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 n^d where the vertices are points of the d-dimensional 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 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 n^d there exists an automorphism of n^d preserving the colors. We show that this problem is GI-complete. [3]

1 Introduction

Let us denote $[n] = \{1, \dots, n\}$. Let $[n]^d$ be the set of all points $(p_1, \dots, p_d)$ such that $p_i \in [n]$ for every $1 \le i \le d$. Let $s = (s^1, \dots, s^n)$ be a sequence of n distinct points of $[n]^d$. 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. Note that at least one sequence $\tilde{s}_j$ is nonconstant as s is a sequence of n distinct points. 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 $(q^1, q^2, \dots, q^n)$. We denote the set of all lines of $[n]^d$ by $\mathbb{L}(n^d)$. A *combinatorial cube* n^d is a hypergraph $\big([n]^d, \mathbb{L}(n^d)\big)$. Note that there is a fundamental difference between the combinatorial cube n^d and another well-studied structure, the *hypercube* Q_d, defined as the graph $Q_d = \big(\{0,1\}^d, E\big)$ where $\{u, v\} \in E$ if and only if the vectors u, v differ in exactly one coordinate.

We denote the group of all permutations on n elements by $\mathbb{S}_n$. A permutation $S \in \mathbb{S}_{n^d}$ is an *automorphism* of the cube n^d if $\ell = \{v_1, \dots, v_n\} \in \mathbb{L}(n^d)$ implies

⋆ 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 Czech Science Foundation GAČR (grant #19-27871X).

⋆⋆ T. Valla acknowledges the support of the OP VVV MEYS funded project 10 CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics".

[3] A preliminary version of this work appeared in the proceedings of Computing and Combinatorics – 22nd International Conference, COCOON 2016.

$S(\ell) = \{S(v_1), \dots, S(v_n)\} \in \mathbb{L}(n^d)$. 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 two groups of automorphisms for characterization of the group $\mathbb{T}_n^d$ as follows.

The first is a group $\mathbb{G}_n^d$ which is isomorphic to the hypercube automorphism group $\mathbb{Q}_d$ [10]. Generators of $\mathbb{Q}_d$ are

1. *Translations* T_a by $a \in \{0,1\}^d$, $T_a([x_1, \dots, x_d]) = [x_1 + a_1, \dots, x_d + a_d]$ where the sum is modulo 2.
2. *Rotations* R_π by $\pi \in \mathbb{S}_d$, $R_\pi([x_1, \dots, x_d]) = [x_{\pi(1)}, \dots, x_{\pi(d)}]$.

It is known that every automorphism of the hypercube can be composed as $T \circ R$ for a translation T and a rotation R. To use automorphisms in $\mathbb{Q}_d$ for the combinatorial cube, we need to change the definition of the translations. The rotations can be used immediately. Thus, the group $\mathbb{G}_n^d$ is generated by

1. *Translations* T_a by $a \in \{0,1\}^d$, $T_a([x_1, \dots, x_d]) = [\mathit{flip}(x_1, a_1), \dots, \mathit{flip}(x_d, a_d)]$ where
$$\mathit{flip}(i, b) = \begin{cases} i & b = 0, \\ n - i + 1 & b = 1. \end{cases}$$
2. *Rotations* R_π by $\pi \in \mathbb{S}_d$, $R_\pi([x_1, \dots, x_d]) = [x_{\pi(1)}, \dots, x_{\pi(d)}]$.

It is clear that groups $\mathbb{G}_n^d$ and $\mathbb{Q}_d$ are isomorphic and thus every automorphism in $\mathbb{G}_n^d$ can be composed as $T \circ R$ for a translation T and a rotation R.

The second group is a group of permutation automorphisms $\mathbb{F}_n$ that contains mappings $F_\rho([x_1, \dots, x_d]) = [\rho(x_1), \dots, \rho(x_d)]$ where $\rho \in \mathbb{S}_n$ such that it has a *symmetry property*: if $\rho(i) = j$ then $\rho(n - i + 1) = n - j + 1$.

Our main result is summarized in the following theorem. For the proof we use and generalize some ideas of Silver [12], who characterized the group of automorphisms of the cube 4^3.

Theorem 1. *Let $n > 2$. The group $\mathbb{T}_n^d$ is generated by the elements of $\mathbb{G}_n^d \cup \mathbb{F}_n$. 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 $\{v_1, \dots, v_r\} \subseteq V_1$, $\{v_1, \dots, v_r\} \in E_1 \Leftrightarrow \{f(v_1), \dots, f(v_r)\} \in E_2$. 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[4] for CHI—see Arvind et. al. [3, 2]. The problem Colored Cube Isomorphism is defined as the problem CHI where both $H_1, H_2 = n^d$. 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 decision 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* $n^2 \to [2]$.

The paper is organized as follows. In Section 2 we present some basic properties of the combinatorial cube n^d, prove that $\mathbb{G}_n^d$ and $\mathbb{F}_n$ are automorphism groups and also we count the order of the group $\mathbb{T}_2^d$, which structure is different from other automorphism groups. Next in Sections 3 and 4, we characterize the generators for $\mathbb{T}_n^d$. 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 prove Theorem 2.

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 is a draw if both players play optimally. However, the game can be generalized to a 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 [11] 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

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

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 results are usually achieved for large n or large d. For example, by the famous Hales and Jewett theorem [9], for any n there is (an enormously large) d such that the hypergraph 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 [12] 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 n^d has polynomially many edges in the number of vertices. Therefore, from a point of view of polynomial-time algorithms it does not matter if there are hypergraphs n^d with colorings or only colorings on the input of Colored Cube Isomorphism. 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, 10]).

2 Preliminaries

Beck [5] in his work defined lines to be ordered (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 $q = (q^1, \ldots, q^n)$ be an ordering of ℓ into a linear sequence. Note that every line in $\mathbb{L}(n^d)$ has two such orderings. Another ordering of ℓ into a linear sequence is $(q^n, \ldots, q^1)$. We define a *type* of a sequence $\tilde{q}_j = (q_j^1, \ldots, q_j^n)$ as $+$ if $\tilde{q}_j$ is strictly increasing, $-$ if $\tilde{q}_j$ is strictly decreasing, c if $\tilde{q}_j$ is constant and $q_j^i = c$ for every $1 \le i \le n$. A type of q is $\mathit{type}(q) = \big(\mathit{type}(\tilde{q}_1), \ldots, \mathit{type}(\tilde{q}_n)\big)$.

Type of a line ℓ is a type of an ordering q of ℓ into a linear sequence such that the first non-constant entry of $type(q)$ is $+$. For example, let

$$\ell = \big\{[1,1,4],[1,2,3],[1,3,2],[1,4,1]\big\} \in \mathbb{L}(4^3)$$

and q_1 and q_2 be distinct orderings of ℓ into a linear sequence. Then, $type(q_1) = (1,+,-)$ and $type(q_2) = (1,-,+)$. By definition $type(\ell) = type(q_1) = (1,+,-)$.

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 $\dim(\ell) = \big|\big\{i \in \{1,\dots,d\} | type(\ell)_i \in \{+,-\}\big\}\big|$. 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 1 and n. 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 $x_i \in \{1,n\}$. 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 a *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.

