Any Finite Group is the Group of Some Binary, Convex Polytope

Jean-Paul Doignon
Any Finite Group is the Group of Some Binary, Convex Polytope

Jean-Paul Doignon

Abstract For any given finite group, Schulte and Williams (Discrete Comput Geom 54(2):444–458, 2015) establish the existence of a convex polytope whose combinatorial automorphisms form a group isomorphic to the given group. We provide here a shorter proof for a stronger result: the convex polytope we build for the given finite group is binary, and even combinatorial in the sense of Naddef and Pulleyblank (J Combin Theory Ser B 31(3):297–312, 1981); the diameter of its skeleton is at most 2; any combinatorial automorphism of the polytope is induced by some isometry of the space; any automorphism of the skeleton is a combinatorial automorphism.

Keywords Automorphism · Group · Graph · Convex polytope

Mathematics Subject Classification 05E18 · 52B15

1 Introduction

A combinatorial automorphism of a convex polytope is a permutation of its set of vertices that maps the set of vertices of any face to the set of vertices of some face. Recently, Schulte and Williams [14] established that any finite group is isomorphic to the group of combinatorial automorphisms of some convex polytope. Their proof is rather long and involved. We propose here a shorter one which even establishes a stronger result because the convex polytope we build for a given group is always
binary: all its vertices have coordinates equal to 0 or 1. The polytope is moreover combinatorial in the sense of Naddef and Pulleyblank [12]: it is a binary polytope on which every two nonadjacent vertices have their midpoint equal to the midpoint of two other vertices (such combinatorial polytopes appear also, for instance, in [10]).

Throughout the paper, we consider $\mathbb{R}^d$ as a euclidean vector space with the usual dot product. The isometries of $\mathbb{R}^d$ are the permutations of $\mathbb{R}^d$ that preserve distance. For a subset $P$ of $\mathbb{R}^d$, the isometries of $P$ are the isometries of $\mathbb{R}^d$ that stabilize $P$.

**Theorem 1.1** For each finite group $G$ there exist a natural number $d$ and a convex polytope $P_G$ in $\mathbb{R}^d$ satisfying Properties (i)–(v):

(i) the group of combinatorial automorphisms of the convex polytope $P_G$ is isomorphic to $G$;
(ii) any combinatorial automorphism of $P_G$ is the restriction to the set of vertices of some isometry of $P_G$;
(iii) the convex polytope $P_G$ is binary, and even combinatorial;
(iv) the diameter of the skeleton (graph) of $P_G$ is at most 2;
(v) any automorphism of the skeleton of $P_G$ is a combinatorial automorphism of $P_G$.

We denote by $G$ a given, finite group. The required polytope $P_G$ for $G$ arises from a two-step construction. In Sect. 2 we recall results on the existence of a graph $\Gamma(G)$ whose automorphism group is isomorphic to $G$. In Sect. 3 we build for almost any graph $\Gamma$ a polytope $P(\Gamma)$ whose combinatorial automorphism group is isomorphic to the automorphism group of the graph $\Gamma$. It happens that $P(\Gamma)$ is a combinatorial polytope; moreover, any combinatorial automorphism of the polytope $P(\Gamma)$ is the restriction of some isometry of $P(\Gamma)$ (Proposition 3.5). The proof also shows that all isometries of $P(\Gamma)$ are in fact coordinate permutations of the space $\mathbb{R}^d$ in which we build $P(\Gamma)$. Incidentally, we notice that any graph on $d$ nodes is an induced subgraph of the graph of some binary, combinatorial, convex polytope of dimension $d$.

For any given group $G$, the two-step construction produces a convex polytope $P_G = P(\Gamma(G))$ which satisfies Properties (i)–(iv) in Theorem 1.1 (as we will see in Sect. 4, we might need to replace $\Gamma(G)$ with its complement graph; also we handle the two smallest groups $G$ in another way). In Sect. 4, after completing the proof, we discuss how to decrease the dimension and/or the number of vertices of such a polytope $P_G$. Next, we indicate how to construct the polytope $P_G$ in order that it moreover satisfies Property (v). We also mention a curious, immediate consequence: for any finite group $G$, there is a directed graph for which the asymmetric travelling-salesman polytope has its automorphism group isomorphic to $G$.

