a face of* n^d*, and let an automorphism* $T \in \mathbb{T}_n^d$ *fixes all 4 corners of* F*, i.e., points* $[0, \ldots, 0]$*,* $[n-1, 0, \ldots, 0]$*,* $[0, n-1, 0, \ldots, 0]$ *and* $[n-1, n-1, 0, \ldots, 0]$*. Then, if* T *fixes a point* $[i, 0, \ldots, 0], i \in [n]$ *it also fixes a point* $[n-i-1, 0, \ldots, 0]$*.*

Lemma 2. *Every automorphism* $T \in \mathbb{T}_n^d$ *maps a main diagonal* $m \in \mathbb{L}_m(n^d)$ *onto a main diagonal* $m' \in \mathbb{L}_m(n^d)$*.*

Lemma 3. *Let $T \in \mathbb{T}_n^d$, e be an edge and p be a corner, such that $p \in e$. If the corner p is fixed by T, then $T(e) = e'$ is an edge such that $p \in e'$.*

Lemma 4. *If an automorphism $T \in \mathbb{T}_n^d$ fixes the corner $[0, \dots, 0]$ and all its neighbors, then T fixes all corners of the cube n^d.*

We also use the following easy observations.

Observation 3 *If an automorphism $T \in \mathbb{T}_n^d$ fixes two collinear points $p, q \in n^d$, then T also fixes a line $\ell \in \mathbb{L}(n^d)$ such that $p, q \in \ell$.*

Proof. For any two distinct points $p_1, p_2 \in n^d$ there is at most one line $\ell \in \mathbb{L}(n^d)$ such that $p_1, p_2 \in \ell$. Therefore, if the points p and q are fixed then the line ℓ has to be fixed as well. □

Observation 4 *If two lines $\ell_1, \ell_2 \in \mathbb{L}(n^d)$ are fixed by $T \in \mathbb{T}_n^d$ then their intersection, a point $p = \ell_1 \cap \ell_2$, is fixed by T.*

Proof. For any two lines ℓ, ℓ' there is at most one point in $\ell \cap \ell'$. Therefore, if the lines ℓ_1 and ℓ_2 are fixed then the point p has to be fixed as well. □

3.1 Generators of $\mathbb{T}_n^3$

In this section we characterize generators of the group $\mathbb{T}_n^3$. We use two basic groups of automorphisms. The group of permutation automorphisms $\mathbb{F}_n$. The group second group is the group of rotations $\mathbb{R}$ of a 3-dimensional cube. The generators of $\mathbb{R}$ are rotations

$$\begin{aligned} R_x\big([x, y, z]\big) &= [x, n - z - 1, y], \\ R_y\big([x, y, z]\big) &= [n - z - 1, y, x], \\ R_z\big([x, y, z]\big) &= [n - y - 1, x, z]. \end{aligned}$$

Definition 1. *Let $\mathbb{A}_n^3$ be a group generated by elements of $\mathbb{R} \cup \mathbb{F}_n$.*

We prove that $\mathbb{A}_n^3 = \mathbb{T}_n^3$. The idea of the proof, that resembles a similar proof of Silver [11], is composed of two steps:

1. For any automorphism $T \in \mathbb{T}_n^3$ we find an automorphism $A \in \mathbb{A}_n^3$ such that $T \circ A$ fixes every point in a certain set S.
2. If an automorphism $T' \in \mathbb{T}_n^3$ fixes every point in S then T' is the identity.

Hence, for every $T \in \mathbb{T}_n^3$ we find an inverse element T' such that T' is composed only by elements of $\mathbb{R} \cup \mathbb{F}_n$, therefore $T \in \mathbb{A}_n^3$. The proof of the second part is very similar to the proof for a general cube n^d. Thus, it is proved only for the general cube in the next section.

Theorem 5. *For every $T \in \mathbb{T}_n^3$ there exists $A \in \mathbb{A}_n^3$, such that $T \circ A$ fixes all corners and every point of the line $\ell = \big\{[i, 0, 0] | i \in [n]\big\}$.*

Proof. First we find an automorphism $A' \in \mathbb{A}_n^3$ such that $T \circ A'$ fixes all corners. We start with the point $p_0 = [0,0,0]$. A point $T(p_0)$ has to be on a main diagonal (by Lemma 2). Without loss of generality $T(p_0) = [i,i,n-i-1]$. We take $f_\pi \in \mathbb{F}_n$ such that $\pi(i) = 0$, $\pi(0) = i$, $\pi(n-i-1) = n-1$, $\pi(n-1) = n-i-1$, and $\pi(k) = k$ otherwise. Therefore, $T \circ F_\pi(p_0)$ is a corner. Then we take $R_1 \in \mathbb{R}$ such that the automorphism $T_1 = T \circ F_\pi \circ R_1$ fixes p_0.