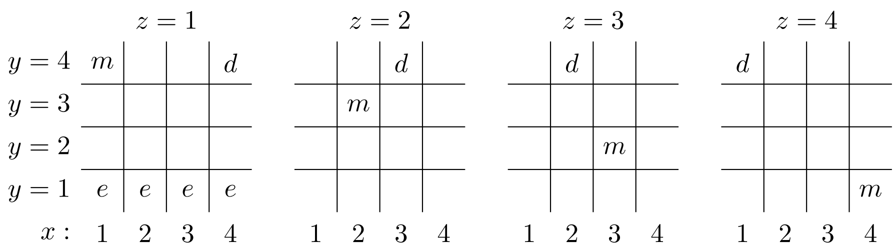

Fig. 1. The cube 4^3 with some examples of lines. An edge e has a type $(+,1,1)$, a line d has a dimension 2 and a type $(+,4,-)$ and a main diagonal m has a type $(+,-,+)$.

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 $I, J \subseteq \{1,\dots,d\}, I \cap J = \emptyset, |I| + |J| = d - k$ and for each point $[x_1,\dots,x_d]$ in F holds that $x_i = 1$ for each $i \in I$ and, $x_j = n$ for each $j \in J$. For example, $\big\{[x,y,1,n] | x,y \in [n]\big\}$ is a 2-dimensional face of the cube n^4. Note that an edge is an 1-dimensional face.

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

For n odd, we denote $\gamma = \frac{n+1}{2}$ and the *center* of the cube n^d is the point $c = [\gamma,\dots,\gamma]$.

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

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

Proposition 1. *The 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 2^d is the complete graph on 2^d vertices. □

We further assume that $n > 2$.

2.2 Basic Groups

In this subsection we prove that the basic groups $\mathbb{F}_n$ and $\mathbb{G}_n^d$ are groups of automorphisms of the combinatorial cube n^d. In the following proofs we use ℓ as an arbitrary line and $q = (q^1, \dots, q^n)$ as an ordering of ℓ into a linear sequence.

Lemma 1. *Every $F_\rho \in \mathbb{F}_n$ is an automorphism of the combinatorial cube n^d.*

Proof. We recall that $F_\rho\big([x_1, \dots, x_d]\big) = \big[\rho(x_1), \dots, \rho(x_d)\big]$ where $\rho \in \mathbb{S}_n$. Let $\sigma = \rho^{-1}$ and

$$p = \Big(\big[\rho\big(q_1^{\sigma(1)}\big), \dots, \rho\big(q_d^{\sigma(1)}\big)\big], \dots, \big[\rho\big(q_1^{\sigma(n)}\big), \dots, \rho\big(q_d^{\sigma(n)}\big)\big]\Big).$$

We claim that p is an ordering of $F_\rho(\ell)$ into a linear sequence. Consider sequences of the j-th coordinations of q and p. Thus,

$$\begin{aligned} \tilde{q}_j &= \big(q_j^1, \dots, q_j^n\big), \\ \tilde{p}_j &= \Big(\rho\big(q_j^{\sigma(1)}\big), \dots, \rho\big(q_j^{\sigma(n)}\big)\Big). \end{aligned}$$

If $\mathit{type}(\tilde{q}_j) = c$ then clearly $\mathit{type}(\tilde{p}_j) = \rho(c)$. If $\mathit{type}(\tilde{q}_j) = +$ then $q_j^i = i$ and

$$\Big(\rho\big(q_j^{\sigma(1)}\big), \dots, \rho\big(q_j^{\sigma(n)}\big)\Big) = \Big(\rho\big(\sigma(1)\big), \dots, \rho\big(\sigma(n)\big)\Big) = (1, \dots, n).$$

Thus, $\mathit{type}(\tilde{p}_j) = +$. In the last case, if $\mathit{type}(\tilde{q}_j) = -$ then $q_j^i = n - i + 1$. In this case we use that ρ has the symmetry property $\big(\rho(n - i + 1) = n - \rho(i) + 1\big)$. For all $i \in [n]$ holds that

$$\rho\big(q_j^{\sigma(i)}\big) = \rho\big(n - \sigma(i) + 1\big) = n - i + 1.$$

Thus, $\big(\rho\big(q_j^{\sigma(1)}\big), \dots, \rho\big(q_j^{\sigma(n)}\big)\big) = (n, \dots, 1)$ and $\mathit{type}(\tilde{p}_j) = -$. Therefore, we prove that $F_\rho(\ell)$ is a line. □

Lemma 2. *Every translation $T_a \in \mathbb{G}_n^d$ is an automorphism of the combinatorial cube n^d.*

Proof. We recall that $T_a\big([x_1 \ldots, x_d]\big) = \big[\mathit{flip}(x_1, a_1), \ldots, \mathit{flip}(x_d, a_d)\big]$, where

$$\mathit{flip}(i, b) = \begin{cases} i & b = 0, \\ n - i + 1 & b = 1. \end{cases}$$

Let $p = \big(T_a(q^1), \ldots, T_a(q^n)\big)$. We prove that p is an ordering of $T_a(\ell)$ into a linear sequence. Consider a sequence $\tilde{q}_j$ (or $\tilde{p}_j$) of the j-th coordinates of q (or p). If $\mathit{type}(\tilde{q}_j) = c$ then $\mathit{type}(\tilde{p}_j) = c$ if $a_j = 0$ or $\mathit{type}(\tilde{p}_j) = n - c + 1$ if $a_j = 1$. If $\mathit{type}(\tilde{q}_j) = +$ then $p^i_j = i$ if $a_j = 0$ or $p^i_j = n - i + 1$ if $a_j = 1$. Thus,

$$\big(T_a(q^1)_j, \ldots, T_a(q^n)_j\big) = \begin{cases} (1, \ldots, n) & a_j = 0, \\ (n, \ldots, 1) & a_j = 1. \end{cases}$$

Thus, $\mathit{type}(\tilde{p}_j) = +$ or $-$ depending on a_j. If $\mathit{type}(\tilde{q}_j) = -$ the situation is opposite. If $a_j = 0$ then $p^i_j = n - i - 1$ and $p^i_j = i$ if $a_j = 1$. Thus, again $\mathit{type}(\tilde{p}_j) = +$ or $-$. $\square$

Lemma 3. *Every rotation $R_\pi \in \mathbb{G}^d_n$ is an automorphism of the combinatorial cube n^d.*

Proof. We recall that $R_\pi\big([x_1 \ldots, x_d]\big) = [x_{\pi(1)}, \ldots, x_{\pi(d)}]$, where $\pi \in \mathbb{S}_d$. We claim that $p = \big(R_\pi(q^1), \ldots, R_\pi(q^n)\big)$ is an ordering of $R_\pi(\ell)$ into a linear sequence. Let $\tilde{q}_j$ and $\tilde{p}_j$ be sequences of j-th coordinates of q or p, respectively. Let $\sigma = \pi^{-1}$. Note that the sequence $\tilde{p}_j$ is exactly the sequence $\tilde{q}_{\sigma(j)}$. Thus, every sequence $\tilde{p}_j$ has a type $+$, $-$ or a constant. $\square$

3 Corners, Main Diagonals and Edges

In this section we investigate how every automorphism $S \in \mathbb{T}^d_n$ maps main diagonals, edges and corners. First, we prove some easy observation, which were also used by Silver [12].

