



Resolute and symmetric mechanisms for two-sided matching problems

Daniela Bubboloni ^a, Michele Gori ^{b,*}, Claudia Meo ^c

^a Dipartimento di Matematica e Informatica U.Dini, Università degli Studi di Firenze, viale Morgagni 67/a, 50134 Firenze, Italy

^b Dipartimento di Scienze per l'Economia e l'Impresa, Università degli Studi di Firenze, via delle Pandette 9, 50127 Firenze, Italy

^c Dipartimento di Scienze Economiche e Statistiche, Università degli Studi di Napoli Federico II, via Cintia, 80126 Napoli, Italy

ARTICLE INFO

Manuscript handled by Editor H. Gaoji

Keywords:

Matching mechanism
Stability
Fairness
Symmetry
Group theory

ABSTRACT

We focus on the one-to-one two-sided matching model with two disjoint sets of agents of equal size, where each agent in a set has preferences on the agents in the other set modeled by a linear order. A matching mechanism associates a set of matchings to each preference profile; resoluteness, that is the capability to select a unique matching, and stability are important properties for a matching mechanism. The two versions of the deferred acceptance algorithm are resolute and stable matching mechanisms but they are unfair since they strongly favor one side of the market. We introduce a property for matching mechanisms that relates to fairness; such property, called symmetry, captures different levels of fairness and generalizes existing notions. We provide several possibility and impossibility results mainly involving the most general notion of symmetry, known as gender fairness, resoluteness, stability, weak Pareto optimality and minimal optimality. In particular, we prove that: resolute, gender fair matching mechanisms exist if and only if each side of the market consists of an odd number of agents; there exists no resolute, gender fair, minimally optimal matching mechanism. Those results are obtained by employing algebraic methods based on group theory, an approach not yet explored in matching theory.

1. Introduction

In this paper, we analyze issues about fairness for matching models with two sides. In these models there are two disjoint sets of agents and each agent on one side has preferences over the agents on the other side. Agents on different sides have to be matched taking into account these preferences. A wide range of allocation problems from diverse fields can be analyzed within such a framework. Well-known examples include the college admissions market, the labor market for medical interns, and online dating markets.

Our focus is, in particular, on the most basic example of matching models with two sides, the so-called marriage model (Gale and Shapley, 1962). We denote by W and M the two disjoint sets of women and men, respectively, and assume that they have the same size, called the market size. Moreover, the preference relation of each woman is modeled by a linear order on the set M ; analogously, the preference relation of each man is modeled by a linear order on the set W . Since the two sets W and M are fixed, a marriage model is described by a profile of linear orders, one for each individual. Given a marriage model, one is interested to determine a matching, that is, a bijective function from the set $I = W \cup M$ of individuals to itself that associates

each woman with a man, each man with a woman, and has the additional property of being equal to its inverse.

Stability is a highly desirable property a matching may meet. A matching is stable if there is no blocking pair, namely, a woman and a man who both prefer each other to their current partners in the matching. In their seminal paper, Gale and Shapley (1962) proved that every marriage model admits a stable matching and described an algorithm that finds such a matching. The algorithm has two versions that differ in terms of which group proposes matches and which one accepts or rejects each proposal. In general, the stable matchings produced by the two versions are different. Gale and Shapley proved that the stable matching generated by the algorithm when women propose is optimal for all the women, in the sense that it pairs each woman with the best partner she can obtain among all the stable matchings. However, it pairs each man with the worst partner he can obtain among all the stable matchings.¹ This matching is called the woman-proposing stable matching. Symmetrically, the man-proposing stable matching is the best stable matching for men and the worst stable matching for women.

A correspondence that associates a set of matchings with each preference profile is called a matching mechanism. Hence, a matching

* Corresponding author.

E-mail addresses: daniela.bubboloni@unifi.it (D. Bubboloni), michele.gori@unifi.it (M. Gori), claudia.meo@unina.it (C. Meo).

¹ This property is a consequence of a more general result due to Knuth (1976). See, also, Roth (1990), Theorem 2.13 and Corollary 2.14.

² For the definitions of these two mechanisms see Section 4.1.

mechanism operates as a centralized clearinghouse that collects the preferences of all market participants and provides a set of matchings. Several properties may be imposed on a matching mechanism. First, a matching mechanism is required to be non-empty valued. Especially when used for practical applications, a matching mechanism should also be resolute, that is, it should be able to select a unique matching for each preference profile. Stability is a further desirable property for matching mechanisms, particularly from a practical point of view: a matching mechanism is stable if it selects a set of stable matchings for each preference profile. Among stable matching mechanisms, the two mechanisms GS_w and GS_m , which associate with each preference profile the woman-proposing stable matching and the man-proposing stable matching respectively, are very popular and have been implemented in practice, for instance, in the National Resident Matching Program (NRMP) to match doctors to residency programs or fellowships and also in some school districts to match students to high schools (Roth, 1984; Abdulkadiroğlu and Sönmez, 2003). In many cases, matching mechanisms that are not stable had largely failed and been abandoned while the stable ones succeeded and survived (see, for example, Roth, 1991). However, especially when matchings are imposed rather than proposed to agents, other properties appear more compelling than stability. Indeed, a matching mechanism is expected to be non-discriminatory towards agents, that is, some form of fairness should be satisfied. The two mechanisms GS_w and GS_m clearly fail such objective because they favor one side of the market (women and men, respectively) over the other. This has motivated the design of alternative matching mechanisms in order to reduce the conflict of interests between women and men. We can mention, among others, the Sex-Equal matching mechanism (Gusfield and Irving, 1989; Romero-Medina, 2001) and the Egalitarian Stable matching mechanism (Gusfield and Irving, 1989).² All these mechanisms share a common approach: first, a measure is introduced to quantify the fairness of a matching; then, such measure is optimized (usually, minimized due to its interpretation) on the set of stable matchings. A recap of several of these matching mechanisms can be found in Cooper and Manlove (2020).

In this paper, we take a different approach to fairness based on the idea that individuals should be treated independently of their identities: a mechanism is fair if a change in the identities of the individuals results in the same change in the output.³ Given the bilateral nature of the model, fairness may concern either just agents belonging to the same group (women or men) or the totality of individuals. Indeed, in many situations, it is natural to require that no woman should gain a systematic advantage over the other women on the basis of her identity and, symmetrically, no man should gain a systematic advantage on the other men on the basis of his identity. This property is called anonymity in the literature (see, for instance, Sasaki and Toda, 1992; Halaburda, 2010). On the other hand, in other circumstances, it could be natural to require that neither women nor men should have an advantage on the other group solely on the basis of their gender. A fairness notion of the latter kind has been firstly introduced in Masarani and Gokturk (1989) under the name of gender indifference: roughly speaking, it states that if we rename women as men and men as women according to a given fixed rule, this should result in a corresponding change of names in the matchings selected by the matching mechanism.⁴ A more

general version of gender indifference has been provided by Özkal-Sanver (2004) under the name of gender fairness; in such notion, which implies anonymity,⁵ women are renamed as men and men are renamed as women in any possible fashion.

In this paper, we introduce a general notion of fairness for matching mechanisms that we call symmetry. Anonymity, gender indifference and gender fairness can be seen as special instances of this notion. In order to provide an informal definition of symmetric mechanisms, we first need some preliminary notions about how to model changes both in the identities and, subsequently, in the preferences of the individuals.

First, we use permutations over the set I of individuals in order to model changes in the individual identities. In particular, we are interested in changes in the identities that account for the presence of two different types of individuals in the market. Hence, we focus on permutations over I that keep the partition $\{W, M\}$ of I fixed. We denote by G^* the set of such permutations. A permutation in G^* may refer to a change in individuals' identities either within the sets W and M or across them. We denote by G the set of permutations satisfying the former condition.

Second, we account for the fact that every permutation in G^* also affects preference profiles, that is, the complete list of individual preference relations. Suppose, for instance, that $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$ and let $\varphi \in G^*$ be the permutation that switches 1 and 4, 2 and 5, 3 and 6. If woman 1's preferences on M are $[5, 6, 4]$ ⁶ in a given preference profile, when individual identities are changed according to φ , we get that man 4's preferences on W are $[2, 3, 1]$ in the preference profile modified by φ .

The notion of symmetry that we introduce is the following. Consider a subset U of G^* . We say that a matching mechanism is U -symmetric if a change in individuals' names in the input according to a permutation in U entails the same change of names in the matchings of the output. The definition of U -symmetry is very general and allows to model diverse levels of fairness depending on which subset U of G^* is considered. In particular, gender fairness coincides with the notion of $(G^* \setminus G)$ -symmetry; anonymity is equivalent to G -symmetry; gender indifference coincides with $\{\varphi\}$ -symmetry, where φ is a matching. It is also worth mentioning that if $U \subseteq V \subseteq G^*$, then V -symmetry implies U -symmetry and so G^* -symmetry is the strongest possible level of symmetry a matching mechanism may meet.

By analyzing some matching mechanisms frequently used in the literature, a clear contrast between resoluteness and G^* -symmetry emerges. For instance, the matching mechanisms GS_w and GS_m are resolute, G -symmetric (i.e. anonymous) but, as one may expect, fail to be G^* -symmetric. On the other hand, the mechanism that associates with any preference profile the set of the stable matchings is G^* -symmetric but far from being resolute. Analogously, the Sex-Equal and the Egalitarian Stable matching mechanisms, introduced by Gusfield and Irving (1989) to reduce the conflict of interests between the two parts by selecting suitable stable matchings, are both G^* -symmetric but not resolute.⁷

On the basis of those observations, in this paper we undertake the following research project: under the assumption that W and M have the same size, studying the existence of matching mechanisms that are resolute, satisfy some form of symmetry and, possibly, fulfill some optimality properties like, for instance, stability.

The following theorem, which is the main finding in our paper, is about the strongest possible level of symmetry and does not involve any optimality condition.

³ Our interpretation of fairness is somehow close to the concept of procedural fairness analyzed in Klaus and Klijn (2006) and based on probabilistic considerations: a (random) mechanism is procedurally fair whenever each agent has the same probability to move at a certain point in the procedure that determines the final probability distribution.

⁴ Masarani and Gokturk (1989) only consider resolute matching mechanisms (or, matching algorithms, as they call them). Moreover, they account only for a specific change in the identities of individuals, namely, if $W = \{1, \dots, n\}$ and $M = \{n+1, \dots, 2n\}$, then woman 1 becomes man $n+1$ and vice versa, woman 2 becomes man $n+2$ and vice versa, and so on. Endriss (2020) and Root and Bade (2023) also analyze gender indifference, with the latter authors referring to this property as weak gender-neutrality.

⁵ See Proposition 3.1 in Özkal-Sanver (2004). See also Section 3.4 in this paper.

⁶ Throughout the paper we represent linear orders with ordered lists with obvious meaning: for instance, the writing $[5, 6, 4]$ representing woman 1's preferences on M means that woman 1 prefers man 5 to man 6, and man 6 to man 4.

⁷ See Propositions 9 and 10 in Appendix B.2.

Theorem 1. *There exists a resolute and G^* -symmetric matching mechanism if and only if the market size is odd.*

Assuming that the market size is odd, a natural question is whether the existence of a resolute and G^* -symmetric matching mechanism continues to be guaranteed when one also asks for some optimality condition. We provide a negative answer. Indeed, we prove that resoluteness and G^* -symmetry together cannot coexist even with a very weak optimality condition that we introduce in our paper and call minimal optimality.⁸

Theorem 2. *For every market size, there exists no resolute, G^* -symmetric and minimally optimal matching mechanism.*

Since minimal optimality is weaker than both Pareto optimality and weakly Pareto optimality⁹ which, in turn, are weaker than stability (see Proposition 1), the previous result implies that there are no resolute, G^* -symmetric and stable [Pareto optimal; weakly Pareto optimal] matching mechanisms.

From Theorem 2, it turns out that resoluteness and G^* -symmetry are basically incompatible with any type of optimality condition. On the other hand, for every $U \subseteq G$, that is, for every set of permutations that exchange individuals' identities only within the two groups W and M , resoluteness and U -symmetry are consistent with stability. Indeed, as already observed, GS_w and GS_m are resolute, stable and G -symmetric, and then they are U -symmetric, as well. We investigate then whether some optimality conditions may be consistent with resoluteness and a minimal level of symmetry across the two groups W and M , that is, $\{\varphi\}$ -symmetry, where $\varphi \in G^* \setminus G$ is a fixed matching. The results we find are summarized below.

Theorem 3. *For every market size and every matching φ , there exists a resolute, $\{\varphi\}$ -symmetric and weakly Pareto optimal matching mechanism.*

Theorem 4. *If the market size is 2, then, for every matching φ , there exists a resolute, $\{\varphi\}$ -symmetric and stable matching mechanism.*

Theorem 5. *If the market size is at least 3, then, for every matching φ , there exists no resolute, $\{\varphi\}$ -symmetric and stable matching mechanism.*

Thus, while Theorem 3 shows that resoluteness and $\{\varphi\}$ -symmetry are consistent with weak Pareto optimality, Theorems 4 and 5 state that they are not consistent with stability, unless the market size is two.