Let us mention in passing that Babai [3] characterizes the isometry groups of convex polytopes (binary or not) which are transitive on the set of vertices. The only excluded groups are the generalized dicyclic groups and the abelian groups of exponent at least 2 (see [3,5], for a definition of generalized dicyclic groups and, for instance, [13] for further group terminology).
2 Building a Graph for Any Group

Our graphs $\Gamma = (V, E)$ have neither loops nor multiple links. We use the terms ‘node’ and ‘link’ for an element of respectively $V$ and $E$ (while keeping ‘vertex’ and ‘edge’ for polytopes). Let again $G$ be a finite group. Frucht [7] was the first to show the existence of some graph whose automorphism group is isomorphic to $G$ (for a historical perspective, see Hevia [9]). For reasons which will become clear in Sect. 4, we would like to select, given the group $G$, a graph having $G$ as its automorphism group and moreover having the least possible number of nodes.

Babai [2] proves that, with the exception of the three cyclic groups $C_3$, $C_4$ and $C_5$ (of orders 3, 4 and 5), there exists, for any finite group $G$, a graph having at most $2|G|$ nodes with automorphism group $G$. For many finite groups $G$, there is a graph on $|G|$ nodes or less with the stronger property that its automorphism group is isomorphic to $G$ and acts regularly on the set of nodes (we will not make use of the latter property). As found by Godsil [8] and reported by Babai and Godsil [5], such a graph exists for any finite group $G$ except for

– the abelian groups of exponent at least 3;
– the generalized dicyclic groups;
– 13 other groups of orders at most 32.

Now forgetting about regularity, we mention that Arlinghaus [1] provides for each finite, abelian group $G$ the minimum number of nodes in a graph having $G$ as its automorphism group.

3 Building a Binary Polytope for Any Graph

Throughout the section, $\Gamma = (V, E)$ is a graph with at least one node. For two nodes $u, v$ in $V$, we write $u \sim v$ when $u$ and $v$ are linked in $\Gamma$. For a given node $u$ of $\Gamma$, we denote by $N(u)$ the set of neighbours of $u$ (not including $u$), as well as the graph induced by $\Gamma$ on $N(u)$.

We canonically identify $\mathbb{R}^V$ with the euclidean vector space $\mathbb{R}^{|V|}$. The characteristic vector $\chi(S)$ of a subset $S$ of $V$ is the vector in $\mathbb{R}^V$ defined by

$$\chi(S)_v = \begin{cases} 1 & \text{if } v \in S, \\ 0 & \text{if } v \notin S. \end{cases}$$

The polytope $P(\Gamma)$ of the graph $\Gamma = (V, E)$ is the convex hull in $\mathbb{R}^V$ of the characteristic vectors of the empty set, the one-element subsets of $V$ and the links in $E$:

$$P(\Gamma) = \text{conv}\{\chi(\emptyset)\} \cup \{\chi(\{v\}) \mid v \in V\} \cup \{\chi(e) \mid e \in E\}. \quad (1)$$

A series of statements now collect properties of the polytope $P(\Gamma)$, starting with a description of its skeleton.

**Proposition 3.1** The vertices of the polytope $P(\Gamma)$ are all the characteristic vectors appearing in Equation (1). Adjacency among the vertices is as follows:
(i) the vertex \( \chi(\emptyset) \) is adjacent to each vertex \( \chi(\{v\}) \), for \( v \) in \( V \), and to no other vertex;
(ii) the vertices \( \chi(\{u\}) \) and \( \chi(\{v\}) \), for distinct nodes \( u, v \) in \( V \), are adjacent if and only if the nodes \( u \) and \( v \) are not linked in \( \Gamma \) (that is, \( u \sim v \));
(iii) two vertices \( \chi(\{v\}) \) and \( \chi(\{u, w\}) \), for \( v \in V \) and \( \{u, w\} \in E \), are adjacent if and only if either \( v \in \{u, w\} \) or \( (v \notin \{u, w\} \) and neither \( v \sim u \) nor \( v \sim w \);
(iv) for distinct links \( e, f \) in \( E \), the vertices \( \chi(e) \) and \( \chi(f) \) are adjacent if and only if either \( e \) and \( f \) have a common node, or \( e \) and \( f \) are disjoint and not contained in any four-cycle in the graph \( G \).