Observation 3 *If an automorphism $S \in \mathbb{T}^d_n$ fixes two collinear points $p, q \in [n]^d$, then S 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. $\square$

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

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. $\square$

Lemma 4. *Let $F = \{[x, y, 1, \ldots, 1] | x, y \in [n]\}$ be a 2-dimensional face of n^d, and let an automorphism $S \in \mathbb{T}_n^d$ fixes all 4 corners of F, i.e., points $[1, \ldots, 1]$, $[n, 1, \ldots, 1]$, $[1, n, 1, \ldots, 1]$ and $[n, n, 1, \ldots, 1]$. Then, if S fixes a point $[i, 1, \ldots, 1], i \in [n]$ it also fixes a point $[n - i + 1, 1, \ldots, 1]$.*

Proof. The automorphism S fixes all 4 corners of F, therefore by Observation 3, it fixes both diagonals $d_1, d_2 \subset F$. The types of d_1 and d_2 are $type(d_1) = (+, +, 1, \ldots, 1)$ and $type(d_2) = (+, -, 1, \ldots, 1)$.

Suppose that S fixes a point $p = [i, 1, \ldots, 1]$, where $i \in \{2, \ldots, n-1\}$ (corners are already fixed). In three steps we show that the point $p_5 = [n-i+1, 1, \ldots, 1]$ is fixed (note that for $i = n - i + 1$ the proof is trivial, thus we suppose $i \neq \gamma$ for odd n). Fixed points in a face 7×7 are depicted in Figure 2.

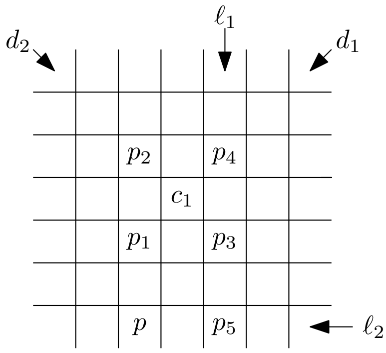

Fig. 2. How to fix points by diagonals in a front 2-dimensional face.

First we show that $p_1 = [i, i, 1, \ldots, 1]$ is fixed by S. A point $S(p_1)$ must be on d_1 and it must be collinear with p. There are 2 points collinear with p on d_1: $[i, i, 1, \ldots 1]$ and $[1, \ldots, 1]$, but the second one is already fixed as a corner. Therefore, the point p_1 is fixed. A point $p_2 = [i, n - i + 1, 1, \ldots, 1] \in d_2$ is fixed by a similar argument.

Next we show that S fixes a point $p_3 = [n - i + 1, i, 1, \ldots, 1]$. A point $S(p_3)$ must be on d_2 and it must be collinear with p_1. If n is even there are two points on d_2 collinear with p_1: p_2 and p_3, but p_2 is fixed due to step 1. If n is odd, there are 3 points collinear with p_1: p_2, p_3 and the face center $c_1 = [\gamma, \gamma, 1, \ldots, 1]$. However, the point c_1 is fixed due to Observation 4 because it is an intersection of the lines d_1 and d_2. Therefore, the point p_3 cannot be mapped onto c_1. A point $p_4 = [n - i + 1, n - i + 1, 1, \ldots, 1]$ is fixed by a similar argument.

Let ℓ_1 be a line such that $type(\ell_1) = (n - i + 1, +, 1, \ldots, 1)$ and ℓ_2 be a line such that $type(\ell_2) = (+, 1, \ldots, 1)$. Both lines ℓ_1 and ℓ_2 are fixed because $p_4, p_3 \in \ell_1$ and ℓ_2 connects two fixed corners. Therefore, the point p_5, which is an intersection of ℓ_1 and ℓ_2, is fixed by Observation 4 as well. $\square$

In the proofs of the following lemmas we use the notions of blocks. Let $p = [x_1, \ldots, x_d]$. We call a set $B_j(p) = \{i \in [d] | x_i = j \vee x_i = n - j + 1\}$ *j-block* of p. Note that j-block and $(n-j+1)$-block are the same set. We say a line ℓ such that $p \in \ell$ is *active* in the j-block $B_j(p)$ if there exists some $i \in B_j(p)$ such that $\mathit{type}(\ell)_i \in \{+,-\}$. For example $p = [1,1,2,4]$ be a point of the cube 4^4 then 1-block of p is the set $\{1,2,4\}$ and a line $\ell \in \mathbb{L}(4^4)$ of a type $\mathit{type}(\ell) = (+,1,2,-)$ is active in $B_1(p)$. We consider only non-empty blocks. We say that the point p from the example has blocks $B_1(p)$ and $B_2(p) = \{3\}$.

Lemma 5. *Let p be a point of n^d and ℓ be a line such that $p \in \ell$. Then, there is exactly one $j \in [n]$ such that ℓ is active in $B_j(p)$.*

Proof. It is clear that there is at least one $j \in [n]$ such that ℓ is active in $B_j(p)$. Suppose ℓ is active in $B_i(p)$ and $B_j(p)$, $i \neq j$. Therefore, p has some coordinates equal to i or $n-i+1$ and some coordinates equal to j or $n-j+1$. Suppose p has some coordinates equal to i and j (other cases are analogous). Without loss of generality $p = [i,j,\dots]$. Since $i \neq j$, $\mathit{type}(\ell) \neq (+,+,\dots)$. Thus, $\mathit{type}(\ell) = (+,-,\dots)$. However, it means that $j = n-i+1$ and $B_i(p) = B_{n-i+1}(p)$. □

Lemma 6. *Let $p = [x_1,\dots,x_d]$ be a point of n^d and it has a block $B_j(p)$ for $j \neq \gamma$. Then, there are $2^k - 1$ active lines in $B_j(p)$ where $k = \left|B_j(p)\right|$.*

Proof. For every $J \subseteq B_j(p), J \neq \emptyset$ we define a line ℓ_J active in $B_j(p)$ in the following way. Let q_J be a linear sequence such that $p \in q_J$ and for $i \in [d]$,

$$\mathit{type}(q_J)_i = \begin{cases} x_i & i \notin J, \\ + & i \in J \text{ and } x_i = j, \\ - & i \in J \text{ and } x_i = n-j+1. \end{cases}$$

For example,

$$p = [\overbrace{n-j+1, j, \dots, j}^{k}, x_{k+1}, \dots, x_d] \text{ and } J = \{1,2\}$$

the linear sequence q_J has the type

$$\mathit{type}(q_J) = (-,+,j\dots,j,x_{k+1},\dots,x_d).$$

Note that for each $J_1, J_2 \subseteq B_j(p), J_1 \neq J_2$ the linear sequences q_{J_1} and q_{J_2} represent different lines.