We remark that some impossibility results concerning stability, resoluteness, and some sort of fairness have been provided in the literature about matching mechanisms. Masarani and Gokturk (1989) basically show that resoluteness, G^* -symmetry, stability, and a further axiom called maximin optimality cannot coexist. Endriss (2020) instead proves Theorem 5 using tools from logic and computer science. We present here an alternative proof of Theorem 5. In fact, our paper is based on a strongly innovative methodology. Specifically, all our main results are proved by exploiting notions and techniques from group theory. While an algebraic approach based on symmetric groups and groups actions has been already successfully used in social choice literature (Egocioğlu, 2009; Egocioğlu and Giritligil, 2013; Bubboloni and Gori, 2014, 2015, 2016, 2021, 2025; Doğan and Giritligil, 2015;

⁸ A matching is minimally optimal if there is at least an individual who does not obtain her/his worst choice (Definition 1). A matching mechanism is minimally optimal if it only selects minimally optimal matchings (Definition 4).

⁹ A matching is Pareto optimal if there is no other matching that makes at least one individual better off and no individuals worse off; weakly Pareto optimal if there is no other matching that makes all the individual better off (Definition 1). A matching mechanism is Pareto optimal [weakly Pareto optimal] if it only selects Pareto optimal [weakly Pareto optimal] matchings (Definition 4).

Bartholdi et al., 2021; Kivinen, 2023, 2024), at the best of our knowledge, this is the first time that such an approach has been employed in matching theory to provide general possibility and impossibility results.

Concepts and theorems from group theory turn out to be powerful tools in situations where permutations play an important role. Since matchings are themselves special permutations of the set I and the various levels of fairness that a matching mechanism may meet can be described through suitable sets of permutations of the set I , the application of group theory within matching theory emerges naturally. The use of group theory allows for new methods to prove known results (e.g., Theorem 5) and helps in finding new results (e.g., Theorem 1). Furthermore, group theory enhances our understanding of symmetry. In particular, it is possible to prove that a matching mechanism is symmetric with respect to a set U of permutations of I if and only if it is symmetric with respect to the group generated by U (Proposition 2). That fact has significant consequences: for instance, using non-obvious results from group theory, it can be shown that the combination of anonymity and gender indifference is equivalent to G^* -symmetry, and that gender fairness is also equivalent to G^* -symmetry. Moreover, knowing that only subgroups matter, we get that the possible levels of symmetry of a matching mechanism are as many as the subgroups of G^* .

The paper is organized as follows. Section 2 contains some basic preliminaries about groups, permutations and relations needed for the model. In Section 3 we illustrate the setup and the key notion of symmetric matching mechanism. In Section 4 we state our research problem and present the main results of the paper. A generalization to the model with outside option is presented in Section 5. Finally, Section 6 concludes. The appendices collect several notions and results about matchings, matching mechanisms and group theory, and most of the proofs. Appendix C, in particular, is crucial as it presents technical results from group theory that play a central role in the proof of the main theorem of our paper.

2. Preliminaries

Throughout the paper, $\mathbb{N}$ denotes the set of positive integers. Given $k \in \mathbb{N}$, we set $\llbracket k \rrbracket := \{m \in \mathbb{N} : m \leq k\}$.

2.1. Groups and permutations

A finite group is a finite set endowed with an operation that is associative, admits a neutral element and has the property that each element admits an inverse. In a generic group the neutral element is denoted by 1. However, for specific groups, the notation can be specialized. Let H be a finite group and $K \subseteq H$. We say that K is a subgroup of H , and we write $K \leq H$, if the restriction of the operation on H to the set K produces a group structure for K . It is well known that, since H is finite, $K \leq H$ if and only if $K \neq \emptyset$ and, for every $h, k \in K$, the product hk belongs to K . Clearly, if $K' \leq K$ and $K \leq H$, then $K' \leq H$.¹⁰

Let X be a finite set. $\text{Sym}(X)$ denotes the group of bijective functions from X to itself with the operation defined, for every $\varphi_1, \varphi_2 \in \text{Sym}(X)$, by the right-to-left composition $\varphi_1 \varphi_2 \in \text{Sym}(X)$.¹¹ The neutral element of $\text{Sym}(X)$ is the identity function on X , denoted by id_X . $\text{Sym}(X)$ is called the symmetric group on X and its elements are called permutations of X .

Given $k \in \mathbb{N}$ with $2 \leq k \leq |X|$, we say that $\varphi \in \text{Sym}(X)$ is a k -cycle if there exist distinct $x_1, \dots, x_k \in X$ such that $\varphi(x_i) = x_{i+1}$ for all

¹⁰ We refer to Milne (2021) for a reader-friendly but wide introduction to group theory, which turns out to be substantially exhaustive for the purposes of our paper.

¹¹ One of the reasons why we refer to Milne (2021) instead of to more classical references, such as Robinson (1996), is that Milne adopts the right-to-left composition while usually the left-to-right one is used.

$i \in \llbracket k-1 \rrbracket$, $\varphi(x_k) = x_1$, and $\varphi(x) = x$ for all $x \in X \setminus \{x_1, \dots, x_k\}$. In such a case, φ is denoted by $(x_1 \dots x_k)$, the set $\{x_1, \dots, x_k\}$ is called the support of φ and k is called the length of φ . For instance, if $X = \llbracket 5 \rrbracket$, $\varphi = (134)$ denotes the element of $\text{Sym}(X)$ such that $\varphi(1) = 3$, $\varphi(2) = 2$, $\varphi(3) = 4$, $\varphi(4) = 1$, $\varphi(5) = 5$, and is a 3-cycle. We say that a permutation of X is a cycle if it is a k -cycle for some $k \in \mathbb{N}$ with $2 \leq k \leq |X|$. A result on permutations (see Proposition 4.26 in Milne, 2021) ensures that any permutation of X different from id_X can be expressed, in a unique way up to reordering, as the product of commuting cycles whose supports are pairwise disjoint. Such a product is called the cycle decomposition of the permutation. For instance, if $X = \llbracket 6 \rrbracket$ and $\varphi \in \text{Sym}(X)$ is defined by $\varphi(1) = 3$, $\varphi(2) = 4$, $\varphi(3) = 1$, $\varphi(4) = 6$, $\varphi(5) = 5$, $\varphi(6) = 2$, we have that $\varphi = (13)(246) = (246)(13)$. In what follows, we always write permutations different from the identity using their cycle decomposition.

2.2. Relations

Let X be a nonempty and finite set. A relation on X is a subset of X^2 . The set of the relations on X is denoted by $\mathbf{R}(X)$.

Let $R \in \mathbf{R}(X)$. Given $x, y \in X$, we usually write $x \geq_R y$ instead of $(x, y) \in R$ and $x >_R y$ instead of $(x, y) \in R$ and $(y, x) \notin R$. We say that R is complete if, for every $x, y \in X$, $x \geq_R y$ or $y \geq_R x$; antisymmetric if, for every $x, y \in X$, $x \geq_R y$ and $y \geq_R x$ imply $x = y$; transitive if, for every $x, y, z \in X$, $x \geq_R y$ and $y \geq_R z$ imply $x \geq_R z$; a linear order if it is complete, transitive and antisymmetric. The set of linear orders on X is denoted by $\mathbf{L}(X)$.

Let $R \in \mathbf{L}(X)$. Given $x \in X$, we set $\text{Rank}_R(x) = |\{y \in X : y \geq_R x\}|$. If $|X| = n$, we represent R by an ordered list $[x_1, \dots, x_n]$, where $X = \{x_1, \dots, x_n\}$ and, for every $i, j \in \llbracket n \rrbracket$, $x_i \geq_R x_j$ if and only if $i \leq j$. Such a representation completely encodes the relation R . Note also that if $R = [x_1, \dots, x_n]$, then, for every $i \in \llbracket n \rrbracket$, $\text{Rank}_R(x_i) = i$. Thus, for every $x \in X$, the number $\text{Rank}_R(x)$ represents the position of x in the ordered list representing R .

Let $R \in \mathbf{L}(X)$, Y be a finite set with $X \subseteq Y$, and $\varphi \in \text{Sym}(Y)$. We denote by φR the relation on $\varphi(X)$ defined by

$$\varphi R := \{(x, y) \in \varphi(X)^2 : (\varphi^{-1}(x), \varphi^{-1}(y)) \in R\}. \quad (1)$$

Note that, for every $x, y \in X$, $(x, y) \in R$ if and only if $(\varphi(x), \varphi(y)) \in \varphi R$. It can be easily checked that if $\varphi_1, \varphi_2 \in \text{Sym}(Y)$, then $(\varphi_1 \varphi_2) R = \varphi_1(\varphi_2 R)$. Hence, the writing $\varphi_1 \varphi_2 R$ is not ambiguous.

The following lemma will be fundamental to set up our model in the next section.

Lemma 1. *Let X and Y be nonempty finite sets with $X \subseteq Y$, $R \in \mathbf{L}(X)$ and $\varphi \in \text{Sym}(Y)$. Then the following facts hold true:*

- (i) *if $R = [x_1, \dots, x_n]$, where $X = \{x_1, \dots, x_n\}$, then $\varphi R \in \mathbf{L}(\varphi(X))$ and $\varphi R = [\varphi(x_1), \dots, \varphi(x_n)]$;*
- (ii) *$\varphi R = R$ if and only if, for every $x \in X$, $\varphi(x) = x$.*

Proof. (i) Assume that $R = [x_1, \dots, x_n]$, where $X = \{x_1, \dots, x_n\}$. Of course, $\varphi(X) = \{\varphi(x_1), \dots, \varphi(x_n)\}$. Consider $i, j \in \llbracket n \rrbracket$. We know that $x_i \geq_R x_j$ if and only if $i \leq j$. By the definition of φR , we deduce that $\varphi(x_i) \geq_{\varphi R} \varphi(x_j)$ if and only if $x_i \geq_R x_j$. Thus, we have that $\varphi(x_i) \geq_{\varphi R} \varphi(x_j)$ if and only if $i \leq j$. Then, we conclude that $\varphi R \in \mathbf{L}(\varphi(X))$ and $\varphi R = [\varphi(x_1), \dots, \varphi(x_n)]$.

(ii) If, for every $x \in X$, $\varphi(x) = x$, then, by (i), we get $\varphi R = R$. Assume now, conversely, that $\varphi R = R$. Then, the relations φR and R must be defined on the same set and so $\varphi(X) = X$. Moreover, they must have the same representation as ordered lists. Thus, we have that $[x_1, \dots, x_n] = [\varphi(x_1), \dots, \varphi(x_n)]$, which implies that $\varphi(x_i) = x_i$ for all $i \in \llbracket n \rrbracket$, that is, $\varphi(x) = x$ for all $x \in X$. $\square$

3. Setup of the model

3.1. Preference profiles

Let W and M be two finite disjoint sets with $|W| = |M| = n \geq 2$ and let $I := W \cup M$. We refer to the sets W , M and I as the set of women, the set of men and the set of individuals, respectively. We refer to n as the market size. For simplicity, we assume $W = \{1, \dots, n\}$ and $M = \{n+1, \dots, 2n\}$. In order to simplify the reading, we adopt the following rule throughout the paper (with few exceptions): the letter x is used to denote the elements of W , the letter y is used to denote the elements of M and the letter z is used to denote the elements of I .

Each woman has preferences on the set M and each man has preferences on the set W . We assume that the preferences of women are represented by linear orders on M and the preferences of men are represented by linear orders on W . A preference profile p is a function from I to $\mathbf{L}(W) \cup \mathbf{L}(M)$ such that, for every $x \in W$, $p(x) \in \mathbf{L}(M)$ and, for every $y \in M$, $p(y) \in \mathbf{L}(W)$. We denote by $\mathcal{P}$ the set of preference profiles. We represent a preference profile $p \in \mathcal{P}$ by the table

1	...	n	$n+1$	...	$2n$
$p(1)$	...	$p(n)$	$p(n+1)$	...	$p(2n)$

where in the first row there are the names of individuals and in the second row the corresponding preferences. For instance, if $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$, the table

1	2	3	4	5	6
4	4	6	2	3	3
5	6	5	1	1	2
6	5	4	3	2	1

(2)

represents the preference profile p such that

$$p(1) = [4, 5, 6] \in \mathbf{L}(M), \quad p(2) = [4, 6, 5] \in \mathbf{L}(M), \quad p(3) = [6, 5, 4] \in \mathbf{L}(M),$$

$$p(4) = [2, 1, 3] \in \mathbf{L}(W), \quad p(5) = [3, 1, 2] \in \mathbf{L}(W), \quad p(6) = [3, 2, 1] \in \mathbf{L}(W).$$

Note that, in the first row of the table representing a preference profile, the elements of I are written in increasing order. However, a reordering of the columns is always allowed. For example, the table in (2) and the tables

3	2	1	4	6	5
6	4	4	2	3	3
5	6	5	1	2	1
4	5	6	3	1	2

and

4	6	5	2	1	3
2	3	3	4	4	6
1	2	1	6	5	5
3	1	2	5	6	4

all represent the same preference profile.

3.2. Matchings

A matching is a permutation $\mu \in \text{Sym}(I)$ such that, for every $x \in W$, $\mu(x) \in M$; for every $y \in M$, $\mu(y) \in W$; for every $z \in I$, $\mu(\mu(z)) = z$. Since $y = \mu(x)$ implies $\mu(y) = \mu(\mu(x)) = x$, μ decomposes into the product of n disjoint 2-cycles, each of them having the form $(z \mu(z))$. Hence, the cycle decomposition of μ clearly illustrates what couples are formed under the matching μ . The set of matchings is denoted by $\mathcal{M}$.