By Lemma 3 the line $T_1(\ell)$ must be mapped onto an edge e such that $p_0 \in e$. If the corner $p_1 = [n-1,0,0]$ is fixed by T_1, we take $T_2 = T_1$. Otherwise it can be mapped onto $[0,n-1,0]$ (or $[0,0,n-1]$). We take a rotation $R_2\big([x,y,z]\big) = [y,z,x]$ (or $[z,x,y]$). Thus, the automorphism $T_2 = T_1 \circ R_2$ fixes corners p_1 and p_0. Note that $R_2\big([0,0,0]\big) = [0,0,0]$.

If a corner $p_2 = [0,n-1,0]$ is fixed by T_2 we take $T_3 = T_2$. Otherwise it can be mapped only onto $[0,0,n-1]$. We take a rotation $R_3\big([x,y,z]\big) = [n-x-1, n-z-1, n-y-1]$ and permutation automorphism F_σ, where $\sigma(i) = n-i-1$. Hence, $T_3 = T_2 \circ R_3 \circ F_\sigma$ fixes the points p_0, p_1, p_2 as follows. For p_0,

$$T_2 \circ R_3 \circ F_\sigma\big([0,0,0]\big) = R_3 \circ F_\sigma\big([0,0,0]\big) = F_\sigma\big([n-1,n-1,n-1]\big) = [0,0,0].$$

For p_1,

$$T_2 \circ R_3 \circ F_\sigma\big([n-1,0,0]\big) = R_3 \circ F_\sigma\big([n-1,0,0]\big) = F_\sigma\big([0,n-1,n-1]\big) = [n-1,0,0].$$

For p_2,

$$T_2 \circ R_3 \circ F_\sigma\big([0,n-1,0]\big) = R_3 \circ f_\sigma\big([0,0,n-1]\big) = f_\sigma\big([n-1,0,n-1]\big) = [0,n-1,0].$$

A corner $p_3 = [0,0,n-1]$ is fixed by T_3 automatically, because it is neighbor of p_0 and all others neighbors are already fixed. All other corners are fixed due to Lemma 4. The automorphism $T_3 = T \circ A'$ for some $A' \in \mathbb{A}_n^3$ fixes all corners of the cube n^3.

Now we find an automorphism A such that $T \circ A$ fixes all corners and all points on the line ℓ. The line ℓ is fixed by T_3 due to Observation 3. Let $k = \lfloor \frac{n}{2} \rfloor - 1$. We construct the automorphism A by induction over $i \in \{0,\dots,k\}$. We show that in a step i an automorphism Y_i fixes all corners and every point in a set

$$Q_i = \big\{[j,0,0], [n-j-1,0,0] | 0 \le j \le i\big\}.$$

First, let $i = 0$ and $Y_0 = T_3$. The automorphism Y_0 fixes all corners and Q_0 contains only $[0,0,0]$ and $[n-1,0,0]$, which are also corners. Suppose that $i > 0$. By induction hypothesis, we have an automorphism Y_{i-1} which fixes all corners and every point in the set Q_{i-1}. If $Y_{i-1}([i,0,0]) = [i,0,0]$ then $Y_i = Y_{i-1}$. Otherwise $Y_{i-1}([i,0,0]) = [j,0,0]$. Note that $i < j < n-i-1$ because points from Q_{i-1} are already fixed. Let us consider $F_\pi^i \in \mathbb{F}_n$ where $\pi(j) = i$, $\pi(i) = j$, $\pi(n-j-1) = n-i-1$, $\pi(n-i-1) = n-j-1$, and $\pi(k) = k$ otherwise. The automorphism $Y_i = Y_{i-1} \circ F_\pi^i$ fixes the following points:

1. All corners, as the automorphism Y_{i-1} fixes all corners by the induction hypothesis and $\pi(0) = 0$ and $\pi(n-1) = n-1$.

2. Set Q_{i-1}, as the automorphism Y_{i-1} fixes the set Q_{i-1} by the induction hypothesis and $\pi(k) = k$ for all $k < i$ and $k > n - i - 1$.
3. Point $[i, 0, 0]$: $Y_{i-1} \circ F^i_\pi\big([i, 0, 0]\big) = F^i_\pi\big([j, 0, 0]\big) = [i, 0, 0]$.
4. Point $[n - i - 1, 0, 0]$ by Lemma 1.