On the other hand, every line ℓ active in $B_j(p)$ defines a non-empty subset of $B_j(p)$ as coordinates where ℓ has non-constant coordinate sequences. Therefore, the number of lines active in $B_j(p)$ is the number of non-empty subsets of $B_j(p)$, which is $2^k - 1$. □

Lemma 7. *Let $p = [x_1,\dots,x_d]$ be a point of n^d and it has block $B_\gamma(p)$. Then, there are $\frac{3^k-1}{2}$ active lines in $B_\gamma(p)$ where $k = \left|B_\gamma(p)\right|$.*

Proof. The proof is very similar to the previous one. For every $J \subseteq B_\gamma(p), J \neq \emptyset$ we define a line ℓ_J such that $p \in \ell_J$. Let q_J be a linear sequence such that for $i \in \{1, \dots, d\}$

$$type(q_J)_i = \begin{cases} x_i & i \notin J, \\ + & i \in J. \end{cases}$$

And for every $K \subseteq J$ we define a linear sequence q'_{JK} such that $p \in q'_{JK}$, and for $j \in \{1, \dots, d\}$,

$$type(q'_{JK})_j = \begin{cases} type(q_J)_j & j \notin K, \\ - & j \in K. \end{cases}$$

For example,

$$p = [\overbrace{\gamma, \dots, \gamma}^{k}, x_{k+1}, \dots, x_d] \text{ and } J = \{1, 2, 3\}, K = \{3\}$$

the linear sequence q'_{JK} has a type

$$type(q'_{JK}) = (+, +, -, \gamma, \dots, \gamma, x_{k+1}, \dots, x_d).$$

Note that for fixed J, K and $M = J \setminus K$ the linear sequences q'_{JK} and q'_{JM} represent the same lines. Again every line ℓ active in $B_\gamma(p)$ and its two orderings q_1 and q_2 into linear sequence define two pairs of the set $J, K \subseteq B_\gamma(p)$:

1. $J = \big\{i \in B_\gamma(p) | type(q_1)_i \in \{+, -\}\big\} = \big\{i \in B_\gamma(p) | type(q_2)_i \in \{+, -\}\big\}$.
2. $K = \{i \in B_\gamma(p) | type(q_1)_i = +\} = \{i \in B_\gamma(p) | type(q_2)_i = -\}$.
3. $M = \{i \in B_\gamma(p) | type(q_1)_i = -\} = \{i \in B_\gamma(p) | type(q_2)_i = +\}$.

Therefore, the numbers of lines active in $B_\gamma(p)$ is a half of the number of pairs (J, K) such that J is a non-empty subset of $B_\gamma(p)$ and K is a subset of J. We have $\sum_{m=1}^{k} \binom{k}{m}$ choices for the set J. For fixed J of size m, we have 2^m choices for $K \subseteq J$. Therefore the number of these lines is

$$\frac{1}{2} \sum_{m=1}^{k} \left(\binom{k}{m} 2^m \right) = \frac{3^k - 1}{2}.$$

$\square$

Lemma 8. *Let n be odd and $\ell \in \mathbb{L}(n^d)$ such that the cube center c is in ℓ and* $\dim(\ell) = k$. *Let $p \in \ell, p \neq c$. Then, $deg(p) = 2^k - 1 + \frac{3^{d-k}-1}{2}$.*

Proof. Since $p \in \ell$ and $p \neq c$, the point p has exactly 2 blocks $B_j(p)$ and $B_\gamma(p)$. Note that $\big|B_j(p)\big| = k$. Thus, the point p is incident with $2^k - 1$ lines active in $B_j(p)$ and with $\frac{3^{d-k}-1}{2}$ lines active in $B_\gamma(p)$ (by Lemma 6 and Lemma 7). By Lemma 5, the lines active in $B_j(p)$ are disjoint from the lines active in $B_\gamma(p)$ and there are no other lines incident with p. $\square$

Lemma 9. *Every automorphism $S \in \mathbb{T}_n^d$ maps a main diagonal $m \in \mathbb{L}_m(n^d)$ onto a main diagonal $m' \in \mathbb{L}_m(n^d)$.*

Proof. Every point on a main diagonal has only one block. For n even the proof is trivial. For every point $q \in [n]^d$ it holds that any of blocks of q is not the γ-block. Therefore, every point $p \in m$ has degree $2^d - 1$ and any point which is not in any main diagonal has at least two blocks and thus the degree at most 2^{d-1} (by Lemma 6). Every automorphism $S \in \mathbb{T}_n^d$ has to preserve the point degree. Thus, a point $p \in m$ has to be mapped onto a point $p' \in m'$.

Now we prove the lemma for n odd. The center of the cube c is always mapped onto c (c is the only point of degree $\frac{3^d-1}{2}$). Therefore, the main diagonal $m \in \mathbb{L}_m(n^d)$ has to be mapped onto a line $\ell \in \mathbb{L}(n^d)$ such that $c \in \ell$. By Lemma 8, we know the degree of a non-central point $p \in \ell$ is $\deg(p) = 2^k - 1 + \frac{3^{d-k}-1}{2}$.

The degree of a non-central point $q \neq c$ on a main diagonal $m \in \mathbb{L}_m(n^d)$ is $\deg(q) = 2^d - 1$. We show that if $k \neq d$ then $2^k - 1 + \frac{3^{d-k}-1}{2} \neq 2^d - 1$. For contradiction let us suppose that $2^d - 2^k = \frac{3^{d-k}-1}{2}$ and $k < d$. We rewrite the formula into binary numbers:

$$\begin{array}{cr} 2^d & 1\overbrace{0\ldots\ldots\ldots0}^{d} \\ -2^k & -1\overbrace{0\ldots0}^{k} \\ \hline \frac{3^{d-k}-1}{2} & \overbrace{1\ldots1\underbrace{0\ldots0}_{k}}^{d} = \beta > 0. \end{array}$$

It is easy to prove by induction that 4 divides $3^{d-k} - 1$ if and only if $d - k$ is even. The number β must be even so $d - k$ must be even as well. We use the well-known divisibility-by-3 test in the binary system for $\delta = 2\beta + 1$ (it should be equal to $3^{d-k} > 1$). The binary number is divisible by 3 if and only if the number E of even order digits and the number O of odd order digits are equal modulo 3. Note that

$$\delta = \overbrace{1\ldots1}^{d-k}\overbrace{0\ldots0}^{k}1.$$

The number $d - k$ is even, thus the numbers of digits of the orders 1 to d are equal, but $|E - O| = 1$ (because of the 1 at the order 0). Therefore δ is not divisible by 3, which is the contradiction. □

Lemma 10. *Let $S \in \mathbb{T}_n^d$, e be an edge and p be a corner, such that $p \in e$. If the corner p is fixed by S, then $S(e) = e'$ is an edge such that $p \in e'$.*

Proof. Without loss of generality the corner p is $[1, \ldots, 1]$ and the type of e is *type*$(e) = (+, 1, \ldots, 1)$. First we prove the lemma for odd n. Let $k = \dim\big(S(e)\big)$ and suppose that $1 < k < d$ (the line $S(e)$ can not have a dimension d as main diagonals are mapped on to main diagonals by Lemma 9). Without loss of generality

$$type\big(S(e)\big) = (\overbrace{+,\ldots,+}^{k}, 1, \ldots, 1).$$

Let c_1 be the center of e, i.e., the point $[\gamma, 1, \ldots, 1]$. Note that c_1 is collinear with the cube center c. Thus, the point $S(c_1)$ has to be also collinear with the cube center and

$$S(c_1) = [\overbrace{\gamma,\ldots,\gamma}^{k}, 1, \ldots, 1].$$

Consider the set of lines

$$L = \big\{\ell \in \mathbb{L}(n^d) \mid \forall i \leq k : type(\ell)_i \in \{+, -\}, \forall i > k : type(\ell)_i = 1\big\}.$$