Consider, for instance, $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$. Then we have that

$$\mathcal{M} = \left\{ (14)(25)(36), (14)(26)(35), (16)(25)(34), (15)(24)(36), (15)(26)(34), (16)(24)(35) \right\}.$$

Thus, for example, the matching $(14)(25)(36)$ pairs woman 1 with man 4, woman 2 with man 5 and woman 3 with man 6.

Note that $\mathcal{M}$ is a subset of $\text{Sym}(I)$, but it is not a subgroup $\text{Sym}(I)$ since $\text{id}_I \notin \mathcal{M}$.

Let us introduce some optimality conditions that a matching may meet. The first three are well known. The last one, to the best of our knowledge, is new.

Definition 1. Let $p \in \mathcal{P}$ and $\mu \in \mathcal{M}$. We say that μ is:

- *stable* for p if there is no pair $(x, y) \in W \times M$ such that $y \succ_{p(x)} \mu(x)$ and $x \succ_{p(y)} \mu(y)$;
- *Pareto optimal* for p if there is no matching $\mu' \in \mathcal{M}$ such that, for every $z \in I$, $\mu'(z) \succeq_{p(z)} \mu(z)$ and, for some $z^* \in I$, $\mu'(z^*) \succ_{p(z^*)} \mu(z^*)$;
- *weakly Pareto optimal* for p if there is no matching $\mu' \in \mathcal{M}$ such that, for every $z \in I$, $\mu'(z) \succeq_{p(z)} \mu(z)$;
- *minimally optimal* for p if there exists $z \in I$ such that $\text{Rank}_{p(z)}(\mu(z)) < n$.

Thus, a matching is not stable for p if there is a pair of individuals formed by a woman and a man such that both prefer each other to the partners assigned to them by the matching; such pairs are called, in the literature, “blocking pairs”. A matching is not Pareto optimal for p if there exists another matching making some individual better off without making any other individual worse off; not weakly Pareto optimal for p if there exists another matching making every individual better off; not minimally optimal for p if all the individuals are matched with their least preferred choice. It is worth noting that, given a preference profile p , there exists at most one matching that is not minimally optimal for p . The following proposition describes the relation among the properties in Definition 1. Its proof is in Appendix A.

Proposition 1. Let $p \in \mathcal{P}$ and $\mu \in \mathcal{M}$. Then the following facts hold true:

- (i) if μ is stable for p , then μ is Pareto optimal for p ;
- (ii) if μ is Pareto optimal for p , then μ is weakly Pareto optimal for p ;
- (iii) if μ is weakly Pareto optimal for p , then μ is minimally optimal for p .

Gale and Shapley (1962) proved that, for every $p \in \mathcal{P}$, a stable matching exists and provided an algorithm to find such a matching. In this algorithm, each side is assigned a specific role: according to their preferences, individuals on one side make proposals to individuals on the other side who are allowed to accept or refuse the proposals. Hence, the algorithm has two distinct versions, each producing a stable matching. Those matchings, in general, differ from each other, but both possess a special property. Indeed, Gale and Shapley proved that the matching resulting from the algorithm where women make proposals associates each woman with the best possible partner she can obtain within stable matchings, and each man with the worst possible partner he can obtain within stable matchings. Symmetrically, the algorithm where men make proposals associates each man with the best possible partner he can obtain within stable matchings, and each woman with the worst possible partner she can obtain within stable matchings. In the literature, these two matchings are frequently referred to as the woman-proposing stable matching and the man-proposing stable matching, respectively.

3.3. Matching mechanisms

A matching mechanism is a correspondence from $\mathcal{P}$ to $\mathcal{M}$. Thus, a matching mechanism is a procedure that allows to select a set of matchings for any given preference profile.

We denote by TO the matching mechanism that associates with any $p \in \mathcal{P}$ the whole set $\mathcal{M}$; by ST the matching mechanism that associates with any $p \in \mathcal{P}$ the set of matchings that are stable for p ; by GS_w [GS_m] the matching mechanism that associates with any $p \in \mathcal{P}$ the set having as unique element the woman-proposing [man-proposing] stable matching for p ; by GS the matching mechanism that associates with any $p \in \mathcal{P}$ the set whose elements are the woman-proposing stable matching and the man-proposing stable matching for p ; by PO the matching mechanism that associates with any $p \in \mathcal{P}$ the set of matchings that are Pareto optimal for p ; by WPO the matching mechanism that associates with any $p \in \mathcal{P}$ the set of matchings that

are weakly Pareto optimal for p ; by MO the matching mechanism that associates with any $p \in \mathcal{P}$ the set of the matchings that are minimally optimal for p .¹²

Let us introduce some basic definitions.

Definition 2. Let F be a matching mechanism. We say that F is:

- *decisive* if, for every $p \in \mathcal{P}$, $F(p) \neq \emptyset$;
- *resolute* if, for every $p \in \mathcal{P}$, $|F(p)| = 1$.

Of course, if F is resolute, then F is decisive. Note that GS , ST , PO , WPO , MO and TO are decisive but they are not resolute; on the other hand, GS_w and GS_m are resolute (Gale and Shapley, 1962).

Definition 3. Let F and F' be matching mechanisms. We say that F' is a *refinement* of F if, for every $p \in \mathcal{P}$, $F'(p) \subseteq F(p)$. If F' is a refinement of F we write $F' \subseteq F$.

Note that if F , F' and F'' are matching mechanisms, then $F'' \subseteq F'$ and $F' \subseteq F$ imply $F'' \subseteq F$. Moreover, we have that $GS \subseteq ST \subseteq PO \subseteq WPO \subseteq MO \subseteq TO$, $GS_w \subseteq GS$ and $GS_m \subseteq GS$.

Given a matching mechanism F , it is natural to interpret any refinement of F as a way to reduce the ambiguity of F . Resolute refinements of F are particularly important as they allow to completely eliminate the ambiguity of F . Of course, any decisive matching mechanism admits in general many resolute refinements, so it becomes important to understand whether some of them fulfill desirable properties.

The next definition presents some properties that a matching mechanism may have.

Definition 4. Let F be a matching mechanism. We say that F is *stable* [Pareto optimal; weakly Pareto optimal; minimally optimal] if, for every $p \in \mathcal{P}$ and $\mu \in F(p)$, μ is stable [Pareto optimal; weakly Pareto optimal; minimally optimal] for p .

Note that a matching mechanism F is stable [Pareto optimal; weakly Pareto optimal; minimally optimal] if and only if F is a refinement of ST [PO ; WPO ; MO].

3.4. Symmetric matching mechanisms

In this section, we define the key concept of our paper, that is, the notion of symmetric matching mechanism. Some preliminaries are needed before providing such a definition. First, we introduce some notation in order to model changes in individuals' identities. To this aim, we consider the subsets of $\text{Sym}(I)$ given by

$$G^* := \{\varphi \in \text{Sym}(I) : \{\varphi(W), \varphi(M)\} = \{W, M\}\},$$

and

$$G := \{\varphi \in \text{Sym}(I) : \varphi(W) = W, \varphi(M) = M\}.$$

It is immediately checked that G^* and G are subgroups of $\text{Sym}(I)$, G is a subgroup of G^* , and $\mathcal{M}$ is a subset of $G^* \setminus G$. These two groups will play a main role throughout the paper. G^* is formed by the permutations over I that keep the partition $\{W, M\}$ of I fixed; these permutations model changes in individuals' identities either within the sets W and M (i.e. women are renamed as women and men are renamed as men) or across them (i.e. women are renamed as men and men are renamed as women). G is formed by the permutations over I that transform the set W into itself and the set M into itself; those permutations only model changes in individuals' identities within the sets W and M . Note that, as a consequence, the permutations in $G^* \setminus G$ rename each woman with

¹² TO , ST , GS , PO , WPO , MO stand for “Total”, “Stable”, “Gale and Shapley”, “Pareto Optimal”, “Weakly Pareto Optimal”, “Minimally Optimal”, respectively.

one of men's names and each man with one of women's names. We can also distinguish two further subgroups of $\text{Sym}(I)$, namely

$$G_W := \{\varphi \in \text{Sym}(I) : \varphi(y) = y \text{ for all } y \in M\},$$

$$G_M := \{\varphi \in \text{Sym}(I) : \varphi(x) = x \text{ for all } x \in W\}.$$

G_W consists of the permutations of individuals' names that leave men's names unchanged; G_M consists of the permutations of individuals' names that leave women's names unchanged. Of course, G_W and G_M are subgroups of G . We also note that $|G^*| = 2(n!)^2$, $|G| = (n!)^2$ and $|G_W| = |G_M| = n!$, where n is the size of the market.

For example, if $W = \{1, 2\}$ and $M = \{3, 4\}$, we have that

$$G^* = \{id_I, (12), (12)(34), (13)(24), (14)(23), (1324), (1423)\}, \quad (3)$$

$$G = \{id_I, (12), (34), (12)(34)\}, \quad G_W = \{id_I, (12)\}, \quad G_M = \{id_I, (34)\}.$$

Given $p \in \mathcal{P}$ and $\varphi \in G^*$, taking into account (1), we denote by p^φ the preference profile defined, for every $z \in I$, by

$$p^\varphi(z) := \varphi p(\varphi^{-1}(z)). \quad (4)$$

By Lemma 1, it is easily checked that p^φ actually belongs to $\mathcal{P}$. Moreover, (4) is equivalent to stating that, for every $z \in I$,

$$p^\varphi(\varphi(z)) = \varphi p(z), \quad (5)$$

which is more intuitive than (4). Indeed, consider $\varphi \in G^*$ and $p \in \mathcal{P}$ represented by the table

1	...	n	n+1	...	2n
p(1)	...	p(n)	p(n+1)	...	p(2n)

Then, by (5), we deduce that p^φ is represented by the table

$\varphi(1)$	...	$\varphi(n)$	$\varphi(n+1)$	...	$\varphi(2n)$
$\varphi p(1)$	...	$\varphi p(n)$	$\varphi p(n+1)$	...	$\varphi p(2n)$

For a concrete example, consider the preference profile p represented by the table in (2). If $\varphi = (1426)(35) \in G^*$, then

$$p^\varphi = \begin{array}{|c|c|c|} \hline 4 & 6 & 5 \\ \hline 2 & 2 & 1 \\ \hline 3 & 1 & 3 \\ \hline 1 & 3 & 2 \\ \hline \end{array} \begin{array}{|c|c|c|} \hline 2 & 3 & 1 \\ \hline 6 & 5 & 5 \\ \hline 4 & 4 & 6 \\ \hline 5 & 6 & 4 \\ \hline \end{array} = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 5 & 6 & 5 \\ \hline 6 & 4 & 4 \\ \hline 4 & 5 & 6 \\ \hline \end{array} \begin{array}{|c|c|c|} \hline 4 & 5 & 6 \\ \hline 2 & 1 & 2 \\ \hline 3 & 3 & 1 \\ \hline 1 & 2 & 3 \\ \hline \end{array}.$$

Let us now introduce some basic notions and facts from group theory that will be crucial for defining the concept of symmetry for matching mechanisms. We first define the conjugate of an element of a group. We then define the multiplication of subsets of a group, clarifying some properties that will be useful for our purposes. Finally, we define the conjugate of a subset of a group as a special product of subsets.

Let H be a group. Given $h, k \in H$, the conjugate of k by h is defined as $hkh^{-1} \in H$ and is denoted by k^h . The map from H to H taking each $k \in H$ into k^h is a bijection, called the conjugation by h . As a fundamental example, let $\mu \in \mathcal{M}$ be a matching and $\varphi \in G^*$ be a renaming rule. Since $\mathcal{M} \subseteq G^*$, it follows that $\mu \in G^*$, and thus we can consider $\mu^\varphi = \varphi\mu\varphi^{-1} \in G^*$. Notably, μ^φ actually belongs to $\mathcal{M}$ and corresponds to the matching obtained from μ by renaming individuals according to φ . Consider, for instance, $W = \{1, 2, 3\}$, $M = \{4, 5, 6\}$, the matching $\mu = (14)(25)(36) \in \mathcal{M}$ and the renaming rule $\varphi = (1426)(35) \in G^*$. A straightforward computation shows that

$$\mu^\varphi = [(14)(25)(36)]^{(1426)(35)} = (42)(63)(51) \in \mathcal{M},$$

which is the matching obtained by $(14)(25)(36)$ by renaming the individuals according to $(1426)(35)$. This is a general fact in permutation groups. Indeed, if a permutation σ is a product of the permutations $\sigma_1, \dots, \sigma_r$ and φ is a further permutation, then¹³

$$(\sigma_1 \cdots \sigma_r)^\varphi = \sigma_1^\varphi \cdots \sigma_r^\varphi. \quad (6)$$

¹³ In the language of group theory, we are just expressing the well-known fact that conjugation is a homomorphism.

Moreover, if $\sigma = (x_1 \cdots x_m)$ is a m -cycle, then

$$\sigma^\varphi = (\varphi(x_1) \cdots \varphi(x_m)). \quad (7)$$

In particular, the cycle structure of a permutation, that is, the number of its fixed points and the number of cycles in which it splits and their lengths, is invariant by conjugation. For further details on the computation of conjugates in symmetric groups, see Example 4.29 and Chapter 4 in Milne (2021).