Note that if n is odd a point $[\frac{n-1}{2}, 0, \ldots, 0]$ is fixed as well by an automorphism Y_k. Thus, the automorphism $Y_k = T \circ A$ for some $A \in \mathbb{A}^d_n$ fixes all points of the line ℓ and all corners of the cube. □

4 Generators of the Group $\mathbb{T}^d_n$

In this section we characterize the generators of the general group $\mathbb{T}^d_n$. As we stated in Section 1, we use the groups $\mathbb{R}_d$, $\mathbb{F}_n$ and $\mathbb{X}$.

Definition 2. *Let $\mathbb{A}^d_n$ be a group generated by elements of $\mathbb{R}_d \cup \mathbb{F}_n \cup \mathbb{X}$.*

We prove that $\mathbb{A}^d_n = \mathbb{T}^d_n$ in the same two steps as we proved $\mathbb{A}^3_n = \mathbb{T}^3_n$.

1. For any automorphism $T \in \mathbb{T}^d_n$ we find an automorphism $A \in \mathbb{A}^d_n$, such that $T \circ A$ fixes all corners of the cube n^d and one edge.
2. If an automorphism $T' \in \mathbb{T}^d_n$ fixes all corners and one edge then T' is identity.

Theorem 6. *For all $T \in \mathbb{T}^d_n$ there exists $A \in \mathbb{A}^d_n$ such that $T \circ A$ fixes every corner of the cube n^d and every point of a line $\ell = \big\{[i, 0, \ldots, 0] | i \in [n]\big\}$.*

Proof (Sketch). First we construct an automorphism $A' \in \mathbb{A}^n_d$ such that $T \circ A'$ fixes all corners. We start with the point $p_0 = [0, \ldots, 0]$. By Lemma 2, the point $T(p_0)$ has to be on a main diagonal. We choose $F \in \mathbb{F}_n$ such that $T \circ F(p_0)$ is a corner. Then, we choose $R \in \mathbb{R}_d$ such that $T \circ F \circ R(p_0) = p_0$.

By induction over i we can construct automorphisms Z_i to fix the points p_0 and

$$p_i = [0, \ldots \underset{i}{n - 1}, \ldots 0]$$

for all $i \in \{0, \ldots, d-2\}$. We start with the automorphism $Z_0 = T \circ F \circ R$ and in a step i we compose the automorphism Z_{i-1} with a suitable rotation in $\mathbb{R}^d$. If Z_{d-2} fixes p_{d-1}, then $Z_{d-1} = Z_{d-2}$. Otherwise p_{d-1} is mapped onto p_d and then $Z_{d-1} = Z_{d-2} \circ X$, where $X \in \mathbb{X}$ and $X \neq Id$. Thus, the automorphism Z_{d-1} fixes all points of P_{d-1} and the corner p_d is fixed automatically because there is no other possibility where the corner p_d can be mapped. The automorphism Z_{d-1} fixes the corner $p_0 = [0, \ldots, 0]$ and all its neighbors. Therefore by Lemma 4, the automorphism $Z_{d-1} = T \circ A'$ for some $A' \in \mathbb{A}^n_d$ fixes all corners of the cube.

The automorphism fixing points on the line ℓ is constructed in the same way as in the proof of Theorem 5. We find an automorphism Y fixing all corners and points on the line ℓ by induction. We start with the automorphism Z_{d-1}. In step i of the induction we compose the automorphism from the step $i - 1$ and an automorphism $F_i \in \mathbb{F}_n$ which fixes points $[i, 0, \ldots, 0]$ and $[n - i - 1, 0, \ldots, 0]$. □

It remains to prove that if an automorphism $T \in \mathbb{T}_n^d$ fixes all corners and all points in the line $\ell = \{[i, 0, \ldots, 0] | i \in [n]\}$ then T is the identity. We prove it in two parts. First, we prove that if $d = 2$ then the automorphism T is the identity. Then, we prove it for a general dimension by an induction argument.

Theorem 7. *Let an automorphism $T \in \mathbb{T}_n^2$ fixes all corners of the cube and all points in the line $\ell = \{[i, 0] | i \in [n]\}$. Then, the automorphism T is the identity.*

Proof. Let $d_1, d_2 \in \mathbb{L}(n^2)$. Thus, $type(d_1) = (+, +)$ and $type(d_2) = (+, -)$. Since all corners are fixed, the diagonals d_1 and d_2 are fixed as well due to Observation 3. Let $p \in d_1 \cup d_2$ such that p is not a corner. The point p is collinear with the only one point $q \in \ell$ such that q is not a corner. Therefore, every point on the diagonals d_1 and d_2 is fixed.