Note that the set L contains all lines incident to the vertex $S(c_1)$ which are active in the block $B_\gamma\big(S(c_1)\big)$. Moreover, each line in L intersect exactly 2 main diagonals and the intersections points are corners (in particular not the cube center c). The line $S(e)$ is in L. Since $k > 1$, there is a line $\ell' \in L$ different from $S(e)$. Let ℓ be a preimage of ℓ', i.e., $\ell = S(\ell')$. The line ℓ has to intersect exactly 2 main diagonals as main diagonals are mapped onto main diagonals by Lemma 9. Moreover, the line ℓ can not intersect the main diagonals in the cube center c. Note that $\ell \neq e$. There is only one line ℓ_1 incident to c_1, different from e, such that it intersects some main diagonal. The type of ℓ_1 is

$$type(\ell_1) = (\gamma, +, \ldots, +).$$

However, the line ℓ_1 intersects the main diagonals in the cube center c. Thus, the line ℓ' does not have a preimage, which is a contradiction and $k = \dim\big(S(e)\big) = 1$.

We now complete the proof for even n. For a contradiction suppose that $\dim(e') \geq 2$. Without loss of generality the type of e' is $(+, \ldots, +, 1, \ldots, 1)$. Let $p_2 = [2, 1, \ldots, 1]$ and $p_3 = [3, 1, \ldots, 1]$. Since $n \geq 4$, the points p_2 and p_3 are not corners. Therefore, the point p_i (for $i \in \{2, 3\}$) has blocks $B_i(p_i) = \{1\}$ and $B_1(p_i) = \{2, \ldots, d\}$. Let L_2 be a set of lines incident with p_2 without the edge e and similarly L_3 be a set of lines incident with p_3 without e. Note that lines in L_i (for $i \in \{2, 3\}$) can be active only in the block $B_1(p_i)$. Let $\ell_2 \in L_2$ and $\ell_3 \in L_3$. For ℓ_2 holds that $type(\ell_2)_1 = 2$ and for ℓ_3 holds that $type(\ell_3)_1 = 3$. Therefore, the lines ℓ_2 and ℓ_3 cannot intersect.

Now take images of p_2 and p_3. Let $q_2 = S(p_2) = [i, \ldots, i, 1, \ldots, 1]$ and $q_3 = S(p_3) = [j, \ldots, j, 1, \ldots, 1]$. Since $\dim(e') \geq 2$, the point q_2 is incident with a line k_2 such that $type(k_2) = (+, i, \ldots, i, 1, \ldots, 1)$. Similarly, the point q_3 is incident with a line k_3 such that $type(k_3) = (j, +, \ldots, +, 1, \ldots, 1)$. The lines k_1 and k_2 have to be images of some lines in L_1 and L_2, respectively. However, the lines k_1 and k_2 intersect in a point $[j, i, \ldots, i, 1, \ldots, 1]$, which is a contradiction. □

Lemma 11. *If an automorphism $S \in \mathbb{T}_n^d$ fixes the corner $[1, \ldots, 1]$ and all its neighbors, then S fixes all corners of the cube n^d.*

Proof. We prove the automorphism S fixes all corners $p = [x_1, \ldots, x_d]$ by induction over

$$k(p) = \big|\{i \in [d] : x_i = n\}\big|.$$

By the assumption, the automorphism S fixes corners p such that $k(p) \in \{0, 1\}$. Without loss of generality, a corner q such that $k(q) > 1$ has coordinates

$$q = [\overbrace{n, \ldots, n}^{k(q)}, 1, \ldots, 1].$$

We take neighbors q_1, q_2 of the corner q as

$$\begin{aligned} q_1 &= [\overbrace{n, \ldots, n}^{k(q)-1}, 1, \ldots, 1] \\ q_2 &= [1, \underbrace{n, \ldots, n}_{k(q)-1}, 1, \ldots, 1]. \end{aligned}$$

The corners q_1 and q_2 have two common neighbors: q and

$$q_3 = [1, \overbrace{n, \ldots, n}^{k(q)-2}, 1, \ldots, 1].$$

Corners q_1, q_2 and q_3 are fixed by the induction hypothesis. Therefore, corner q is also fixed as it must be the neighbor of q_1 and q_2. □

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

In this section we characterize the generators of the group $\mathbb{T}_n^d$. As we stated in Section 1, we use the groups $\mathbb{G}_n^d$, $\mathbb{F}_n$.

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

We prove that $\mathbb{A}_n^d = \mathbb{T}_n^d$. The idea of the proof, that resembles a similar proof of Silver [12], is composed of two steps:

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

Hence, for every $S \in \mathbb{T}_n^d$ we find an inverse element A such that A is composed only by elements of $\mathbb{A}_n^d$, therefore $S \in \mathbb{A}_n^d$. We divide the construction of the automorphism A into two steps. In the proof of Theorem 5 we construct an automorphism $A' \in \mathbb{A}_n^d$ such that $S \circ A'$ fixes all corners of the cube. In the proof of Theorem 6 we construct an automorphism $A'' \in \mathbb{A}_n^d$ such that $S \circ A' \circ A''$ fixes all corners and one edge of the cube.

In the next proofs we use the following permutations. For $i, j \in [n]$ and $i, j \neq \gamma$ (in a case of odd n), let $\rho = \rho(i, j)$ be a permutation in $\mathbb{S}_n$ such that

1. $\rho(i) = j, \rho(j) = i$.
2. $\rho(n-i+1) = n-j+1, \rho(n-j+1) = n-i+1$.
3. $\rho(k) = k$ for all other $k \notin \{i, j, n-i+1, n-j+1\}$.

Note that the permutation $\rho(i,j)$ has exactly two cycles of the length two (or one cycle if $i = n-j+1$) and it has the symmetry property, i.e. $F_{\rho(i,j)} \in \mathbb{F}_n$.

Theorem 5. *For all $S \in \mathbb{T}_n^d$ there exists $A' \in \mathbb{A}_n^d$ such that $S \circ A'$ fixes every corner of the cube n^d.*

Proof. We start with the point $p_0 = [1, \ldots, 1]$. By Lemma 9, the point $S(p_0) = [x_1, \ldots, x_d]$ has to be on a main diagonal, i.e., there is some $j \in [n]$ such that each x_i is equal j or $n-j+1$. The point p_0 cannot be mapped onto the cube center, thus $j \neq \gamma$. We choose $F = F_{\rho(j,1)} \in \mathbb{F}_n$. Thus, $S \circ F(p_0)$ is a corner. Then, we choose a translation $T_a \in \mathbb{G}_n^d$ where $a_i = 1$ if and only if $\big[S \circ F(p_0)\big]_i = n$. Therefore, $S \circ F \circ T_a(p_0) = p_0$.