**Proof** The first assertion follows from the fact that characteristic vectors have all their coordinates equal to 0 or 1. We now consider one by one the cases of adjacency.

(i) \( \chi(\emptyset) \) is adjacent to each \( \chi(\{v\}) \) because adjacency of the same vertices holds on the unit cube. Moreover, \( \chi(\emptyset) \) is not adjacent to any vertex \( \chi(e) \), with \( e \in E \): indeed, the midpoint of \( \chi(\emptyset) \) and \( \chi(e) \) is the same as the midpoint of two other vertices, namely \( \chi(\{u\}) \) and \( \chi(\{v\}) \) if \( e = \{u, v\} \);
(ii) if \( u \sim v \), then the vertices \( \chi(\emptyset) \) and \( \chi(\{u, v\}) \) have the same midpoint as the vertices \( \chi(\{u\}) \) and \( \chi(\{v\}) \). So \( \chi(\{u\}) \) and \( \chi(\{v\}) \) are not adjacent. Second, if \( u \sim v \), then the affine inequality on \( R^V \)
\[
x_{uv} + x_{uv} - 2 \sum_{i \in V \setminus \{u, v\}} x_i \leq 1
\]
defines a face of \( P(\Gamma) \) which is the segment \([\chi(\{u\}), \chi(\{v\})]\) (meaning the inequality is valid for \( P(\Gamma) \) and it is satisfied with equality only at the points of \( P(\Gamma) \) which belong to the segment). Thus the vertices \( \chi(\emptyset) \) and \( \chi(\{u, v\}) \) are adjacent;
(iii) if \( v \in \{u, w\} \), adjacency in \( P(\Gamma) \) results from adjacency in the unit cube. If \( v \notin \{u, w\} \), notice that if \( u \sim v \), then \( \chi(\{v\}) \) and \( \chi(\{u, w\}) \) have the same midpoint as \( \chi(\{w\}) \) and \( \chi(\{u, v\}) \), so \( \chi(\{v\}) \) and \( \chi(\{u, w\}) \) are not adjacent. The argument is similar if \( v \sim w \). Conversely, if \( v \notin \{u, w\} \) and \( u \sim v, v \sim w \), the affine inequality
\[
x_v + \frac{1}{2} x_u + \frac{1}{2} x_w - 2 \sum_{i \in V \setminus \{u, v, w\}} x_i \leq 1
\]
defines a face of \( P(\Gamma) \) which is \([\chi(\{v\}), \chi(\{u, w\})]\);
(iv) this can be proved with arguments similar to those used in (i)–(iii). For another proof, consider the edge polytope \( P_E = \text{conv} \{ \chi(e) \mid e \in E \} \) of the graph \( \Gamma \) (as for instance in Tran and Ziegler [15]). Notice that \( P_E \) is the face of \( P(\Gamma) \) defined by the inequality \( \sum_{i \in V} x_i \leq 2 \). Thus the two vertices \( \chi(e) \) and \( \chi(f) \) of \( P(\Gamma) \) are adjacent if and only if they are adjacent in \( P_E \), and the latter happens exactly if the condition in (iv) is satisfied (see [15]). \( \Box \)

For a vertex \( p \) of the polytope \( P(\Gamma) \), let \( \mathcal{N}(p) \) denote both the neighborhood of \( p \) in the skeleton, and the graph induced by the skeleton on the neighborhood.
Corollary 3.2 There hold for the skeleton of the polytope $P(\Gamma)$:

(i) the diameter is at most 2;

(ii) the vertices forming the neighborhood $\mathcal{N}(\chi(\emptyset))$ of $\chi(\emptyset)$ are all the vertices $\chi(\{u\})$, for $u \in V$; the mapping

$$V \to \mathcal{N}(\chi(\emptyset)) : u \mapsto \chi(\{u\})$$

is an isomorphism from the complement graph $\overline{\Gamma}$ to the induced graph $\mathcal{N}(\chi(\emptyset))$.