Now we prove that every line in $\mathbb{L}(n^2)$ is fixed. Let $\ell_1 \in \mathbb{L}(n^2)$ be a line of a dimension 1. Suppose n is even. The line ℓ_1 intersects the diagonals d_1 and d_2 in distinct points, which are fixed. Therefore, the line ℓ_1 is fixed as well by Observation 3.

Now suppose n is odd. If ℓ_1 does not contain the face center $c_1 = [\frac{n-1}{2}, \frac{n-1}{2}, 0, \ldots, 0]$ then ℓ is fixed by the same argument as in the previous case. Thus, suppose $c_1 \in \ell_1$. There are two lines ℓ_2, ℓ_3 in $\mathbb{L}(n^2)$ of dimension 1 which contains c_1. Their types are $type(\ell_2) = (\frac{n-1}{2}, +)$ and $type(\ell_3) = (+, \frac{n-1}{2})$. The line ℓ_2 also intersects the line ℓ. Therefore, the lines contains two fixed points c_1 and $[\frac{n-1}{2}, 0]$ and thus the line ℓ_2 is fixed. The line ℓ_3 is fixed as well because every other line is fixed. For better understanding of all lines and points used in the proof see Figure 2 with example of the cube 5^2.

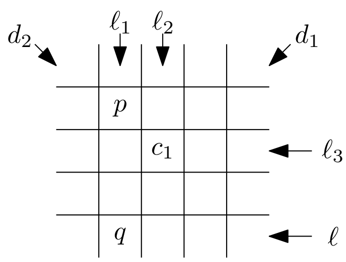

Fig. 2. Points and lines used in the proof of Theorem 7.

Every point in 5^2 is fixed due to Observation 4 because every point is in an intersection of at least two fixed lines. □

Theorem 8. *Let an automorphism $T \in \mathbb{T}_n^d$ fix all corners of the cube n^d and all points of an arbitrary edge e. Then, the automorphism T is the identity.*

Proof. We prove the theorem by induction over dimension d of the cube n^d. The basic case for $d = 2$ is Theorem 7.

Therefore, we can suppose $d > 2$ and the theorem holds for all dimensions smaller then d. Without loss of generality, $e = \{[i, 0, \dots, 0] | i \in [n]\}$. We consider the face $F = \{[x_1, \dots, x_{d-1}, 0] | x_1, \dots, x_{d-1} \in [n]\}$. The face F has a dimension $d-1$ and $e \subset F$. Therefore, all points of F are fixed by the induction hypothesis. Then we take all faces G of dimension $d-1$ such that $F \cap G \neq \emptyset$. Corners $c \in G$ are fixed. There is at least one edge f such that $f \subseteq F \cap G$. Therefore the points of f are also fixed and the points $p \in G$ are fixed by the induction hypothesis. By this argument we show that every outer point is fixed. Every line $\ell \in \mathbb{L}(n^d)$ is fixed due to Observation 3 because every line contains at least two outer points. Therefore by Observation 4, every point $q \in n^d$ is fixed because every point is an intersection of at least two lines. □

5 Order of the Group $\mathbb{T}_n^d$

In the previous section we characterized the generators of the group $\mathbb{T}_n^d$. Now we compute the order of $\mathbb{T}_n^d$. First, we state several technical lemmas whose proofs are omitted in this conference paper.

Lemma 5. *Orders of the basic groups are as follows.*

1. $|\mathbb{R}_d| = 2d|\mathbb{R}_{d-1}| = 2^{d-1}d!$, $|\mathbb{R}_2| = 4$
2. $|\mathbb{F}_n| = \prod_{i=0}^{\lfloor \frac{n}{2} \rfloor - 1} (2\lfloor \frac{n}{2} \rfloor - 2i)$
3. $|\mathbb{X}| = 2$

Lemma 6. *The groups $\mathbb{R}_d$ and $\mathbb{F}_n$ commute, and the groups $\mathbb{X}$ and $\mathbb{F}_n$ commute.*

Lemma 7. *Let $X \in \mathbb{X}$ such that $X \neq Id$. Then, for all $R_1 \in \mathbb{R}_d$ there exists $R_2 \in \mathbb{R}_d$ such that $R_1 \circ X = X \circ R_2$.*

By Lemma 6 and Lemma 7 we can conclude that any automorphism $A \in \mathbb{T}_n^d$ can be written as $A = R \circ F \circ X$ where $R \in \mathbb{R}_d$, $F \in \mathbb{F}_n$ and $X \in \mathbb{X}$. Thus, the product

$$\mathbb{R}_d\mathbb{F}_n\mathbb{X} = \{R \circ F \circ X | R \in \mathbb{R}_d, F \in \mathbb{F}_n, X \in \mathbb{X}\}$$

is exactly the group $\mathbb{T}_n^d$. We state the well-known product formula for a group product.