Given $S, T \subseteq H$, their multiplication is defined as $ST := \{st \in H : s \in S, t \in T\}$. If $S = \{s\}$, we write sT instead of $\{s\}T$; if $T = \{t\}$, we write St instead of $S\{t\}$. From the associativity of the operation in H , we immediately deduce that, for every $S, T, U \subseteq H$, we have $S(TU) = (ST)U$. Thus, brackets are not necessary to deal with multiplications of three or more subsets of a group. Note that if $S \subseteq T \subseteq H$ and $U \subseteq H$, then $US \subseteq UT$ and $SU \subseteq TU$. Given $K \subseteq H$ and $h \in H$, the conjugate of K by h is defined as $hKh^{-1} = \{k^h \in H : k \in K\}$ and is denoted by K^h . Note that, for every $k, h_1, h_2 \in H$ and $K \subseteq H$, we have

$$(k^{h_1})^{h_2} = k^{h_2 h_1} \quad \text{and} \quad (K^{h_1})^{h_2} = K^{h_2 h_1}. \quad (8)$$

Finally, given $k_1, k_2 \in H$ [$K_1, K_2 \subseteq H$], we say that k_1 and k_2 [K_1 and K_2] are conjugate if there exists $h \in H$ such that $k_2 = k_1^h$ [$K_2 = K_1^h$].

We are now ready to provide the definition of symmetry for a matching mechanism. As can be noticed, it involves the conjugate of a subset of $\mathcal{M}$ by an element of G^* .

Definition 5. Let F be a matching mechanism and $U \subseteq G^*$. We say that F is U -symmetric if, for every $p \in \mathcal{P}$ and $\varphi \in U$, $F(p^\varphi) = F(p)^\varphi$.

In order to describe the intuition behind the definition, assume that $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$ and consider $U \subseteq G^*$ and a U -symmetric matching mechanism F . Assume that $\varphi = (1426)(35) \in U$ and that

$$F(p) = \{(14)(25)(36), (15)(26)(34)\}.$$

Then, by Definition 5, and using (6) and (7), we get

$$\begin{aligned} F(p^\varphi) &= F(p)^\varphi = \{[(14)(25)(36)]^\varphi, [(15)(26)(34)]^\varphi\} \\ &= \{(42)(63)(51), (43)(61)(52)\}. \end{aligned}$$

The above example clearly shows that, if F is U -symmetric, a change in individuals' names in the input according to a permutation in U entails the same change of names in the matchings of the output. This means that the notion of U -symmetry models a notion of fairness, which may assume various shapes depending on the choice of U . For instance, if F is G_W -symmetric, then women are equally treated among themselves by F ; if F is G_M -symmetric, then men are equally treated among themselves by F ; if F is G -symmetric, then women are equally treated among themselves and men are equally treated among themselves by F ; if F is G^* -symmetric, then women are equally treated among themselves, men are equally treated among themselves, and the two groups of women and men are equally treated by F .

Definition 5 provides a generalization of several properties analyzed in the literature on matching mechanisms. Indeed, the standard concept of anonymity, called peer indifference by Masarani and Gokturk (1989), coincides with G -symmetry; the property of gender indifference introduced by Masarani and Gokturk (1989) coincides with $\{\varphi\}$ -symmetry, where φ is a suitable element of $\mathcal{M}$ (see also Endriss, 2020); the property of gender fairness by Özkal-Sanver (2004) coincides with $(G^* \setminus G)$ -symmetry. Of course, a matching mechanism F satisfies both peer indifference and gender indifference if and only if F is $(G \cup \{\varphi\})$ -symmetric.

4. Research problem and main results

This section is divided into three parts. We first illustrate and motivate our research problem; then, we present an existence condition which is fundamental for proving the possibility and impossibility theorems that represent the main results of our paper; in the last part of the section we collect those results.

4.1. The research problem

Proving or disproving the existence of resolute and symmetric matching mechanisms, possibly satisfying further properties, is certainly an interesting and not trivial problem. Since a resolute and symmetric matching mechanism can be seen as a resolute and symmetric refinement of TO (that is, the matching mechanism that associates with any preference profile the whole set $\mathcal{M}$ of matchings), and since many properties of matching mechanisms can be described using the concept of refinement (e.g. stability, Pareto optimality, weak Pareto optimality, minimal optimality), the aforementioned existence problem can be fruitfully specialized in the following existence problem.

Main Problem. Let $U \subseteq G^*$ and F be a matching mechanism. Find conditions on U and F that guarantee the existence of a resolute refinement of F that is U -symmetric.

Unfortunately, a strong tension emerges among resoluteness, G^* -symmetry, and optimality requirements. Indeed, GS_w and GS_m are resolute and G -symmetric but fail to be G^* -symmetric; on the other hand, GS , ST , PO , WPO , MO and TO are G^* -symmetric but not resolute (see Proposition 9 in Appendix B.2 for the proof of the symmetry properties of the aforementioned matching mechanisms).

Several stable matching mechanisms have been introduced in the literature with the aim to guarantee more fairness between the two sets W and M than the one obtained by GS_w and GS_m . The Sex-Equal mechanism, introduced by Gusfield and Irving (1989) and analyzed in Romero-Medina (2001), and the Egalitarian Stable mechanism, introduced in Gusfield and Irving (1989), are two of them. Roughly speaking, both of them are based on the idea to quantify first, for every stable matching, the envy perceived by every individual and then consider the stable matchings minimizing a suitable function involving the level of envy of all the individuals. Given a preference profile p , a matching μ and $z \in I$, we have that the number $\text{Rank}_{p(z)}(\mu(z)) - 1$ counts the number of individuals envied by z under the matching μ . Indeed, consider, for instance, $x \in W$. Then x envies the partners of all the men $y \in M$ such that $y \succ_{p(x)} \mu(x)$ and their number is exactly $\text{Rank}_{p(x)}(\mu(x)) - 1$. For every $p \in \mathcal{P}$ and $\mu \in \mathcal{M}$, we can consider then the quantities

$$\delta(p, \mu) := \left| \sum_{x \in W} \text{Rank}_{p(x)}(\mu(x)) - \sum_{y \in M} \text{Rank}_{p(y)}(\mu(y)) \right|,$$

and

$$e(p, \mu) := \sum_{x \in W} \text{Rank}_{p(x)}(\mu(x)) + \sum_{y \in M} \text{Rank}_{p(y)}(\mu(y)).$$

Since

$$\sum_{x \in W} \text{Rank}_{p(x)}(\mu(x)) \quad \text{and} \quad \sum_{y \in M} \text{Rank}_{p(y)}(\mu(y))$$

basically represent the aggregate level of envy of the men and the aggregate level of envy of the women, we have that $\delta(\mu, p)$ measures the distance between these two values while $e(\mu, p)$ measures the overall level of envy in the society. The Sex-Equal matching mechanism, denoted by SE , is the matching mechanism defined, for every $p \in \mathcal{P}$, by

$$SE(p) := \arg \min_{\mu \in ST(p)} \delta(p, \mu);$$

the Egalitarian Stable matching mechanism, denoted by ES , is the matching mechanism defined, for every $p \in \mathcal{P}$, by

$$ES(p) := \arg \min_{\mu \in ST(p)} e(p, \mu).$$

Of course, SE and ES are decisive and stable. Moreover, they are also G^* -symmetric, as proved in Proposition 10 in Appendix B.2. However, by Example 1 in Romero-Medina (2001, page 201), they are not resolute.

4.2. A preliminary existence condition

Here, we present a general existence result for U -symmetric resolute refinements of U -symmetric matching mechanisms (Proposition 4). Some preliminary notions and results are needed to state such a theorem. They are illustrated in what follows.

Let H be a finite group and $K \subseteq H$. The subgroup of H generated by K , denoted by $\langle K \rangle$, is the intersection of all the subgroups of H containing K . For instance, $\langle \emptyset \rangle = \{1\}$. If $h \in H$, we write $\langle h \rangle$ instead of $\langle \{h\} \rangle$. Of course, if $K \leq H$, then $\langle K \rangle = K$. It is well known that, since H is finite, when $K \neq \emptyset$, $\langle K \rangle$ is the set made up of all the elements of K and the products of a finite number of elements in K . For further details, see Chapter 1 in Milne (2021).

As a first result, we show that dealing with symmetry for subsets of G^* is equivalent to dealing with symmetry for subgroups of G^* . The proof of Proposition 2 is in Appendix B.2.

Proposition 2. Let F be a matching mechanism and $U \subseteq G^*$. Then F is U -symmetric if and only if F is $\langle U \rangle$ -symmetric.

Proposition 2 is remarkable and emblematic of the role that group theory may play in the context of matching theory. In fact, it points out that whenever one focuses on the symmetry with respect to a set of permutations, it inevitably ends up with considering the symmetry with respect to a subgroup of permutations. As a consequence, while considering various levels of symmetry, we are allowed to restrict our attention to subgroups of G^* only. As a further consequence, since $\langle G^* \setminus G \rangle = \langle G \cup \{\varphi\} \rangle = G^*$ (see Proposition 8 in Appendix B.2), we immediately deduce the following result.

Corollary 1. G^* -symmetry, gender fairness, and the combination of peer indifference and gender indifference are equivalent.

We emphasize that, to the best of our knowledge, the fact that requiring gender fairness is the same as requiring both peer indifference and gender indifference does not seem to be present in the literature.

Let us introduce another concept that will turn out very important for our research.

Definition 6. Let $U \leq G^*$ and $p \in \mathcal{P}$. The U -stabilizer of p is the set

$$\text{Stab}_U(p) := \{\varphi \in U : p^\varphi = p\}.$$

Remarkably, $\text{Stab}_U(p)$ is a subgroup of U and, for every $\varphi \in U$, we have $\text{Stab}_U(p^\varphi) = [\text{Stab}_U(p)]^\varphi$. Moreover, it is immediately checked that $\text{Stab}_U(p) = \text{Stab}_{G^*}(p) \cap U$. That explains, in particular, the central role of the G^* -stabilizers. Indeed, the knowledge of the G^* -stabilizer of a preference profile allows to know its U -stabilizer for all $U \leq G^*$.

As an easy example, let $W = \{1, 2\}$, $M = \{3, 4\}$ and p be the preference profile represented by the table

$$p = \begin{array}{cc|cc} 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 3 & 1 & 2 \end{array}. \quad (9)$$

Using (3), it turns out that $\text{Stab}_{G^*}(p) = \{id_I, (1324), (12)(34), (1423)\}$. As a consequence, if $U := \{id_I, (12)(34)\}$, we find $\text{Stab}_U(p) = \{id_I, (12)(34)\}$; if instead $U := \{id_I, (12)\}$, we find $\text{Stab}_U(p) = \{id_I\}$.

In the next definition we introduce, for every $U \leq G^*$, a matching mechanism denoted by C^U . Such a mechanism plays a crucial role to address the aforementioned Main Problem, as shown by all the subsequent results of the section, especially by Proposition 4.

Definition 7. Let $U \leq G^*$. We denote by C^U the matching mechanism defined, for every $p \in \mathcal{P}$, by

$$C^U(p) := \{\mu \in \mathcal{M} : \forall \varphi \in \text{Stab}_U(p), \mu^\varphi = \mu\}.$$

The letter C intentionally resembles the word centralizer, which is widely used by group theorists. Let H be a group and $K \leq H$. The centralizer of K in H is defined by

$$C_H(K) := \{h \in H : \forall k \in K, kh = hk\}.$$

It is well known that $C_H(K)$ is a subgroup of H and that, for every $h \in H$, $C_H(K^h) = [C_H(K)]^h$.

It is then clear that, given $U \leq G^*$ and $p \in \mathcal{P}$,

$$C^U(p) = \{\mu \in \mathcal{M} : \forall \varphi \in \text{Stab}_U(p), \varphi\mu = \mu\varphi\} = C_{G^*}(\text{Stab}_U(p)) \cap \mathcal{M}. \quad (10)$$

The next proposition, whose proof is in [Appendix B.2](#), illustrates the properties of C^U . Its purpose is, on the one hand, to provide a better understanding of the new concept and, on the other hand, to convey a more vivid intuition of it.

Proposition 3. *Let $U \leq G^*$. Then the following facts hold true:*

- (i) C^U is U -symmetric;
- (ii) if F is a resolute and U -symmetric matching mechanism, then F is a refinement of C^U .

By [Proposition 3](#), it turns out that C^U is the natural container for all the resolute and U -symmetric matching mechanisms.

We are now ready to state the main result of the section. Its proof is in [Appendix B.3](#).

Proposition 4. *Let $U \leq G^*$ and F be a U -symmetric matching mechanism. Then, F admits a U -symmetric and resolute refinement if and only if, for every $p \in \mathcal{P}$, $F(p) \cap C^U(p) \neq \emptyset$.*

It is worth noting that considering $F = TO$ in [Proposition 4](#) immediately leads to the following corollary.

Corollary 2. *Let $U \leq G^*$. Then, there exists a resolute and U -symmetric matching mechanism if and only if C^U is decisive.*

Unfortunately, C^U may fail to be decisive for some values of the market size and for some subgroups U of G^* . Assume, for instance, $W = \{1, 2\}$, $M = \{3, 4\}$, and $U = G^*$. If p is the preference profile in [\(9\)](#), we know that $\text{Stab}_{G^*}(p) = \{id_I, (1324), (12)(34), (1423)\}$. Using [\(3\)](#), a direct computation shows that $C_{G^*}(\text{Stab}_{G^*}(p)) = \text{Stab}_{G^*}(p)$. As a consequence, we have $C^{G^*}(p) = C_{G^*}(\text{Stab}_{G^*}(p)) \cap \mathcal{M} = \text{Stab}_{G^*}(p) \cap \mathcal{M} = \emptyset$.