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

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

for all $i \in \{1, \ldots, d\}$. For $i = 0$, the point p_0 is fixed by $Z_0 = S \circ F \circ T_a$. For $i > 0$, by induction hypothesis we have an automorphism Z_{i-1} such that it fixes all points in the set $P_{i-1} = \big\{p_k | 0 \leq k \leq i-1\big\}$. The corner p_i is mapped onto p_j for $j \geq i$ because edges incident with p_0 are mapped onto edges incident with p_0 (by Lemma 10) and points in P_{i-1} are already fixed. If $Z_{i-1}(p_i) = p_i$, we choose $Z_i = Z_{i-1}$. Otherwise, we choose a rotation R_π where π switches i and j coordinates, thus

$$R_\pi\big([x_1, \ldots, x_i, \ldots, x_j, \ldots, x_d]\big) = [x_1, \ldots, x_j, \ldots, x_i, \ldots, x_d]:$$
$$R_\pi(p_j) = R_\pi\big([1, \ldots, \underset{i}{1}, \ldots, \underset{j}{n}, \ldots, 1]\big) = [1, \ldots, \underset{i}{n}, \ldots, \underset{j}{1}, \ldots, 1]$$

We set $Z_i = Z_{i-1} \circ R_\pi$. Hence, the automorphism Z_i fixes p_i and all points of P_i because the rotation R_π does not affect the first $i-1$ coordinates. Note that it also fixes p_0. In this way we can fix all corners p_i for $i \in \{0, \ldots, d-1\}$. 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 $p_0 = [1, \ldots, 1]$ and all its neighbors. Therefore by Lemma 11, the automorphism $Z_{d-1} = S \circ A'$ for some $A' \in \mathbb{A}_d^n$ fixes all corners of the cube. $\square$

Theorem 6. *For all $S \in \mathbb{T}_n^d$ there exists $A \in \mathbb{A}_n^d$ such that $S \circ A$ fixes every corner of the cube n^d and every point of a line $\ell = \big\{[i, 1, \ldots, 1] | i \in [n]\big\}$.*

Proof. By Theorem 5 we have an automorphism $A' \in \mathbb{A}_n^d$ such that $S' = S \circ A'$ fixes all corners of the cube. We find an automorphism $A'' \in A_n^d$ such that $S' \circ A''$ fixes all corners and all points on the line ℓ. The line ℓ is fixed by S' due to Observation 3. Let $k = \lfloor \frac{n}{2} \rfloor$. We construct the automorphism A'' by induction over $i \in \{1, \ldots, k\}$. We show that in a step i an automorphism Y_i fixes all corners and every point in the set

$$Q_i = \big\{[j, 1, \ldots, 1], [n - j + 1, 1, \ldots, 1] | 1 \leq j \leq i\big\}.$$

First, let $i = 1$ and $Y_1 = S'$. The automorphism Y_1 fixes all corners and Q_1 contains only $[1, \ldots, 1]$ and $[n, 1, \ldots, 1]$, which are also corners. Suppose that $i > 1$. By induction hypothesis, we have an automorphism Y_{i-1} which fixes all corners and every point in the set Q_{i-1}. If $Y_{i-1}\big([i, 1, \ldots, 1]\big) = [i, 1, \ldots, 1]$ then $Y_i = Y_{i-1}$. Otherwise, $Y_{i-1}\big([i, 1, \ldots, 1]\big) = [j, 1, \ldots, 1]$. Note that $i < j \leq n-i+1$ because points in Q_{i-1} are already fixed. Also in the case of odd n, it holds that $j \neq \gamma$ as $i \neq \gamma$ and $[i, 1, \ldots, 1]$ is not collinear with the cube center, thus the point $Y_{i-1}\big([i, 1, \ldots, 1]\big)$ is not collinear with the cube center as well. Let us consider $F_\rho \in \mathbb{F}_n$ for $\rho = \rho(i, j)$. The automorphism $Y_i = Y_{i-1} \circ F_\rho$ fixes the following points:

1. All corners, as the automorphism Y_{i-1} fixes all corners by the induction hypothesis and $\rho(1) = 1$ and $\rho(n) = n$.
2. Set Q_{i-1}, as the automorphism Y_{i-1} fixes the set Q_{i-1} by the induction hypothesis and $\rho(s) = s$ for all $s < i$ and $s > n - i + 1$.
3. Point $[i, 1, \ldots, 1]$: $Y_{i-1} \circ F_\rho\big([i, 1, \ldots, 1]\big) = F_\rho\big([j, 1, \ldots, 1]\big) = [i, 1, \ldots, 1]$.
4. Point $[n - i + 1, 1, \ldots, 1]$ by Lemma 4.

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

It remains to prove that if an automorphism $S \in \mathbb{T}_n^d$ fixes all corners and all points in the line $\ell = \big\{[i, 1, \ldots, 1] | i \in [n]\big\}$ then S is the identity. We prove it in two parts. First, we prove that if $d = 2$ then the automorphism S is the identity. Then, we prove it for a general dimension by an induction argument.

Theorem 7. *Let an automorphism $S \in \mathbb{T}_n^2$ fixes all corners of the cube n^2 and all points in the line $\ell = \big\{[i, 1] | i \in [n]\big\}$. Then, the automorphism S is the identity.*

Proof. Let $d_1, d_2 \in \mathbb{L}_m(n^2)$. 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 cube center $c_1 = [\gamma, \gamma]$ 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*$(\ell_2) = (\gamma, +)$ and *type*$(\ell_3) = (+, \gamma)$. The line ℓ_2 also intersects the line

ℓ. Therefore, the line ℓ_2 contains two fixed points c_1 and $[\gamma, 1]$ and thus it 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 3 with an example of the cube 5^2.

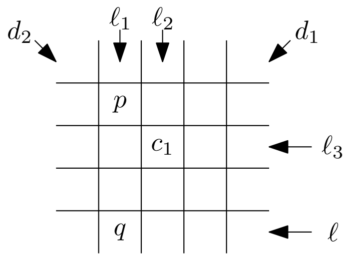

Fig. 3. Points and lines used in the proof of Theorem 7.

Every point in n^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 $S \in \mathbb{T}_n^d$ fix all corners of the cube n^d and all points of an arbitrary edge e. Then, the automorphism S 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, $e = \big\{[i, 1, \ldots, 1] \big| i \in [n]\big\}$. For $s \in \{1, n\}$ and $i \in [d]$, let F_i^s be a $(d-1)$-dimensional face which fix the i-th coordinate to s, i.e.,

$$F_i^s = \big\{[x_1, \ldots, x_d] | x_i = s, x_j \in [n] \text{ for } j \neq i\big\}.$$

Note that the faces $F_2^1, \ldots, F_d^1$ cotanins the line e. Therefore, all points of the faces $F_2^1, \ldots, F_d^1$ are fixed by the induction hypothesis as all corners are fixed as well. Let e_1 be an edge of type $(1, 1, +, 1, \ldots, 1)$ (since $d > 2$, the edge e_1 is well-defined). It holds that $e_1 \subseteq F_1^1 \cap F_2^1$. Thus, all corners of the face F_1^1 are fixed and all points of one edge of F_1^1 are fixed. Therefore, all points of face F_1^1 are fixed by the induction hypothesis.