Lemma 8 (Product formula [4]). *Let S and T be subgroups of a finite group G. Then, for an order of a product ST holds that*

$$|ST| = \frac{|S| \cdot |T|}{|S \cap T|}.$$

Thus, for computing the order of $\mathbb{T}_n^d$ we need to compute the orders of intersections of the basic groups $\mathbb{R}_d$, $\mathbb{F}_n$ and $\mathbb{X}$.

Lemma 9. *If d is odd, then $\mathbb{R}_d \cap \mathbb{F}_n = \{Id\}$. If d is even, then $\mathbb{R}_d \cap \mathbb{F}_n = \{Id, F_\sigma\}$ where $\sigma(i) = n - i - 1$.*

Lemma 10. *The group $\mathbb{X}$ can be generated by elements of the groups $\mathbb{R}_d$ and $\mathbb{F}_n$ if and only if d is odd.*

Theorem 9. *The order of the group $\mathbb{T}_n^d$ is $|\mathbb{R}_d| \cdot |\mathbb{F}_n|$.*

Proof. If d is odd $|\mathbb{R}_d \cap \mathbb{F}_n| = 1$ due to Lemma 9. Moreover, the group $\mathbb{X}$ is a subset of $\mathbb{R}_d\mathbb{F}_n$ due to Lemma 10. Therefore, the group $\mathbb{T}_n^d$ is exactly a product $\mathbb{R}_d\mathbb{F}_n$ and the theorem holds by Lemma 8.

Now suppose d is even. By Lemma 9, $|\mathbb{R}_d \cap \mathbb{F}_n| = 2$. Thus by Lemma 8, $|\mathbb{R}_d\mathbb{F}_n| = |\mathbb{R}_d| \cdot |\mathbb{F}_n|/2$. The order of the intersection $|\mathbb{X} \cap \mathbb{R}_d\mathbb{F}_n|$ is 1 by Lemma 10. Hence, $|\mathbb{T}_n^d| = 2|\mathbb{R}_d\mathbb{F}_n| = |\mathbb{R}_d| \cdot |\mathbb{F}_n|$. □

As a corollary of Theorem 9 we get the second part of Theorem 1.

Corollary 1. *Let $k = \lfloor \frac{n}{2} \rfloor$. Then, $|\mathbb{T}_d^n| = 2^{d-1+k} d! k!$.*

Proof. By Theorem 9, the order $|\mathbb{T}_d^n|$ is $2^{d-1} d! \prod_{i=0}^{k-1} (2k - 2i)$ for $k = \lfloor \frac{n}{2} \rfloor$. There are k even numbers from 2 to $2k$ in the product $\prod_{i=0}^{k-1} (2k - 2i)$. Therefore, it can be rewritten as $2^k k!$. □

Corollary 2. *The groups $\mathbb{T}_{2k}^d$ and $\mathbb{T}_{2k+1}^d$ are isomorphic for $k \geq 2$.*

Proof. The rotation group for generating $\mathbb{T}_{2k}^d$ and $\mathbb{T}_{2k+1}^d$ is the same. For every permutation $\pi \in \mathbb{S}_{2k+1}$ with the symmetry property holds that $\pi(k) = k$. Therefore, the group $\mathbb{F}_{2k}$ is isomorphic to the group $\mathbb{F}_{2k+1}$. Whether $\mathbb{X}$ is generated by $\mathbb{F}_n$ and $\mathbb{R}_d$ depends only on the dimension. □

6 The Complexity of Colored Cube Isomorphism

In this section we prove Theorem 2. As we stated before, CHI is in GI. Therefore, Colored Cube Isomorphism as a subproblem of CHI is in GI as well. It remains to prove the problem is GI-hard.