**Proof** Both assertions follow at once from Proposition 3.1. \(\Box\)

It follows from Corollary 3.2 (ii) that any graph $\Gamma$ on $d$ nodes is an induced subgraph of the skeleton of some binary, combinatorial, convex polytope of dimension $d$ (take the polytope $P(\overline{\Gamma})$ and consider the graph induced by the skeleton on the neighborhood of $\chi(\emptyset)$).

Corollary 3.3 The convex polytope $P(\Gamma)$

(i) has dimension $|V|$;

(ii) it is binary, and even combinatorial.

**Proof** Because $\chi(\emptyset)$ is the origin and the vectors $\chi(\{u\})$’s, for $u \in V$, form a base of the vector space $\mathbb{R}^V$, Assertion (i) holds. Assertion (ii) was established in the proof of Proposition 3.1, except for two nonadjacent vertices of the form $\chi(e)$ and $\chi(f)$ with $e, f \in E$. By (iv) in Proposition 3.1, the links $e$ and $f$ are disjoint, and moreover form a four-cycle with two other links $e'$ and $f'$; then $\chi(e)$ and $\chi(f)$ have the same midpoint as $\chi(e')$ and $\chi(f')$. \(\Box\)

We now prove that the vertex $\chi(\emptyset)$ is particular among all the vertices of $P(\Gamma)$ exactly when the graph $\Gamma$ satisfies the following mild condition (which we will meet again in later statements):

[*] The graph has at least one link ($E \neq \emptyset$) and there does not exist any bipartition of $V$ into two stable sets $C, D$ with some node $v_0$ in $C$ linked to all nodes in $D$.

**Lemma 3.4** The following assertions are equivalent:

(a) all combinatorial automorphisms of the polytope $P(\Gamma)$ fix the vertex $\chi(\emptyset)$;

(b) the graph $\Gamma$ satisfies Condition [*];

(c) the graph $\mathcal{N}(p)$ induced on the neighbourhood of a vertex $p$ of $P(\Gamma)$ is isomorphic to the complement graph $\overline{\Gamma}$ exactly if $p = \chi(\emptyset)$;

(d) all automorphisms of the skeleton of $P(\Gamma)$ fix the vertex $\chi(\emptyset)$.

**Proof** (a) \(\Rightarrow\) (b). Proceeding by contraposition, we assume that the graph $\Gamma$ does not satisfy [*]. Suppose first that $\Gamma$ has no link. Then the polytope $P(\Gamma)$ is a simplex with at least two vertices, and so (a) is not valid. Next, assume $\Gamma$ has a bipartition $C, D$ and a node $v_0$ as in [*]. Consider the affine permutation $T$ mapping the point $x$ of $\mathbb{R}^V$ to the point $x'$ of $\mathbb{R}^V$ with, for $u \in V$,

$$x'_u = \begin{cases} 1 - \sum_{a \in C} x_a & \text{if } u = v_0, \\ x_u & \text{if } u \neq v_0. \end{cases}$$
It is easily checked that $T$ permutes the vertices of the polytope $P(\Gamma)$, more precisely: $T$ exchanges $\chi(\emptyset)$ and $\chi(\{v_0\})$ and, for any node $b$ in $D$, it exchanges $\chi(\{b\})$ with $\chi(\{v_0, b\})$; also, $T$ fixes all other vertices of $P(\Gamma)$ (even those coming from potential links between $C$ and $D$ that do not contain $v_0$). Thus $T$ induces on the set of vertices a combinatorial automorphism which maps the vertex $\chi(\emptyset)$ on some other vertex, so (a) is not valid.

(b) $\Rightarrow$ (c). By Corollary 3.2 (ii), $\mathcal{N}(\chi(\emptyset))$ is isomorphic to $\overline{\Gamma}$.
Proceeding again by contradiction, assume some vertex $p$ of the polytope $P(\Gamma)$, different from $\chi(\emptyset)$, is such that the graph induced by the skeleton on its neighbourhood is isomorphic to the graph $\overline{\Gamma}$. In particular, the number of neighbors of $p$ must be $|V|$.