4.3. Possibility and impossibility results

We are now ready to state the possibility and impossibility results proved in the paper. The proofs of the results collected in this section are in [Appendix D](#). [Theorem 1](#) is about G^* -symmetry and is the main result of the paper. We stress that its proof relies on several results and facts from group theory, some of them definitely non-trivial. Recall that the market size is given by $|W| = |M| = n \geq 2$.

Theorem 1. *There exists a resolute and G^* -symmetric matching mechanism if and only if the market size is odd.*

Given [Theorem 1](#), one may wonder whether it is possible, for the case n odd, to ask for some further property, like minimal optimality, and still get the existence. The next result shows that the answer is negative.

Proposition 5. *If the market size is odd, then there exists no resolute, G^* -symmetric and minimally optimal matching mechanism.*

Taking into account [Theorem 1](#) and [Proposition 5](#), we then get the following general impossibility result.

Theorem 2. *For every market size, there exists no resolute, G^* -symmetric and minimally optimal matching mechanism.*

Of course, as a consequence of the previous theorem and [Proposition 1](#), we also deduce that there exists no resolute, G^* -symmetric and stable [Pareto optimal; weakly Pareto optimal] matching mechanism.

Now we move our focus on the weaker notion of $\{\varphi\}$ -symmetry, where $\varphi \in \mathcal{M}$. As established by [Proposition 2](#), $\{\varphi\}$ -symmetry is equivalent to $\langle \varphi \rangle$ -symmetry and we adopt the latter writing from now on. Clearly, φ exchanges individuals' identities across W and M . Since $\langle \varphi \rangle$ is a subgroup of G^* of order 2, the only smaller subgroup of $\langle \varphi \rangle$ is given by the trivial group $\{id_I\}$. Thus there exists no proper subgroup of $\langle \varphi \rangle$ containing permutations exchanging individuals' identities across W and M . As a consequence, $\langle \varphi \rangle$ -symmetry represents a minimal level of symmetry among those that allow for an exchange of individuals' identities across W and M .

The first result we propose is a possibility result.

Theorem 3. *For every market size and every $\varphi \in \mathcal{M}$, there exists a resolute, $\langle \varphi \rangle$ -symmetric and weakly Pareto optimal matching mechanism.*

Given [Theorem 3](#), one may wonder whether it is possible to replace the assumption of weak Pareto optimality with the stronger property of stability and still get existence. The next two results show that this can actually be done if and only if $n = 2$. Note that [Theorem 5](#) corresponds to [Theorem 6](#) in [Endriss \(2020\)](#).¹⁴ The proof in Endriss is based both on first-order logic and on Satisfiability (SAT) solving techniques. In fact, it is first shown that some properties of matching mechanisms, including stability and $\langle \varphi \rangle$ -symmetry, can be encoded in a specific formal language. Then, it is proved that impossibility results involving these properties can be reduced to impossibility results for the case with three women and three men and that the analysis of this latter case can be fully automated using SAT solving technology. Here, we propose an alternative proof of that impossibility result.

Theorem 4. *If the market size is 2, then, for every $\varphi \in \mathcal{M}$, there exists a resolute, $\langle \varphi \rangle$ -symmetric and stable matching mechanism.*

Theorem 5 ([Endriss, 2020](#)). *If the market size is at least 3, then, for every $\varphi \in \mathcal{M}$, there exists no resolute, $\langle \varphi \rangle$ -symmetric and stable matching mechanism.*

Of course, in light of [Theorem 3](#), one may also wonder whether there are resolute, $\langle \varphi \rangle$ -symmetric and Pareto optimal matching mechanisms. While, by [Theorem 4](#), we get existence if $n = 2$, when $n \geq 3$ the problem is still open.

5. A generalization: the model with outside option

The model studied in this paper considers those situations where individuals are not allowed to stay alone, but are always forced to be matched to another individual. The model where the outside option of being unmatched is given to individuals is important and well studied in the literature. In this section, after recalling how preference profiles, matching and matching mechanisms are defined in the model with outside option, we introduce a concept of symmetry analogous to the one in [Definition 5](#). Then, we propose an impossibility result.

A generalized preference profile is a function $\bar{p}$ from I to the set

$$\left(\bigcup_{x \in W} \mathbf{L}(M \cup \{x\}) \right) \cup \left(\bigcup_{y \in M} \mathbf{L}(W \cup \{y\}) \right)$$

such that, for every $x \in W$, $\bar{p}(x) \in \mathbf{L}(M \cup \{x\})$ and, for every $y \in M$, $\bar{p}(y) \in \mathbf{L}(W \cup \{y\})$. The set of generalized preference profiles is denoted by $\bar{\mathcal{P}}$. We represent a generalized preference profile $\bar{p} \in \bar{\mathcal{P}}$ by the table

1	...	n	$n+1$	...	$2n$
$\bar{p}(1)$	...	$\bar{p}(n)$	$\bar{p}(n+1)$	...	$\bar{p}(2n)$

¹⁴ Observe also that [Theorem 5](#) implies [Theorem 3](#) in [Root and Bade \(2023\)](#).

where in the first row there are the names of individuals and in the second row the corresponding preferences. For instance, if $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$, the table

1	2	3	4	5	6
4	4	6	2	3	6
1	6	5	1	5	2
6	2	3	3	2	1
5	5	4	4	1	3

(11)

represents the preference profile $\bar{p}$ such that

$$\bar{p}(1) = [4, 1, 6, 5] \in \mathbf{L}(M \cup \{1\}), \bar{p}(2) = [4, 6, 2, 5] \in \mathbf{L}(M \cup \{2\}),$$

$$\bar{p}(3) = [6, 5, 3, 4] \in \mathbf{L}(M \cup \{3\}),$$

$$\bar{p}(4) = [2, 1, 3, 4] \in \mathbf{L}(W \cup \{4\}), \bar{p}(5) = [3, 5, 2, 1] \in \mathbf{L}(W \cup \{5\}),$$

$$\bar{p}(6) = [6, 2, 1, 3] \in \mathbf{L}(W \cup \{6\}).$$

Given $\bar{p} \in \bar{\mathcal{P}}$ and $\varphi \in G^*$, taking into account the definition (1), we denote by $\bar{p}^\varphi$ the generalized preference profile defined, for every $z \in I$, by $\bar{p}^\varphi(z) := \varphi \bar{p}(\varphi^{-1}(z))$. Using Lemma 1, it is easily checked that $\bar{p}^\varphi$ actually belongs to $\bar{\mathcal{P}}$. Similarly to what said for preference profiles in Section 3.4, if $\varphi \in G^*$ and $\bar{p} \in \bar{\mathcal{P}}$ is represented by the table

1	...	n	n+1	...	2n
$\bar{p}(1)$	...	$\bar{p}(n)$	$\bar{p}(n+1)$	...	$\bar{p}(2n)$

then $\bar{p}^\varphi$ is represented by the table

$\varphi(1)$	...	$\varphi(n)$	$\varphi(n+1)$	...	$\varphi(2n)$
$\varphi \bar{p}(1)$	...	$\varphi \bar{p}(n)$	$\varphi \bar{p}(n+1)$	...	$\varphi \bar{p}(2n)$

Thus, $\bar{p}^\varphi$ is obtained by $\bar{p}$ as if all individual identities were changed according to φ . For a concrete example, consider the generalized preference profile $\bar{p}$ represented by the table in (11). If $\varphi = (1426)(35) \in G^*$, then

$$\bar{p}^\varphi = \begin{array}{|c|c|c|c|c|c|} \hline 4 & 6 & 5 & 2 & 3 & 1 \\ \hline 2 & 2 & 1 & 6 & 5 & 1 \\ \hline 4 & 1 & 3 & 4 & 3 & 6 \\ \hline 1 & 6 & 5 & 5 & 6 & 4 \\ \hline 3 & 3 & 2 & 2 & 4 & 5 \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 6 & 5 & 2 & 1 & 2 \\ \hline 6 & 4 & 3 & 4 & 3 & 1 \\ \hline 4 & 5 & 6 & 1 & 5 & 6 \\ \hline 5 & 2 & 4 & 3 & 2 & 3 \\ \hline \end{array}.$$

A generalized matching is a permutation $\bar{\mu} \in \text{Sym}(I)$ such that, for every $x \in W$, if $\bar{\mu}(x) \neq x$, then $\bar{\mu}(x) \in M$; for every $y \in M$, if $\bar{\mu}(y) \neq y$, then $\bar{\mu}(y) \in W$; for every $z \in I$, $\bar{\mu}(\bar{\mu}(z)) = z$. The set of generalized matchings is denoted by $\bar{\mathcal{M}}$. For instance, if $W = \{1, 2\}$ and $M = \{3, 4\}$, then

$$\bar{\mathcal{M}} = \{id_I, (13), (14), (23), (24), (13)(24), (14)(23)\}.$$

Recalling (6) and (7), it is clear that, for every $\bar{\mu} \in \bar{\mathcal{M}}$ and $\varphi \in G^*$, we have $\bar{\mu}^\varphi \in \bar{\mathcal{M}}$. Note also that, $\bar{\mu}^\varphi$ is obtained by $\bar{\mu}$ as if all individual identities were changed according to φ . As an example, assume $W = \{1, 2, 3\}$ and $M = \{4, 5, 6\}$ and consider $\bar{\mu} = (15)(26) \in \bar{\mathcal{M}}$ and $\varphi = (1426)(35) \in G^*$. Then $\bar{\mu}^\varphi = (43)(61)$.

Given $\bar{p} \in \bar{\mathcal{P}}$ and $\bar{\mu} \in \bar{\mathcal{M}}$, we say that $\bar{\mu}$ is stable for $\bar{p}$ if there is no $z \in I$ such that $z \succ_{\bar{p}(z)} \bar{\mu}(z)$ and there is no $(x, y) \in W \times M$ such that $y \succ_{\bar{p}(x)} \bar{\mu}(x)$ and $x \succ_{\bar{p}(y)} \bar{\mu}(y)$; Pareto optimal for $\bar{p}$ if there is no $\bar{\mu}' \in \bar{\mathcal{M}}$ such that, for every $z \in I$, $\bar{\mu}'(z) \succeq_{\bar{p}(z)} \bar{\mu}(z)$ and there exists $z^* \in I$ such that $\bar{\mu}'(z^*) \succ_{\bar{p}(z^*)} \bar{\mu}(z^*)$. It can be easily shown that if $\bar{\mu}$ is stable for $\bar{p}$, then it is Pareto optimal for $\bar{p}$.

A (two-sided) generalized matching mechanism is a correspondence from $\bar{\mathcal{P}}$ to $\bar{\mathcal{M}}$. Given a generalized matching mechanism F , we say that F is decisive if, for every $\bar{p} \in \bar{\mathcal{P}}$, $F(\bar{p}) \neq \emptyset$; resolute if, for every $\bar{p} \in \bar{\mathcal{P}}$, $|F(\bar{p})| = 1$; stable if, for every $\bar{p} \in \bar{\mathcal{P}}$, all the elements of $F(\bar{p})$ are stable for $\bar{p}$; Pareto optimal if, for every $\bar{p} \in \bar{\mathcal{P}}$, all the elements of $F(\bar{p})$ are Pareto optimal for $\bar{p}$; U -symmetric, where $U \subseteq G^*$, if, for every $\bar{p} \in \bar{\mathcal{P}}$ and $\varphi \in U$, $F(\bar{p}^\varphi) = F(\bar{p})^\varphi$.

We stress that, even in the considered framework, the properties of G -symmetry (anonymity) and $(G^* \setminus G)$ -symmetry (gender-fairness) are employed by some authors, specifically to obtain characterization results (see, for instance, Theorem 2 in Miyagawa, 2002, and Theorem 3.1 in Nizamogullari and Özkal-Sanver, 2014). It is also worth noting that, using the same argument as in the proof of Proposition 2, we can deduce that, for every $U \subseteq G^*$, a generalized matching mechanism is U -symmetric if and only if it is $\langle U \rangle$ -symmetric. Therefore, by Proposition 8, $(G^* \setminus G)$ -symmetry is equivalent to G^* -symmetry.

As a consequence of Theorem 2, we are able to prove the following impossibility result, whose proof is in Appendix D.

Theorem 6. For every market size, there exists no resolute, G^* -symmetric and Pareto optimal generalized matching mechanism.

Of course, Theorem 6 implies that there exists no resolute, G^* -symmetric and stable generalized matching mechanism. On the other hand, the existence of a resolute and G^* -symmetric generalized matching mechanism remains an open problem.

6. Conclusions and future research

In this paper, we focused on balanced markets and proved several possibility and impossibility results for matching mechanisms satisfying resoluteness, a given level of symmetry, (i.e. G^* -symmetry or $\langle \varphi \rangle$ -symmetry), and possibly other desirable properties (i.e. stability, Pareto optimality, weak Pareto optimality and minimal optimality). The main result of the paper (Theorem 1) states that resoluteness and G^* -symmetry are consistent with each other if and only if the size of the market is odd. Moreover, we prove that resoluteness and G^* -symmetry are inconsistent with minimal optimality, definitely a very weak condition (Theorem 2); there exist resolute and $\langle \varphi \rangle$ -symmetric matching mechanisms that are weak Pareto optimal but none of them can be stable, unless the size of the market is 2 (Theorems 3, 4, 5). Roughly, the conclusions that we can draw from these results could be recap as follows: when we restrict attention to resolute matching mechanisms, the highest level of symmetry, that is G^* -symmetry, is incompatible with any sort of optimality condition while weaker symmetry conditions, still involving a comparison between the two groups of agents, are incompatible with strong optimality conditions, like stability, but may be consistent with other interesting optimality conditions, like weak Pareto optimality.