We will prove that all points of faces F_i^n are fixed by similar argument. Let f_i be an edge of type

$$type(f_i) = \begin{cases} (1, \ldots, 1, +, \underset{i}{n}, 1, \ldots, 1) & \text{if } i > 1 \\ (n, 1, \ldots, 1, +) & \text{if } i = 1. \end{cases}$$

Consider the face F_i^n and set $j = i + 1 \mod d$. The line f_i is contained in the faces F_i^n and F_j^1. Thus by the same argument as above, all points of the faces $F_1^n, \ldots, F_d^n$ are fixed.

We showed 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. $\square$

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

Proof. The groups $\mathbb{G}^d_n$ are all isomorphic to the group of d-dimensional hypercube automorphism for all n. 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 $\mathbb{F}_{2k+1}$. $\square$

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

In the previous section we characterized the generators of the group $\mathbb{T}^d_n$. Now we compute the order of $\mathbb{T}^d_n$. First, we state several technical lemmas.

Lemma 12. *Orders of the basic groups are as follows.*

1. $|\mathbb{G}^d_n| = 2^d d!$.
2. $|\mathbb{F}_n| = 2^k k!$ *for* $k = \lfloor \frac{n}{2} \rfloor$.

Proof. Size of the hypercube automorphism group $\mathbb{Q}_d$ is well known [8].

Size of the group $\mathbb{F}_n$ is the number of permutations $\pi \in \mathbb{S}_n$ with the symmetry property. If n is even, we have n possibilities how to choose the image of the first element, we have $n-2$ possibilities for the second element, and so on, thus there are

$$\prod_{i=0}^{\frac{n}{2}-1} (n-2i)$$

such permutations. If n is odd, the element $\frac{n+1}{2}$ has to be mapped onto itself. Therefore, the order of $\mathbb{F}_n$ where n is odd is the same as the order of $\mathbb{F}_{n-1}$. The general formula is

$$\prod_{i=0}^{k-1} (2k-2i) = 2^k \prod_{i=0}^{k-1} (k-i) = 2^k k!$$

for $k = \lfloor \frac{n}{2} \rfloor$. $\square$

Lemma 13. *The groups $\mathbb{G}^d_n$ and $\mathbb{F}_n$ commute.*

Proof. Let $T_a \circ R_\pi \in \mathbb{G}^d_n$ and $F_\rho \in \mathbb{F}_n$. Note that for ρ holds that $\rho\big(\mathit{flip}(i,b)\big) = \mathit{flip}\big(\rho(i), b\big)$ due to the symmetry property. Then,

$$\begin{aligned}
&T_a \circ R_\pi \circ F_\rho\big([x_1, \ldots, x_d]\big) \\
&\quad = F_\rho\Big(\big[\mathit{flip}(x_{\pi(1)}, a_{\pi(1)}), \ldots, \mathit{flip}(x_{\pi(d)}, a_{\pi(d)})\big]\Big) \\
&\quad = \Big[\rho\big(\mathit{flip}(x_{\pi(1)}, a_{\pi(1)})\big), \ldots, \rho\big(\mathit{flip}(x_{\pi(d)}, a_{\pi(d)})\big)\Big] \\
&\quad = \Big[\mathit{flip}\big(\rho(x_{\pi(1)}), a_{\pi(1)}\big), \ldots, \mathit{flip}\big(\rho(x_{\pi(d)}), a_{\pi(d)}\big)\Big].
\end{aligned}$$

Similarly,

$$F_\rho \circ T_a \circ R_\pi\big([x_1,\dots,x_d]\big) = T_a \circ R_\pi\Big(\big[\rho(x_1),\dots,\rho(x_d)\big]\Big)$$
$$= \Big[\mathit{flip}\big(\rho(x_{\pi(1)}), a_{\pi(1)}\big),\dots,\mathit{flip}\big(\rho(x_{\pi(d)}), a_{\pi(d)}\big)\Big].$$

□

By Lemma 13 we can conclude that any automorphism $A \in \mathbb{T}_n^d$ can be written as $A = G \circ F$ where $G \in \mathbb{G}_n^d$ and $F \in \mathbb{F}_n$. Thus, the product

$$\mathbb{G}_n^d \mathbb{F}_n = \big\{G \circ F | G \in \mathbb{G}_n^d, F \in \mathbb{F}_n\big\}$$

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

Lemma 14 (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 order of the intersection of the basic groups $\mathbb{G}_n^d$ and $\mathbb{F}_n$.

Lemma 15. *The intersection $\mathbb{G}_n^d \cap \mathbb{F}_n = \{Id, F_\sigma\}$ where $\sigma(i) = n - i + 1$.*

Proof. It is clear that $\{Id, F_\sigma\} \subseteq \mathbb{G}_n^d \cap \mathbb{F}_n$ because $F_\sigma = T_a$ where $a = (1,\dots,1)$.

Consider a main diagonal $\ell = \big\{[i,\dots,i] | i \in [n]\big\}$ and its ordering into a linear sequence $(p^1,\dots,p^n)$, where $p^i = [i,\dots,i]$. Every automorphism $G \in \mathbb{G}_n^d$ preserves an order of points on the line ℓ, i.e., a sequence $\big(G(p^1),\dots,G(p^n)\big)$ is an ordering of $G(\ell)$ into a linear sequence.

Consider an automorphism $F_\rho \in \mathbb{F}_n$. We claim that $\big(F_\rho(p^1),\dots,F_\rho(p^n)\big)$ is an ordering of $F_\rho(\ell)$ into a linear sequence if and only if ρ is the identity or σ. Recall that $F_\rho(p^i) = \big[\rho(p_1^i),\dots,\rho(p_d^i)\big]$. Thus, to $\big(F_\rho(p^1),\dots,F_\rho(p^n)\big)$ be a linear sequence it must hold that $\rho(i) = i$ or $\rho(i) = n - i + 1$ for all i. We conclude that if ρ is not the identity and $\rho \neq \sigma$ then $F_\rho \notin \mathbb{G}_n^d$. □

As a corollary of Lemmas 12, 14 and 15 we get the second part of Theorem 1.

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. Let s_1 and s_2 be colorings of a combinatorial cube n^d. We say the colorings s_1 and s_2 are *isomorphic* if there is an automorphism $A \in \mathbb{T}_n^d$ which preserves the colors, i.e., for every point p of a combinatorial cube n^d holds that $s_1(p) = s_2\big(A(p)\big)$.

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 $V = [n]$. We construct the coloring $s^G : [k]^2 \to \{0, 1\}$ for $k = 2n + 4$ as follows. The value of $s^G\big([i, j]\big)$ is 1 if $[i, j] = [n + 1, n + 1]$ or $[i, j] = [n + 1, n + 2]$ or $i, j \le n$ and $\{i, j\} \in E$. The value of $s^G(p)$ for any other point p is 0. We can view the coloring s^G as a matrix M^G such that $M^G_{i,j} = s^G\big([i, j]\big)$. The submatrix of M^G consisting of the first n rows and n columns is exactly the adjacency matrix of the graph G. For example, let P be a path on 3 vertices, then

$$M^P = \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The idea of the reduction is as follows. If two colorings s^{G_1}, s^{G_2} are isomorphic via a cube automorphism $A \in \mathbb{T}^2_k$ then A can be composed only of automorphisms in $\mathbb{F}_k$ (due to the colors of $[n + 1, n + 1]$ and $[n + 1, n + 2]$). Hence, the automorphism $A = F_\rho$ for some permutation $\rho \in \mathbb{S}_k$. Moreover, the permutation ρ maps the numbers in $[n]$ to the numbers in $[n]$ and describes the isomorphism between the graphs G_1 and G_2.