If $p = \chi(\{v\})$, for some $v$ in $V$, we know from Proposition 3.1 that $\chi(\{v\})$ is for sure adjacent to $\chi(\emptyset)$, to $\chi(\{u\})$ when $v \sim u$ and to $\chi(\{v, w\})$ when $v \sim w$ (a total number of $|V|$ vertices). Hence $\chi(\{v\})$ cannot be adjacent to any further vertex. In particular, there is no link between any two nodes of $\Gamma$ not linked to $v$. Then the neighborhood of $\chi(\{v\})$ is the union of two cliques, respectively the clique $C$ formed by the vertex $\chi(\emptyset)$ together with the vertices $\chi(\{u\})$ for $v \sim u$, and the clique $D$ formed by the vertices $\chi(\{v, w\})$ for $v \sim w$. Moreover, $\chi(\emptyset)$ is adjacent to no vertex in $D$. Because of the present assumption on $p = \chi(\{v\})$, there exists a bipartition $C$, $D$ of $V$ as in Condition [*] (with $v_0 = v$), and so (b) does not hold.

If $p = \chi(\{v, w\})$, for some link $\{v, w\}$ in $E$, then $\chi(\{v, w\})$ is adjacent to $\chi(\{v\})$, to $\chi(\{w\})$, to all $\chi(\{v, u\})$ for $v \sim u$, to all $\chi(\{w, u\})$ for $w \sim u$ and to all $\chi(\{u\})$ for $v \sim u$ and $w \sim u$, and to no more vertex. Because $\chi(\{v, w\})$ must be adjacent to $|V|$ vertices, the neighborhoods $N(v)$ of $v$ and $N(w)$ of $w$ in $\Gamma$ must be disjoint and the nodes linked to neither $v$ nor $w$ must form a stable set; also, a node in $\{v\} \cup N(v)$ is never linked to a node linked to neither $v$ nor $w$. Two cliques appear: the clique $C$ formed by the vertex $\chi(\{v\})$, the vertices $\chi(\{v, u\})$ for $u \in N(v)$ and the vertices $\chi(\{w, u\})$ for $u \in N(w)$. Moreover, $\chi(\{v\})$ is adjacent to no vertex in $D$. Because of the present assumption on $p = \chi(\{v, w\})$, there exists a bipartition $C$, $D$ of $V$ as in Condition [*] (with $v_0 = v$).

(c) $\Rightarrow$ (d). The implication is trivial.

(d) $\Rightarrow$ (a). Any combinatorial automorphism of the polytope $P(\Gamma)$ is also an automorphism of the skeleton of $P(\Gamma)$.

To any automorphism $\alpha$ of the graph $\Gamma$, we now associate a combinatorial automorphism $F(\alpha)$ of the polytope $P(\Gamma)$ which fixes the vertex $\chi(\emptyset)$. Because $\alpha$ permutes the nodes $u$ of $\Gamma$, it induces a permutation $\alpha'$ of the characteristic vectors $\chi(\{u\})$. As the latter vectors form the canonical basis of $\mathbb{R}^V$, there is a unique linear permutation $\alpha''$ of $\mathbb{R}^V$ which extends $\alpha'$, and of course $\alpha''$ fixes $\chi(\emptyset)$, the origin. Because the canonical basis is orthonormal, $\alpha''$ is an isometry. Moreover, for any link $\{v, w\}$ of the graph $\Gamma$, we see that $\alpha''$ maps the vertex $\chi(\{v, w\})$ of $P(\Gamma)$ onto the vertex $\chi(\{\alpha(v), \alpha(w)\})$ (because $\chi(\{v, w\}) = \chi(\{v\}) + \chi(\{w\})$ and $\alpha''$ is linear). Thus the linear permutation $\alpha''$ stabilizes the set of vertices of the polytope $P(\Gamma)$, and so $\alpha''$ induces a combinatorial automorphism of the polytope which fixes $\chi(\emptyset)$; we denote this combinatorial automorphism by $F(\alpha)$.
Theorem 3.5 The mapping $F$ defined just above is an injective homomorphism from the group $A$ of automorphisms of the graph $\Gamma$ into the group $B$ of combinatorial automorphisms of the polytope $P(\Gamma)$. When the graph $\Gamma$ satisfies Condition [*], the mapping $F$ is a group isomorphism from $A$ to $B$, and moreover any combinatorial automorphism of $P(\Gamma)$ is induced by some isometry of $P(\Gamma)$.