These results are obtained by employing suitable algebraic methods based on group theory, an approach strongly innovative and not yet explored in matching theory. Our paper demonstrates that such an approach is fruitful and able to provide novel and remarkable insight into issues that pertain to fairness.

All these findings constitute a first step in the direction of a complete understanding of the Main Problem described in Section 4.1. Several other areas deserve attention for future research.

First, one could focus on other forms of fairness which are intermediate between G^* -symmetry and $\langle \varphi \rangle$ -symmetry and economically sound, as well. The purpose is to get, in particular, positive results for these intermediate forms of symmetry when the size of the market is even. As an example, in a framework where it is natural to identify a partition $\{W_1, W_2\}$ of W and a partition $\{M_1, M_2\}$ of M that are economically meaningful and such that $|W_1| = |M_1|$ and $|W_2| = |M_2|$, it could be reasonable to focus on U -symmetry, where

$$U = \{\varphi \in G^* : \varphi(W_1) = W_1 \text{ or } \varphi(W_1) = M_1\}.$$

In other words, one can focus on changes in individual identities within the four sets W_1 , W_2 , M_1 and M_2 , as well as those across W_1 and M_1 , and across W_2 and M_2 .

Another possible approach for getting possibility results consists in analyzing whether it is possible to identify suitable preference domain

restrictions that guarantee the existence of resolute matching mechanisms satisfying strong optimality conditions, such as stability, while maintaining a sufficiently high level of symmetry.

Finally, one could ask whether our notion of U -symmetry and the possibility and impossibility results provided in our paper can be extended to unbalanced markets, namely where the two sets W and M have different sizes (and where, of course, individuals have the outside option to be unmatched). However, we believe that symmetries involving permutations that change individuals' identities across W and M do not make sense in such a framework since W and M are substantially different because of their different sizes. On the other hand, symmetries involving only permutations that change individuals' identities within the two groups (that is, weaker forms of anonymity) may be considered, and it seems reasonable to conjecture that any matching mechanism satisfying a symmetry condition of that type admits a resolute refinement satisfying the same level of symmetry.

CRedit authorship contribution statement

Daniela Bubboloni: Writing – review & editing, Writing – original draft, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Michele Gori:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Claudia Meo:** Writing – review & editing, Writing – original draft, Investigation, Funding acquisition, Formal analysis, Conceptualization.

Declaration of competing interest

We have no competing interests to declare that are relevant to the content of this article.

Acknowledgments

The authors thank an associate editor and two reviewers for their valuable comments, which contributed to improving the paper. The authors also express their gratitude to Pablo Spiga for inspiring discussions and suggestions about centralizers of semiregular subgroups. Finally, the authors thank the members of the CRESE research center in Besançon, the LAMSADE research center in Paris, and the Corvinus University of Budapest, as well as the participants of the 2024 Amsterdam/Saint-Étienne Workshop on Social Choice and the XLVIII AMASES Conference, for their insightful comments. Daniela Bubboloni has been supported by GNSAGA of INdAM (Italy), by the European Union - Next Generation EU, Missione 4 Componente 1, PRIN 2022-2022PSTWLB-Group Theory and Applications, CUP B53D23009410006, and by local funding from the Università degli Studi di Firenze. Michele Gori has been supported by local funding from the Università degli Studi di Firenze. Claudia Meo has been supported by the national project PRIN 2022-2022HPLPMKN-Externalities and Fairness in Allocations and Contracts, CUP E53D23006290006.

Appendix A. Optimality conditions

Let us introduce some notation that will be used in the proof of [Proposition 1](#) and also in the sequel. Let $m \in \mathbb{N}$. Given $x \in \mathbb{Z}$, we denote the equivalence class of x modulo m by $[x]_m := \{x + km : k \in \mathbb{Z}\}$. Note that, for every $x \in \mathbb{Z}$, $[x]_m \cap [m]$ is a singleton whose unique element can be taken as a canonical representative for the set $[x]_m$.

Proof of Proposition 1. (i) Let μ be stable for p . Assume by contradiction that μ is not Pareto optimal for p . Then, there exists $\mu' \in \mathcal{M}$ such that, for every $z \in I$, $\mu'(z) \succeq_{p(z)} \mu(z)$ and there exists $z^* \in I$ such that $\mu'(z^*) \succ_{p(z^*)} \mu(z^*)$. Consider then z^* and set $z' = \mu'(z^*)$. Then we have $z' = \mu'(z^*) \succ_{p(z^*)} \mu(z^*)$ and $z^* = \mu'(z') \succeq_{p(z')} \mu(z')$. Note that $z^* \neq \mu(z')$. Indeed, assume the contrary. Then $z' = \mu(z^*)$ and thus $z' \succ_{p(z^*)} z'$, a

contradiction. As a consequence, we have $z^* = \mu'(z') \succ_{p(z')} \mu(z')$ and hence the pair (z^*, z') blocks μ according to p . Thus, μ is not stable, a contradiction.

(ii) Trivial.

(iii) Let μ be weakly Pareto optimal for p . As already observed, there exists at most one matching that is not minimally optimal for p . If there is none, then μ is minimally optimal for p . Assume instead that there exists $\mu^* \in \mathcal{M}$ that is not minimally optimal for p . Thus, for every $z \in I$, $\text{Rank}_{p(z)}(\mu^*(z)) = n$. In order to prove that μ is minimally optimal for p , it is enough to show that μ^* is not weakly Pareto optimal for p . Let $\mu' \in \mathcal{M}$ be the unique matching such that, for every $y \in M$, $\mu'(y)$ is the unique woman in the set $[\mu^*(y) + 1]_n$. Observe that, since $n \geq 2$, for every $z \in I$, we have $\mu'(z) \neq \mu^*(z)$ and therefore $\text{Rank}_{p(z)}(\mu'(z)) < n$. As a consequence, for every $z \in I$, $\mu'(z) \succ_{p(z)} \mu^*(z)$. Thus, μ^* is not weakly Pareto optimal for p . $\square$

Appendix B. Group theory in our setup

B.1. Basic results of group theory and two actions

We start with some additional basic notions from group theory.¹⁵ Let H be a finite group. Lagrange Theorem states that the size of a subgroup of H divides the size of H (see Theorem 1.26 in [Milne, 2021](#)). Given $h \in H$, the order of h is defined by $|h| := |\langle h \rangle|$ and we have that: $\langle h \rangle = \{h^j : j \in \mathbb{N}\}$; $|h|$ is the minimum $j \in \mathbb{N}$ such that $h^j = 1$; given $b \in \mathbb{N}$, $h^b = 1$ if and only if $|h|$ divides b ; by Lagrange Theorem, $|h|$ divides $|H|$.¹⁶ We say that H is cyclic if there exists $h \in H$ such that $H = \langle h \rangle$. Cauchy Theorem partially reverses Lagrange Theorem ensuring that if r is a prime dividing $|H|$, then there exists in H an element of order r (see Theorem 4.13 in [Milne, 2021](#)).

Let K be a finite group. A homomorphism from H to K is a function $f : H \rightarrow K$ such that, for every $h_1, h_2 \in H$, $f(h_1 h_2) = f(h_1) f(h_2)$, where the operations are denoted by juxtaposition in both groups. A homomorphism f from H to K is called an isomorphism if it is bijective. For instance, if $K \leq H$ and $h \in H$, the conjugation by h is an isomorphism from K to the subgroup K^h of H . The groups H and K are called isomorphic if there exists an isomorphism between them. In such a case, we write $H \cong K$. It is easy to check that two cyclic groups of the same size $m \in \mathbb{N}$ are isomorphic. As a consequence, up to isomorphism, there is a unique cyclic group of order m , denoted by C_m .

Given $K \leq H$, we say that K is a normal subgroup of H if, for every $h \in H$, $K^h = K$ (see Chapter 1 in [Milne, 2021](#)). As an application of this notion to subgroups of G^* , we show that G is a normal subgroup of G^* . Indeed, let $\sigma \in G$ and $\varphi \in G^*$. Since all the cycles in which σ splits have support included in either W or M , it follows from (6) and (7) that the same holds for σ^φ . As a consequence, we have $\sigma^\varphi \in G$, and since conjugation by φ is a bijection, we obtain $G^\varphi = G$.

We next introduce the concept of action. Let X be a nonempty finite set. An action of H on X is a homomorphism f from H to $\text{Sym}(X)$. Assume that H acts on X through the action f . For every $h \in H$ and $x \in X$, we usually write x^h instead of $f(h)(x)$. In particular, the action f is not explicitly mentioned in the notation, although it must always be carefully specified. In this paper, we will focus mainly on actions on the set I of individuals and on the set $\mathcal{P}$ of preference profiles. Given $x \in X$, the H -orbit of x is the set $x^H := \{x^h \in X : h \in H\}$; the H -stabilizer

¹⁵ We are interested to apply those notions to suitable subgroups of G^* , e.g., G^* , G , $\langle \mu \rangle$ with $\mu \in \mathcal{M}$, and the stabilizers of two special actions defined later in this section.

¹⁶ For instance, if μ is a matching, then we know that $\mu \in G^*$ and so $|\mu| = 2$ divides $|G^*|$.

of x is the subgroup of H defined by $\text{Stab}_H(x) := \{h \in H : x^h = x\}$. A well-known result states that, for every $x \in X$,

$$|x^H| = \frac{|H|}{|\text{Stab}_H(x)|},$$

and so, in particular, $|x^H|$ divides $|H|$ (see Chapter 4 in Milne, 2021). The set $X^H := \{x^H \subseteq X : x \in X\}$ is a partition¹⁷ of X called the set of the H -orbits of X or, alternatively, the set of orbits of H on X . Reference to X can be omitted when it is clear from the context.

We now discuss the first action that plays a role in our paper: the so-called natural action. Given $H \leq \text{Sym}(X)$, the natural action f of H on X is defined, for every $\varphi \in H$, by $f(\varphi) = \varphi$. Thus, with respect to this action, for every $x \in X$, we simply have $f(\varphi)(x) = x^\varphi = \varphi(x)$, $x^H = \{\varphi(x) \in X : \varphi \in H\}$ and $\text{Stab}_H(x) = \{\varphi \in H : \varphi(x) = x\}$. We emphasize that, in this paper, this kind of action is used for $H \leq \text{Sym}(X)$ with X being a subset of I , for instance, I , W , and M .

Let $\varphi \in \text{Sym}(X)$. Since $\langle \varphi \rangle \leq \text{Sym}(X)$, we can consider the natural action of $\langle \varphi \rangle$ on X . Given $x \in X$, we have that $x^{\langle \varphi \rangle} = \{\varphi^j(x) \in X : j \in \mathbb{N}\}$ and $|x^{\langle \varphi \rangle}| = 1$ if and only if x is a fixed point for φ , that is $\varphi(x) = x$. The set of the $\langle \varphi \rangle$ -orbits of X , that is the set $X^{\langle \varphi \rangle} = \{x^{\langle \varphi \rangle} \subseteq X : x \in X\}$, is also called the set of the orbits of φ on X . Let $r = |X^{\langle \varphi \rangle}| \in \mathbb{N}$ be the number of the distinct orbits of φ on X and let $x_1, \dots, x_r \in X$ be such that $X^{\langle \varphi \rangle} = \{x_j^{\langle \varphi \rangle} : j \in \llbracket r \rrbracket\}$. The elements $x_1, \dots, x_r$ are called representatives of the orbits of φ on X . For every $j \in \llbracket r \rrbracket$, set $b_j := |x_j^{\langle \varphi \rangle}|$. The type of φ is defined by the unordered list $T_\varphi := [b_1, \dots, b_r]$, whose elements are called the parts of T_φ . We have that $\sum_{j=1}^r b_j = |X|$ and $|\varphi| = \text{lcm}(b_1, \dots, b_r)$, where lcm denotes the least common multiple. Let $J = \{j \in \llbracket r \rrbracket : b_j \geq 2\}$. If $J = \emptyset$, then $\varphi = \text{id}_X$; if $J \neq \emptyset$, then $\varphi \neq \text{id}_X$ and φ decomposes into the $|J|$ disjoint cycles $\varphi_1, \dots, \varphi_{|J|}$, where, for every $j \in J$, φ_j is the b_j -cycle given by $\varphi_j := (x_j \varphi(x_j) \dots \varphi^{b_j-1}(x_j))$. In particular, for every $j \in \llbracket r \rrbracket$ and $x \in x_j^{\langle \varphi \rangle}$, we have $\varphi^{b_j}(x) = x$. When we need to emphasize the distinct parts $b_1, \dots, b_s$ of T_φ , the notation $T_\varphi = [b_1^{(r_1)}, \dots, b_s^{(r_s)}]$ will be used, where, for every $i \in \llbracket s \rrbracket$, r_i counts how many times b_i appears in T_φ . As an example, if $T_\varphi = [1, 1, 2, 2, 3, 4, 4, 4]$, then we can write $T_\varphi = [1^{(2)}, 2^{(2)}, 3, 4^{(3)}]$. It is well known that, given $\varphi_1, \varphi_2 \in \text{Sym}(X)$, we have $T_{\varphi_1} = T_{\varphi_2}$ if and only if φ_1 and φ_2 are conjugate in $\text{Sym}(X)$ (see Proposition 4.30 in Milne, 2021).