First, we describe how we reduce the input of Graph Isomorphism to the input of Colored Cube Isomorphism. Let $G = (V, E)$ be a graph. Without loss of generality $V = \{0, \dots, n-1\}$. We construct the coloring $s^G : [k]^2 \to [2], k = 2n + 4$ as follows. The value of $s^G([i, j])$ is 1 if $[i, j] = [n, n]$ or $[i, j] = [n, n+1]$ or $i, j \leq n - 1$ and $\{i, j\} \in E$. The value of $s^G(p)$ for all other point p is 0. We can view the coloring s^G as a matrix M^G such that $M_{i,j}^G = s^G([i, j])$. The submatrix of M^G consisting of the first n rows and n columns is exactly the adjacency matrix of the graph G.

The idea of the reduction is as follows. If two colorings s^{G_1}, s^{G_2} are isomorphic via a cube automorphism $A \in \mathbb{T}_n^d$ then A can be composed only of permutation automorphisms in $\mathbb{F}_k$. Moreover, if $A = F_\pi$ for some permutation π then the permutation π maps the numbers in $[n]$ to the numbers in $[n]$ and describes the isomorphism between the graphs G_1 and G_2.

Lemma 11. *Let G_1, G_2 be graphs without vertices of degree 0. If colorings s^{G_1}, s^{G_2} are isomorphic via a cube automorphism A then $A = F_\pi \in \mathbb{F}_k$. Moreover, $\pi(i) \leq n-1$ if and only if $i \leq n-1$.*

Proof (Sketch). Let $A = R \circ X \circ F$ where $R \in \mathbb{R}_2, X \in \mathbb{X}, F \in \mathbb{F}_k$ and m_1, m_2 be main diagonals of $[k]^2$ of type $(+,+)$ and $(+,-)$, respectively. Due to the colors of $[n,n]$ and $[n,n+1]$ we can show that A has to fix m_1 and m_2 and that $A \in F_k$. Moreover, if $A = F_\pi$ then $\pi(n) = n$ and $\pi(n+1) = n+1$.

For every $i \leq n-1$ there is at least one point with color 1 on a line of type $(+,i)$ in both colorings s^{G_1}, s^{G_2} because graphs G_1 and G_2 do not contain any vertex of degree 0. On the other hand, for every $i \geq n+2$ there are only points with color 0 on a line of type $(+,i)$ in both colorings. Therefore, if $i \leq n-1$ then i has to be mapped on $j \leq n-1$ by π. □

The proof of the following theorem follows from Lemma 11.

Theorem 10. *Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be graphs without vertices of degree 0. Then, the graphs G_1 and G_2 are isomorphic if and only if the colorings s^{G_1} and s^{G_2} are isomorphic.*

We may suppose that inputs graphs G_1 and G_2 have minimum degree at least 1 for the purpose of the polynomial reduction of Graph Isomorphism to Colored Cube Isomorphism. Thus, Theorem 2 follows from Theorem 10.

References

1. L. V. Allis. *Searching for Solutions in Games and Artificial Intelligence.* PhD thesis, University of Limburg, 1994.
2. V. Arvind, B. Das, J. Köbler, and S. Toda. Colored hypergraph isomorphism is fixed parameter tractable. *Algorithmica*, 71, 2015.
3. V. Arvind and Johannes Köbler. *STACS 2006: 23rd Annual Symposium on Theoretical Aspects of Computer Science, Marseille, France, February 23-25, 2006. Proceedings*, chapter On Hypergraph and Graph Isomorphism with Bounded Color Classes. Springer Berlin Heidelberg, 2006.
4. A. Ballester-Bolinches, R. Esteba-Romero, and M. Asaad. *Products of Finite Groups.* Be Gruyter, 2010.
5. J. Beck. *Tic-tac-toe theory.* Cambridge university press, 2006.
6. K. S. Booth and C. J. Colbourn. Problems polynomially equivalent to graph isomorphism. Technical Report CS-77/04, Department of Computer Science, University of Waterloo, 1977.
7. S. A. Choudum and V. Sunitha. Automorphisms of augmented cubes. *International Journal of Computer Mathematics*, 85, 2008.
8. A.W. Hales and R. Jewett. On regularity and positional games. *Transactions of the American Mathematical Society*, 106, 1963.
9. F. Harary. The automorphism group of a hypercube. *Journal of Universal Computer Science*, 6, 2000.
10. O. Patashnik. Qubic: $4 \times 4 \times 4$ tic-tac-toe. *Mathematics Magazine*, 53, 1980.
11. R. Silver. The group of automorphisms of the game of 3-dimensional ticktacktoe. *The American Mathematical Monthly*, 74, 1967.