Proof By its construction, the mapping $F: A \rightarrow B$ is an injective homomorphism of groups. To show that $F$ is surjective when $\Gamma$ satisfies Condition [*], consider any combinatorial automorphism $\beta$ of the polytope $P(\Gamma)$. By Lemma 3.4, $\beta$ fixes $\chi(\emptyset)$. Hence $\beta$ stabilizes the neighborhood of $\chi(\emptyset)$, and induces an automorphism $\beta^*$ of the graph induced on the neighborhood. As the latter graph is isomorphic to the complement graph $\overbar{\Gamma}$ (Corollary 3.2(ii)), $\beta^* = \alpha'$ for some automorphism $\alpha$ of the graph $\Gamma$ (the notation $\alpha'$ was introduced just before the statement we are now proving). We show $\beta = F(\alpha)$. First, $\beta$ and $F(\alpha)$ are combinatorial automorphisms fixing $\chi(\emptyset)$ which have the same action on the vertices $\chi(\{u\})$ for $u \in V$. Second, for any combinatorial automorphism $\gamma$ fixing $\chi(\emptyset)$, the action of $\gamma$ on the vertices of the form $\chi(e)$, for $e \in E$, is determined by the action of $\gamma$ on the vertices $\chi(\{u\})$, for $u \in V$. Indeed, if $e = \{v, w\}$, then $\chi(e)$ is the only remaining vertex of the 2-dimensional face containing the vertices $\chi(\emptyset), \chi(\{v\})$ and $\chi(\{w\})$ (the latter face is defined by the affine inequality $\sum_{u \in V \setminus \{v, w\}} x_u \geq 0$). Finally, by its definition, $F(\alpha)$ is always the restriction to the set of vertices of an isometry of $P(\Gamma)$. □

The before last argument in the proof shows in fact that any permutation of the set of vertices of $P(\Gamma)$ which fixes $\chi(\emptyset)$ and maps the vertices of any 2-dimensional face to the vertices of some 2-dimensional face is a combinatorial automorphism. It would be nice to characterize the graphs $\Gamma$ for which any automorphism of the skeleton of the polytope $P(\Gamma)$ necessarily is a combinatorial automorphism of $P(\Gamma)$. Proposition 3.7 below provides partial answers.

Example 3.6 Let the graph $\Gamma$ be a six-cycle. Then there is a non-identical automorphism $\rho$ of the skeleton of $P(\Gamma)$ which fixes $\chi(\emptyset)$ and is not a combinatorial automorphism of $P(\Gamma)$. To obtain such an automorphism, let $\rho$ fix all the vertices $\chi(\{u\})$ for $u \in V$, and map the vertex $\chi(e)$ for any link $e$ in $E$ to the vertex $\chi(f)$, with $f$ the link opposite to $e$ in the six-cycle.

No other graph $\Gamma$ which is a cycle leads to a special automorphism of the skeleton as in Example 3.6: the assertion follows from the next proposition. The neighborhood of a link $\{u, w\}$ of the graph $\Gamma$ is the set

$$N(\{u, w\}) = \{v \in V \setminus \{u, w\} \mid v \sim u \text{ or } v \sim w\}.$$  

By Proposition 3.1 (iii), for $v \in V$ and $e \in E$, we have $v \in N(e)$ exactly when the vertices $\chi(v)$ and $\chi(e)$ of $P(\Gamma)$ are not adjacent.

Proposition 3.7 If there exists some automorphism of the skeleton of $P(\Gamma)$ which fixes $\chi(\emptyset)$ and is not a combinatorial automorphism of $P(\Gamma)$, then the graph $\Gamma$ contains two links $e$ and $f$ satisfying

$$e \sim f.$$
χ(∅) of neighbours of ∅ is not a combinatorial automorphism of P(∅).

When the graph Γ does not contain any four-cycle, the converse also holds.