We now consider the second action that plays a crucial role in our paper: the action on the set of preference profiles. First, recall that, given $p \in \mathcal{P}$ and $\varphi \in G^*$, we have defined in (4) the preference profile p^φ . Given now a subgroup U of G^* , consider the function $f : U \rightarrow \text{Sym}(\mathcal{P})$ that maps each $\varphi \in U$ to the function $f(\varphi) : \mathcal{P} \rightarrow \mathcal{P}$ that associates each $p \in \mathcal{P}$ with $p^\varphi \in \mathcal{P}$. Remarkably, the function f is an action of U on $\mathcal{P}$. To establish this, we first need to prove that, for every $\varphi \in U$, $f(\varphi)$ is indeed a bijection from $\mathcal{P}$ to $\mathcal{P}$. Furthermore, we must show that $f : U \rightarrow \text{Sym}(\mathcal{P})$ is in fact a homomorphism between groups. Both facts easily follow from the next proposition.

Proposition 6. Let $p \in \mathcal{P}$ and $\varphi_1, \varphi_2 \in G^*$. Then, $(p^{\varphi_2})^{\varphi_1} = p^{\varphi_1 \varphi_2}$.

Proof. We have to show that, for every $z \in I$, $(p^{\varphi_2})^{\varphi_1}(z) = p^{\varphi_1 \varphi_2}(z)$. Consider $z \in I$. Then we have

$$\begin{aligned} (p^{\varphi_2})^{\varphi_1}(z) &= \varphi_1(p^{\varphi_2}(\varphi_1^{-1}(z))) = \varphi_1(\varphi_2(p(\varphi_2^{-1}(\varphi_1^{-1}(z)))) \\ &= (\varphi_1 \varphi_2)(p((\varphi_1 \varphi_2)^{-1}(z))) = p^{\varphi_1 \varphi_2}(z), \end{aligned}$$

as desired. $\square$

Indeed, given $\varphi \in U$, the map $f(\varphi) : \mathcal{P} \rightarrow \mathcal{P}$ is surjective because, by Proposition 6, for every $p \in \mathcal{P}$, we have

$$f(\varphi)(p^{\varphi^{-1}}) = (p^{\varphi^{-1}})^\varphi = p^{\text{id}_I} = p.$$

¹⁷ A partition of a nonempty set X is a set of nonempty pairwise disjoint subsets of X whose union is X .

Thus, since $\mathcal{P}$ is finite, $f(\varphi)$ is bijective. Moreover, f is a homomorphism from U to $\text{Sym}(\mathcal{P})$ because, as a further application of Proposition 6, for every $\varphi_1, \varphi_2 \in U$, we have $f(\varphi_1 \varphi_2) = f(\varphi_1)f(\varphi_2)$.

B.2. Basic applications of group theory to matchings

In this section, we collect some key points where group theory comes at play in our model. Proposition 7 describes some useful properties of matchings and clarifies the observations made at the beginning of Section 3.2. Proposition 8 establishes that G^* -symmetry, gender fairness, and the combination of peer indifference and gender indifference are equivalent concepts. Propositions 9 and 10 are about the different levels of symmetry exhibited by some matching mechanisms studied in the literature. We also provide the proofs of Propositions 2 and 3 stated in Section 4.2.

Proposition 7. The following facts hold true:

- (i) $\mathcal{M} = \{\mu \in G^* \setminus G : |\mu| = 2\} \neq \emptyset$;
- (ii) $\mathcal{M} = \{\mu \in G^* \setminus G : T_\mu = [2^{(n)}]\}$;
- (iii) for every $\varphi \in G^*$, $\mathcal{M}^\varphi = \mathcal{M}$.

Proof. (i) Let $\mu \in \mathcal{M}$. Then, by definition, μ leaves the partition $\{W, M\}$ of I invariant and swaps W and M ; hence $\mu \in G^* \setminus G$. In particular, $\mu \neq \text{id}_I$. Moreover, the fact that $\mu(\mu(z)) = z$ for all $z \in I$ implies that $|\mu| = 2$. The other inclusion is obvious. The nonemptiness of $\mathcal{M}$ is immediate since $\mu = (1 \ n+1) \dots (n \ 2n)$ is a matching.

(ii) By (i), we just need to show that $\mu \in G^* \setminus G$ has order 2 if and only if $T_\mu = [2^{(n)}]$. If $T_\mu = [2^{(n)}]$, then obviously $|\mu| = 2$. Let $\mu \in G^* \setminus G$ with $|\mu| = 2$. Then $T_\mu = [2^{(k)}, 1^{(s)}]$ with $2k + s = 2|W|$ and $s \geq 0$. Since μ takes W into M and M into W , every orbit of μ contains at least an element in W and an element in M . As a consequence, no part of T_μ can be smaller than 2 and thus $s = 0$.

(iii) We first show that, for every $\varphi \in G^*$, $\mathcal{M}^\varphi \subseteq \mathcal{M}$. Let $\varphi \in G^*$. Consider then $\mu \in \mathcal{M}$ and prove that $\mu^\varphi \in \mathcal{M}$. By (i), we have $\mu \in G^* \setminus G$ and $|\mu| = 2$. Since G^* is a group, $\mu^\varphi \in G^*$. Assume that $\mu^\varphi \in G$. Since G is normal in G^* , we deduce that $\mu = (\mu^\varphi)^{\varphi^{-1}} \in G$, a contradiction. Thus, $\mu^\varphi \in G^* \setminus G$. Moreover, we have $|\mu^\varphi| = |\mu|$ as μ and μ^φ are conjugate. Thus, by (i), we get $\mu^\varphi \in \mathcal{M}$.

We complete the proof showing that, for every $\varphi \in G^*$, $\mathcal{M} \subseteq \mathcal{M}^\varphi$. Let $\varphi \in G^*$. Since $\varphi^{-1} \in G^*$, by the first part of the proof, we get $\mathcal{M}^{\varphi^{-1}} \subseteq \mathcal{M}$ and then $\mathcal{M} = (\mathcal{M}^{\varphi^{-1}})^\varphi \subseteq \mathcal{M}^\varphi$. $\square$

Proof of Proposition 2. Assume that F is $\langle U \rangle$ -symmetric. Then, for every $p \in \mathcal{P}$ and $\varphi \in \langle U \rangle$, $F(p^\varphi) = F(p)^\varphi$. In particular, for every $p \in \mathcal{P}$ and $\varphi \in U$, $F(p^\varphi) = F(p)^\varphi$. Thus, we conclude that F is U -symmetric.

Assume now that F is U -symmetric. Then, for every $p \in \mathcal{P}$ and $\varphi \in U$, $F(p^\varphi) = F(p)^\varphi$. It remains to prove that, for every $p \in \mathcal{P}$ and $\varphi \in \langle U \rangle$, $F(p^\varphi) = F(p)^\varphi$. Let us set $U_1 = U$ and, for every $k \in \mathbb{N}$, let

$$U_k := \{\varphi \in G^* : \exists \sigma_1, \dots, \sigma_k \in U \text{ such that } \varphi = \sigma_1 \dots \sigma_k\}.$$

For every $k \in \mathbb{N}$, consider the following statement, denoted by $S(k)$,

for every $p \in \mathcal{P}$ and $\varphi \in U_k$, we have that $F(p^\varphi) = F(p)^\varphi$.

We claim that, for every $k \in \mathbb{N}$, $S(k)$ is true. We prove that fact by induction. The truth of $S(1)$ is immediate. Assume that $S(k)$ is true and prove that $S(k+1)$ is true. Let $p \in \mathcal{P}$ and $\varphi \in U_{k+1}$ and prove that $F(p^\varphi) = F(p)^\varphi$. Since $\varphi \in U_{k+1}$, we can find $\psi \in U_k$ and $\sigma \in U = U_1$ such that $\varphi = \psi\sigma$. Thus, by Proposition 6, we have that $p^\varphi = p^{\psi\sigma} = (p^\sigma)^\psi$. Thus,

$$F(p^\varphi) = F(p^{\psi\sigma}) = F((p^\sigma)^\psi) = F(p^\sigma)^\psi = (F(p)^\sigma)^\psi = F(p)^{\psi\sigma} = F(p)^\varphi,$$

where the third equality follows from the fact that $S(k)$ is true, the fourth one from the fact that $S(1)$ is true and the fifth one from (8).

By the claim and the fact that $\langle U \rangle = \bigcup_{k \in \mathbb{N}} U_k$, we then deduce that, for every $p \in \mathcal{P}$ and $\varphi \in \langle U \rangle$, $F(p^\varphi) = F(p)^\varphi$, as desired. $\square$

Proof of Proposition 3. (i) We have to show that, for every $p \in \mathcal{P}$ and $\varphi \in U$, $C^U(p^\varphi) = C^U(p)^\varphi$. Consider then $p \in \mathcal{P}$ and $\varphi \in U$. Recalling that conjugation by φ defines a bijection and using (10), Proposition 7(iii) and the properties of stabilizers and centralizers, we have that

$$C^U(p^\varphi) = C_{G^*}(\text{Stab}_U(p^\varphi)) \cap \mathcal{M} = C_{G^*}([\text{Stab}_U(p)]^\varphi) \cap \mathcal{M}^\varphi \\ = (C_{G^*}[\text{Stab}_U(p)])^\varphi \cap \mathcal{M}^\varphi = (C_{G^*}[\text{Stab}_U(p)] \cap \mathcal{M})^\varphi = C^U(p)^\varphi.$$

(ii) Let F be a resolute and U -symmetric matching mechanism. Consider $p \in \mathcal{P}$ and let μ be the unique matching in $F(p)$. By (10), we prove that $\mu \in C^U(p)$ by showing that, for every $\varphi \in \text{Stab}_U(p)$, the equality $\mu^\varphi = \mu$ holds. Let $\varphi \in \text{Stab}_U(p)$. Then, $p^\varphi = p$ and, since F is U -symmetric, we have

$$\{\mu\} = F(p) = F(p^\varphi) = F(p)^\varphi = \{\mu\}^\varphi = \{\mu^\varphi\},$$

that implies the desired equality. $\square$

Proposition 8. Let $\varphi \in \mathcal{M}$. Then $\langle G \cup \{\varphi\} \rangle = \langle G^* \setminus G \rangle = G^*$.

Proof. Let us prove first $\langle G^* \setminus G \rangle = G^*$. Let $U := \langle G^* \setminus G \rangle$. We want to show that $U = G^*$. Since $U \supseteq G^* \setminus G$, it is enough to show that $U \supseteq G$. Consider then $\psi \in G$ and prove that $\psi \in U$. Pick $\varphi \in G^* \setminus G$. Using the fact that G is normal in G^* , we get $G = G^\varphi$. Then there exists $v \in G$ such that $\psi = v^\varphi$. Hence, we have $\psi = \varphi(v\varphi^{-1})$. We cannot have $v\varphi^{-1} \in G$, because that would imply $\varphi \in G$. Thus, we have expressed ψ as the product of two elements in $G^* \setminus G$, and hence $\psi \in U$.

Let us prove now $\langle G \cup \{\varphi\} \rangle = G^*$. Let $U := \langle G \cup \{\varphi\} \rangle$. We want to show that $U = G^*$. Since $U \supseteq G \cup \{\varphi\}$ and $\varphi \in G^* \setminus G$, we have that $U \supseteq G$ and $U \neq G$. By Lagrange Theorem, we then have that $|G|$ properly divides $|U|$. Then $|U| = |G|k$, for some $k \in \mathbb{N}$, with $k \geq 2$. On the other hand, using again Lagrange Theorem, we also have that $|U|$ divides $|G^*| = 2|G|$. As a consequence $|U| = 2|G| = |G^*|$ and hence $U = G^*$. $\square$

Proposition 9. GS_w and GS_m are G -symmetric but they are not G^* -symmetric. GS , ST , PO , WPO , MO and TO are G^* -symmetric.

Proof. The G -symmetry of GS_w and GS_m follows from the nature of the algorithm in Gale and Shapley (1962). Let us prove that GS_w and GS_m are not G^* -symmetric. Indeed, let $W = \llbracket n \rrbracket$, $M = \{y_1, \dots, y_n\}$, and consider the preference profile

$$p^\varphi = \begin{array}{c|cccc|cccc} 1 & 2 & (3) & \dots & (n) & y_1 & y_2 & (y_3) & \dots & (y_n) \\ \hline y_1 & y_2 & (y_3) & \dots & (y_n) & 2 & 1 & (3) & \dots & (n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array},$$

where the vertical dots mean that the missing entries of each linear order can be listed in any possible order. Consider the permutation $\varphi = (1 y_1)(2 y_2) \dots (n y_n) \in G^*$ that switches woman x and man y_x for each $x \in \llbracket n \rrbracket$. Let $\gamma^* = id_I$ if $n = 2$ while $\gamma^* = (3 y_3) \dots (n y_n) \in \text{Sym}(I)$ if $n \geq 3$. Note that, for every $n \geq 2$, we have $\varphi = (1 y_1)(2 y_2)\gamma^*$. It is immediate to check that $GS_w(p) = \{\varphi\}$ and $GS_m(p) = \{(1 y_2)(2 y_1)\gamma^*\}$, and then $GS_w(p) = GS_w(p)^\varphi$ and $GS_m(p) = GS_m(p)^\varphi$. We also have that

$$p^\varphi = \begin{array}{c|cccc|cccc} y_1 & y_2 & (y_3) & \dots & (y_n) & 1 & 2 & (3) & \dots & (n) \\ \hline 1 & 2 & (3) & \dots & (n) & y_2 & y_1 & (y_3) & \dots & (y_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \\ = \begin{array}{c|cccc|cccc} 1 & 2 & (3) & \dots & (n) & y_1 & y_2 & (y_3) & \dots & (y_n) \\ \hline y_2 & y_1 & (y_3) & \dots & (y_n) & 1 & 2 & (3) & \dots & (n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}.$$

Thus, $GS_w(p^\varphi) = \{(1 y_2)(2 y_1)\gamma^*\} \neq GS_w(p)^\varphi$ and $GS_m(p^\varphi) = \{\varphi\} \neq GS_m(p)^\varphi$. As a consequence, GS_w and GS_m fail to be G^* -symmetric.