Lemma 16. *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 $A \in \mathbb{T}^2_k$ then $A = F_\rho \in \mathbb{F}_k$. Moreover, $\rho(i) \le n$ if and only if $i \le n$.*

Proof. Let $A = S \circ F$ where $S \in \mathbb{G}^2_k, F \in \mathbb{F}_k$ and m_1, m_2 be main diagonals of $[k]^2$ of a type $(+, +)$ and $(+, -)$, respectively. Due to the colors of $p_1 = [n+1, n+1]$ and $p_2 = [n + 1, n + 2]$ we will show that A has to fix m_1 and m_2 and that $A \in \mathbb{F}_k$.

Since G_1 and G_2 are simple graphs without loops, there is exactly one point of the color 1 on the main diagonal m_1 (the point p_1) and there are no points of the color 1 on the main diagonal m_2 in both colorings s^{G_1} and s^{G_2}. Therefore, A has to fix m_1 and m_2 and the point p_1. Let ℓ_1 be a line of a type $(n + 1, +)$ and ℓ_2 be a line of a type $(+, n + 1)$. Note that in both coloring the line ℓ_1 contains two points of the color 1 (p_1 and p_2) and ℓ_2 contains only one point of the color 1 (the point p_1). The line ℓ_1 can be mapped only on the lines ℓ_1 or ℓ_2. However, due to the colors of the points p_1 and p_2 in both coloring the line ℓ_1 has to be fixed. Thus, the point p_2 is fixed as well.

Every automorphism in $\mathbb{F}_k$ fixes the lines m_1 and m_2. Thus, the automorphism S has to fix the main diagonals as well. Let $S = T_a \circ R_\pi$. There are 8 automorphisms in $\mathbb{G}_k^2$. By simple case analysis we know that S fixes the lines m_1 and m_2 if and only if $a = (0,0)$ or $a = (1,1)$. If π is the identity, then $S = T_a$ and it is also in $\mathbb{F}_k$ (see Lemma 15).

Let us suppose that $\pi \neq Id$ and $a = (0,0)$. Note that $A(p_1) = \big[\rho(n+1), \rho(n+1)\big]$. The automorphism A fixes the point p_1, thus $\rho(n+1) = n+1$. Therefore, $A(p_2) = \big[\rho(n+2), \rho(n+1)\big] = \big[\rho(n+2), n+1\big] \neq p_2$, which is a contradiction as we proved that A fixes the point p_2. The proof for $a = (1,1)$ is identical. Thus, we conclude that $A \in \mathbb{F}_k$.

Now we prove the last part of the lemma. We already know that $\rho(n+1) = n+1$ and $\rho(n+2) = n+2$. For every $i \leq n$ 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 $i \geq n+3$ there are only points with color 0 on a line of type $(+, i)$ in both colorings. Therefore, if $i \leq n$ then i has to be mapped on $j \leq n$ by ρ. □

The proof of the following theorem follows from Lemma 16.

Theorem 9. *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.*

Proof. First, suppose that s^{G_1} and s^{G_2} are isomorphic. Let $V_1 = V_2 = [n]$. By Lemma 16, we know that s^{G_1} and s^{G_2} are isomorphic via a cube automorphism $F_\rho \in \mathbb{F}_k$. We define the function $f : V_1 \to V_2$ as $f(i) = \rho(i)$. By Lemma 16, f is a well defined bijection. It remains to prove that f is a graph isomorphism:

$$\{i,j\} \in E_1 \Leftrightarrow s^{G_1}\big([i,j]\big) = 1 \Leftrightarrow s^{G_2}\big([\rho(i), \rho(j)]\big) = 1 \Leftrightarrow \big\{f(i), f(j)\big\} \in E_2.$$

Now we prove the other implication. Let $f : V(G_1) \to V(G_2)$ be an isomorphism of G_1 and G_2. We construct the permutation $\rho : [k] \to [k]$ as follows:

$$\rho(i) = \begin{cases} i & n+1 \leq i \leq n+2 \\ f(i) & i \leq n \end{cases}$$

We define values of $\rho(i)$ for $i \geq n+3$ in such a way the symmetry property holds for the permutation ρ.

We prove that $F_\rho \in \mathbb{F}_k$ is an isomorphism between s^{G_1} and s^{G_2}. Let us suppose that $s^{G_1}\big([i,j]\big) = 1$. If $[i,j] = [n+1, n+1]$ or $[i,j] = [n+1, n+2]$ then $s^{G_2}\big(F_\rho([i,j])\big) = 1$ as well. Otherwise, $i, j \leq n$ because there is no other point colored by 1. Thus,

$$s^{G_1}\big([i,j]\big) = 1 \Leftrightarrow \{i,j\} \in E_1 \Leftrightarrow \big\{f(i), f(j)\big\} \in E_2 \Leftrightarrow s^{G_2}\big([\rho(i), \rho(j)]\big) = 1.$$

Hence, we proved that $s^{G_1}\big([i,j]\big) = 1$ if and only if $s^{G_2}\big(F_\rho[i,j]\big) = 1$. □

We may suppose that the input 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 9.

7 Open Problems

We characterized the automorphism group of the cube n^d for finite n and d. It would be interesting to characterize the automorphisms of the cube with an infinite dimension. Would the automorphisms be the same even for uncountable dimension? The lines of the cube n^d cannot be (straightforwardly) generalized to infinite n, because of the decreasing coordinate sequences.

We also proved that the Colored Cube Isomorphism problem is basically as hard as the Graph Isomorphism problem. However, for strategy searching algorithms the most important task is to prune the game tree at upper levels, i.e., after constantly many turns. Thus, a natural question arises: Is there a polynomial time algorithm for the Colored Cube Isomorphism problem if all color classes except one have constant size?

Acknowledgment

We would like to thank the anonymous referees for many tips for improving the presentation and for pointing out the weak spots in the proofs.

References

1. L. V. Allis. *Searching for Solutions in Games and Artificial Intelligence*. PhD thesis, University of Limburg, 1994.
2. V. Arvind, Bireswar Das, Johannes Köbler, and Seinosuke Toda. Colored hypergraph isomorphism is fixed parameter tractable. *Algorithmica*, 71(1):120–138, January 2015.
3. V. Arvind and Johannes Köbler. On hypergraph and graph isomorphism with bounded color classes. In Bruno Durand and Wolfgang Thomas, editors, *STACS 2006*, pages 384–395, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
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(11):1621–1627, 2008.
8. C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer-Verlag, 2004.
9. A.W. Hales and R. Jewett. On regularity and positional games. *Transactions of the American Mathematical Society*, 106:222–229, 1963.
10. F. Harary. The automorphism group of a hypercube. *Journal of Universal Computer Science*, 6(1):136–138, 2000.
11. O. Patashnik. Qubic: $4 \times 4 \times 4$ tic-tac-toe. *Mathematics Magazine*, 53:202–216, 1980.
12. R. Silver. The group of automorphisms of the game of 3-dimensional ticktacktoe. *The American Mathematical Monthly*, 74(3):247–254, 1967.