Proof Let γ be some automorphism of the skeleton of P(Γ) which fixes χ(∅) and is not a combinatorial automorphism of P(Γ). Thus γ stabilizes the set ℳ(χ(∅)) of neighbours of χ(∅), and γ induces an automorphism of the graph induced by the skeleton on ℳ(χ(∅)). Because the induced graph is isomorphic to the complement of Γ (Corollary 3.2), there exists some automorphism α of Γ such that the combinatorial automorphism F(α) and γ acts the same way on ℳ(χ(∅)); they moreover fix χ(∅) (by our assumption on γ and the definition of F(α)). Setting β equal to the product (F(α))⁻¹ ◦ γ, we get an automorphism of the skeleton which fixes χ(∅) and each vertex in ℳ(χ(∅)). As γ is not a combinatorial automorphism, β differs from the identity. Hence β must send some vertex χ(e) to some vertex χ(f), where e and f are distinct links in Γ. Consequently, χ(e) and χ(f) are adjacent to the same vertices in ℳ(χ(∅)). By Proposition 3.1 (iii), e and f satisfy (i) and (ii) in the statement.

Conversely, when Γ does not contain any four-cycle, the graph induced by the skeleton on {χ(d) | d ∈ E} is complete. Then the permutation which exchanges χ(e) and χ(f) (for e and f as in the statement), while leaving all other vertices of P(Γ) fixed, is an automorphism of the skeleton; it is not a combinatorial automorphism (because it fixes χ(∅) and all χ(⟨u⟩) for u ∈ V).

If some graph Γ contains two links e and f as in Proposition 3.7, it is easy to build an augmented graph Γ′ having the same automorphism group as Γ but containing no such pair of links: it suffices to add for any node v of Γ two new nodes v′ and v″ with two new links {v, v′} and {v′, v″} (in case two nodes of Γ have the same neighborhood only if they are unlinked, it even suffices to add for each node v only one new node v′ and one new link {v, v′}).

4 Building a Binary Polytope for Any Group

Given any finite group G, we now build a convex polytope P_G as in Theorem 1.1—however, we first leave Property (v) out of our discussion. As recalled in Sect. 2, there exists a graph Γ = Γ(G) whose automorphism group is G. If Γ does not satisfy Condition [*] of Sect. 3, we replace the graph Γ with its complement but keep the notation Γ for the resulting graph. Notice that now the graph Γ satisfies Condition [*], except for the graph having only one node, and for three particular pairs of complementary graphs on 2, 3 or 4 nodes respectively—each time, a path and its complement. In the first case, we take for our convex polytope P_G the polytope having only one vertex (at the origin); in each of the three other particular cases, the automorphism group of the graph(s) is the cyclic group of order 2 and we take for our polytope P_G the segment in ℝ¹ with endpoints 0 and 1. When the graph Γ satisfies Condition [*], we may apply Corollaries 3.2, 3.3 and Proposition 3.5: the polytope P_G = P(Γ(G)) satisfies Properties (i)–(iv) in Theorem 1.1.

Let us discuss how large the resulting polytope P_G = P(Γ(G)) is with respect to the order n of the group G. First, recall that for any graph Γ the dimension of P(Γ)
equals the number of nodes in $\Gamma$ (Corollary 3.3). We saw in Sect. 2 that there is a graph $\Gamma(G)$ with at most $2n$ nodes, except for the three exceptional groups $C_3, C_4$ and $C_5$. So apart from three exceptional groups, a careful choice of the graph $\Gamma$ delivers a polytope $P_G = P(\Gamma(G))$ of dimension at most $2n$. For $C_3$, there is a graph with 9 nodes, for $C_4$ with 10 nodes, for $C_5$ with 15 nodes such that all three graphs satisfy Condition [*]. It might be that another construction delivers polytopes with the desired properties and dimension less that 9, 10 and 15 respectively. Furthermore, in view of the result of [5] recalled in Sect. 2, we can even build the polytope $P_G$ in a space of dimension at most $n$ when $G$ does not belong to the list of exceptional groups given in Sect. 2.

What about the number of vertices of $P_G = P(\Gamma(G))$? Assuming that the dimension of the polytope has been minimized, we might want to decrease the number of vertices as much as possible. In other words, having minimized the number of nodes in the graph $\Gamma$ with automorphism group $G$, we next want to minimize the number of links. Characterizations of such minimal graphs exist for certain groups, see for instance McCarthy and Quintas [11]. If we agree to increase the dimension of the polytope $P_G$ to (at most) $2n + 1$, where again $n = |G|$, we may use a result of Babai [4]: if $g$ is the minimum number of generators of $G$ and $G$ is neither $C_3, C_4$ or $C_5$, there is a graph $\Gamma$ with automorphism group $G$ and at most $2n + 1$ nodes and $2n(g + 1)$ links (because $\Gamma$ contains three-cycles, it satisfies Condition [*]). Our construction then produces a polytope of dimension at most $2n + 1$ and with at most $2n(g + 2) + 2$ vertices.

We now establish Theorem 1.1, this time taking into account Property (v) on the automorphism group of the skeleton. Assume the given group $G$ is of order at least 3. To prove the full theorem, we again start by taking a graph $\Gamma$ whose automorphism group is $G$. Next, as we did at the end of Sect. 3, we build the augmented graph $\Gamma'$. As $\Gamma'$ always satisfies Condition [*] and has no pair of links $e, f$ as in Proposition 3.7, the polytope $P(\Gamma')$ satisfies all properties in Theorem 1.1 (as seen from Corollaries 3.2, 3.3, Lemma 3.4 and Propositions 3.5, 3.7).

As announced in the introduction, we now deduce that for any finite group $G$ there is a directed graph whose asymmetric traveling-salesman polytope has its automorphism group isomorphic to $G$. This follows at once from Theorem 1.1 combined with a nice result of Billera and Sarangarajan [6], which states that any binary, convex polytope is affinely isomorphic to the asymmetric traveling-salesman polytope of some directed graph.

Acknowledgements We would like to thank Selim Rexhep, a past Ph.D. student, for his many interesting questions and in particular the one asking for the existence of a convex polytope for any finite group. We thank also two anonymous reviewers for their useful comments on a preliminary version.

References

1. Arlinghaus, W.C.: The Classification of Minimal Graphs with Given Abelian Automorphism Group. Memoirs of the American Mathematical Society, vol. 330. American Mathematical Society, Providence (1985)
2. Babai, L.: On the minimum order of graphs with given group. Can. Math. Bull. 17(4), 467–470 (1974)
3. Babai, L.: Symmetry groups of vertex-transitive polytopes. Geom. Dedicata 6(3), 331–337 (1977)
4. Babai, L.: On the abstract group of automorphisms. In: Temperley, H. (ed.) Combinatorics. London Mathematical Society Lecture Notes, vol. 52, pp. 1–40. Cambridge University Press, Cambridge (1981)
5. Babai, L., Godsil, C.D.: On the automorphism groups of almost all Cayley graphs. Eur. J. Comb. 3(1), 9–15 (1982)
6. Billera, L., Sarangarajan, A.: All 0–1 polytopes are traveling salesman polytopes. Combinatorica 16(2), 175–188 (1996)
7. Frucht, R.: Herstellung von Graphen mit vorgegebener abstrakter Gruppe. Compos. Math. 6, 239–250 (1939)
8. Godsil, C.D.: GRRs for nonsolvable groups. In: Algebraic Methods in Graph Theory, Vol. I, II. Colloquium Mathematica Societatis János Bolyai, vol. 25, pp. 221–239. North-Holland, Amsterdam (1981)
9. Hevia, H.: Grafos con grupo dado de automorfismos. Proyecciones 14, 139–167 (2011)
10. Matsui, T., Tamura, S.: Adjacency on combinatorial polyhedra. Discrete Appl. Math. 56(2–3), 311–321 (1995)
11. McCarthy, D.J., Quintas, L.V.: The construction of minimal-line graphs with given automorphism group. In: Frank, F. (ed.) Topics in Graph Theory. Annals of the New York Academy of Science, vol. 328, pp. 144–152. New York Academy of Sciences, New York (1979)
12. Naddef, D., Pulleyblank, W.R.: Hamiltonicity and combinatorial polyhedra. J. Comb. Theory Ser. B 31(3), 297–312 (1981)
13. Robinson, D.J.S.: A Course in the Theory of Groups. Graduate Texts in Mathematics, 2nd edn. Springer, New York (1996)
14. Schulte, E., Williams, G.I.: Polytopes with preassigned automorphism groups. Discrete Comput. Geom. 54(2), 444–458 (2015)
15. Tran, T., Ziegler, G.M.: Extremal edge polytopes. Electron. J. Comb. 21(2), 2.57 (2014)