In order to prove that GS is G^* -symmetric, we need to show that, for every $p \in \mathcal{P}$ and $\varphi \in G^*$, $GS(p^\varphi) = GS(p)^\varphi$. If $\varphi \in G$, that is a consequence of the G -symmetry of GS_w and GS_m . Indeed, $GS(p^\varphi) = \{GS_w(p^\varphi), GS_m(p^\varphi)\} = \{GS_w(p)^\varphi, GS_m(p)^\varphi\} = GS(p)^\varphi$. If $\varphi \in G^* \setminus G$, the proof has been provided in Proposition 3.3 by Özkal-Sanver (2004).

The fact that ST is G^* -symmetric follows immediately from the following property: if $\mu \in \mathcal{M}$, $p \in \mathcal{P}$ and $\varphi \in G^*$, the pair $(x, y) \in W \times M$ blocks μ according to p if and only if the pair $(\varphi(x), \varphi(y))$ blocks μ^φ according to p^φ . We remark that $(\varphi(x), \varphi(y)) \in W \times M$ if $\varphi \in G$, while $(\varphi(x), \varphi(y)) \in M \times W$ if $\varphi \in G^* \setminus G$. Let us prove the stated property. By definition, $(x, y) \in W \times M$ blocks μ according to p if

$$y \succ_{p(x)} \mu(x) \text{ and } x \succ_{p(y)} \mu(y).$$

By (5), that is equivalent to

$$\varphi(y) \succ_{p^\varphi(\varphi(x))} \varphi(\mu(x)) \text{ and } \varphi(x) \succ_{p^\varphi(\varphi(y))} \varphi(\mu(y)),$$

which, in turn, is equivalent to

$$\varphi(y) \succ_{p^\varphi(\varphi(x))} \mu^\varphi(\varphi(x)) \text{ and } \varphi(x) \succ_{p^\varphi(\varphi(y))} \mu^\varphi(\varphi(y)),$$

that is, $(\varphi(x), \varphi(y))$ blocks the matching μ^φ according to p^φ .

The fact that WPO is G^* -symmetric follows immediately from the following property: for every $\mu \in \mathcal{M}$ and $\varphi \in G^*$, μ is not weakly Pareto optimal for p if and only if μ^φ is not weakly Pareto optimal for p^φ . In order to prove the aforementioned property, consider $\mu \in \mathcal{M}$ and $\varphi \in G^*$ and note that, by definition, μ is not weakly Pareto optimal for p if and only if there exists a matching $\mu' \in \mathcal{M}$ such that, for every $z \in I$, $\mu'(z) \succ_{p(z)} \mu(z)$. For every $z \in I$, we have that $\mu'(z) \succ_{p(z)} \mu(z)$ is equivalent to $\varphi(\mu'(z)) \succ_{p^\varphi(\varphi(z))} \varphi(\mu(z))$ that, in turn, is equivalent to $(\mu')^\varphi(\varphi(z)) \succ_{p^\varphi(\varphi(z))} \mu^\varphi(\varphi(z))$. Since that holds true for each $z \in I$ and since $(\mu')^\varphi \in \mathcal{M}$, that is equivalent to state that the matching μ^φ is not weakly Pareto optimal for p^φ .

The proof that PO is G^* -symmetric is similar to the proof that WPO is G^* -symmetric and then omitted.

Let us prove that MO is G^* -symmetric. This is an immediate consequence of the following property: for every $\mu \in \mathcal{M}$ and $\varphi \in G^*$, μ is not minimally optimal for p if and only if μ^φ is not minimally optimal for p^φ . That property can be proved by noticing that $\mu \notin MO(p)$ is equivalent to $\text{Rank}_{p(z)} \mu(z) = n$ for all $z \in I$, which in turn is equivalent to $\text{Rank}_{p^\varphi(\varphi(z))} (\mu^\varphi)(\varphi(z)) = n$ for all $z \in I$, which is equivalent to $\mu^\varphi \notin MO(p^\varphi)$.

Finally, TO is G^* -symmetric since, for every $p \in \mathcal{P}$ and $\varphi \in G^*$, we have that $TO(p) = TO(p^\varphi) = \mathcal{M}$ and, by Proposition 7(iii), $\mathcal{M}^\varphi = \mathcal{M}$. $\square$

Proposition 10. SE and ES are G^* -symmetric.

Proof. Let us prove that SE is G^* -symmetric. Observe first that, immediately from the definition of p^φ , for every $\varphi \in G^*$, $p \in \mathcal{P}$ and $z, u \in I$ of different gender, we have that

$$\text{Rank}_{p^\varphi(\varphi(z))} \varphi(u) = \text{Rank}_{p(z)} u. \quad (12)$$

We next show that, for every $\varphi \in G^*$, $p \in \mathcal{P}$ and $\mu \in \mathcal{M}$, we have

$$\delta(p^\varphi, \mu^\varphi) = \delta(p, \mu). \quad (13)$$

Indeed, using (12), we have

$$\begin{aligned} \delta(p^\varphi, \mu^\varphi) &= \left| \sum_{x \in W} \text{Rank}_{p^\varphi(x)} (\mu^\varphi(x)) - \sum_{y \in M} \text{Rank}_{p^\varphi(y)} (\mu^\varphi(y)) \right| \\ &= \left| \sum_{x \in W} \text{Rank}_{p^\varphi(\varphi(x))} (\mu^\varphi(\varphi(x))) - \sum_{y \in M} \text{Rank}_{p^\varphi(\varphi(y))} (\mu^\varphi(\varphi(y))) \right| \\ &= \left| \sum_{x \in W} \text{Rank}_{p^\varphi(\varphi(x))} (\varphi \mu(x)) - \sum_{y \in M} \text{Rank}_{p^\varphi(\varphi(y))} (\varphi \mu(y)) \right| \\ &= \left| \sum_{x \in W} \text{Rank}_{p(x)} (\mu(x)) - \sum_{y \in M} \text{Rank}_{p(y)} (\mu(y)) \right| = \delta(p, \mu). \end{aligned}$$

As a consequence, using the fact that ST is G^* -symmetric and applying (13), we have that, for every $p \in \mathcal{P}$ and $\varphi \in G^*$,

$$\begin{aligned} SE(p^\varphi) &= \arg \min_{\mu \in ST(p^\varphi)} \delta(p^\varphi, \mu) = \arg \min_{\mu \in ST(p)^\varphi} \delta(p^\varphi, \mu) = \left(\arg \min_{\sigma \in ST(p)} \delta(p^\varphi, \sigma^\varphi) \right)^\varphi \\ &= \left(\arg \min_{\sigma \in ST(p)} \delta(p, \sigma) \right)^\varphi = SE(p)^\varphi. \end{aligned}$$

Thus, SE is G^* -symmetric.

The proof that ES is G^* -symmetric follows the same line of reasoning, and hence, for the sake of brevity, is omitted. $\square$

B.3. Proof of Proposition 4

Given $U \leq G^*$, by means of the action of U on the set $\mathcal{P}$ of preference profiles considered in Appendix B.1, we can transfer the notation and results concerning the action of a group on a set into the framework of matching theory.

For every $p \in \mathcal{P}$, the U -orbit of p in $\mathcal{P}$ is $p^U = \{p^\varphi \in \mathcal{P} : \varphi \in U\}$. We denote by R the size of the set $\mathcal{P}^U = \{p^U : p \in \mathcal{P}\}$ of the U -orbits of $\mathcal{P}$.¹⁸ A system of representatives of the U -orbits of $\mathcal{P}$ is any $(p_j)_{j=1}^R \in \mathcal{P}^R$ such that $\mathcal{P}^U = \{p_j^U : j \in \llbracket R \rrbracket\}$. Moreover, for every $p \in \mathcal{P}$, the U -stabilizer of p is the set $\text{Stab}_U(p) = \{\varphi \in U : p^\varphi = p\}$ (see Definition 6).

Before proving Proposition 4, we propose the following preliminary result.

Lemma 2. Let $U \leq G^*$, $(p_j)_{j=1}^R \in \mathcal{P}^R$ be a system of representatives for the U -orbits of $\mathcal{P}$, and suppose that, for every $j \in \llbracket R \rrbracket$, $C^U(p_j) \neq \emptyset$. Let $(\mu_j)_{j=1}^R$ be a sequence of matchings such that, for every $j \in \llbracket R \rrbracket$, $\mu_j \in C^U(p_j)$. Then, there exists a unique resolute and U -symmetric matching mechanism H such that, for every $j \in \llbracket R \rrbracket$, $H(p_j) = \{\mu_j\}$.

Proof. Observe first that, given $p \in \mathcal{P}$, there exists $j \in \llbracket R \rrbracket$ and $\varphi_j \in U$ such that $p = p_j^{\varphi_j}$. Consider then the matching mechanism H defined, for every $p \in \mathcal{P}$, by $H(p) := \{\mu_j^{\varphi_j}\}$, where $j \in \llbracket R \rrbracket$ and $\varphi_j \in U$ are such that $p = p_j^{\varphi_j}$.

We first prove that H is well defined. Let $p \in \mathcal{P}$ and assume that $p = p_{j_1}^{\varphi_1}$ and $p = p_{j_2}^{\varphi_2}$, where $j_1, j_2 \in \llbracket R \rrbracket$ and $\varphi_1, \varphi_2 \in U$. We have to prove that $\mu_{j_1}^{\varphi_1} = \mu_{j_2}^{\varphi_2}$. Note that, since $(p_j)_{j=1}^R \in \mathcal{P}^R$ is a system of representatives for the U -orbits in $\mathcal{P}$, it must be $j_1 = j_2$; therefore $\mu_{j_1} = \mu_{j_2}$ and $p_{j_1} = p_{j_2}$. We now have that $\mu_{j_1}^{\varphi_1} = \mu_{j_1}^{\varphi_2}$ is equivalent to $(\mu_{j_1}^{\varphi_1})^{\varphi_2^{-1}} = \mu_{j_1}$ that, in turn, is equivalent to $\mu_{j_1}^{\varphi_2^{-1}\varphi_1} = \mu_{j_1}$. In order to prove the equality $\mu_{j_1}^{\varphi_2^{-1}\varphi_1} = \mu_{j_1}$, observe that $\varphi_2^{-1}\varphi_1 \in \text{Stab}_U(p_{j_1})$. Indeed, from $p = p_{j_1}^{\varphi_1}$ and $p = p_{j_1}^{\varphi_2}$, we get $p_{j_1}^{\varphi_1} = p_{j_1}^{\varphi_2}$ and then, using the action, we have $(p_{j_1}^{\varphi_1})^{\varphi_2^{-1}} = p_{j_1}$, that is, $p_{j_1}^{\varphi_2^{-1}\varphi_1} = p_{j_1}$. Since $\mu_{j_1} \in C^U(p_{j_1})$, we can then conclude that $\mu_{j_1}^{\varphi_2^{-1}\varphi_1} = \mu_{j_1}$, as desired. Thus, H is well defined.

Of course, H is resolute and since, for every $j \in \llbracket R \rrbracket$, $p_j = p_j^{\text{id}_U}$, we have that $H(p_j) = \{\mu_j\}$.

Let us prove that H is U -symmetric. Consider then $p \in \mathcal{P}$ and $\varphi \in U$ and let us prove that $H(p^\varphi) = H(p)^\varphi$. Let $j \in \llbracket R \rrbracket$ and $\varphi_j \in U$ be such that $p = p_j^{\varphi_j}$. Thus, $H(p) = \{\mu_j^{\varphi_j}\} = H(p_j)^{\varphi_j}$ and

$$H(p^\varphi) = H\left(\left(p_j^{\varphi_j}\right)^\varphi\right) = H\left(p_j^{\varphi_j\varphi}\right) = H(p_j)^{\varphi_j\varphi} = (H(p_j)^{\varphi_j})^\varphi = H(p)^\varphi.$$

It remains to prove the uniqueness. Consider a U -symmetric and resolute matching mechanism H' such that, for every $j \in \llbracket R \rrbracket$, $H'(p_j) = \mu_j$. We have to prove that, for every $p \in \mathcal{P}$, $H(p) = H'(p)$. Consider then $p \in \mathcal{P}$. There exist $j \in \llbracket R \rrbracket$ and $\varphi_j \in U$ such that $p = p_j^{\varphi_j}$. Thus, using

the U -symmetry of H and H' and the fact that $H(p_j) = H'(p_j) = \{\mu_j\}$, we get

$$H'(p) = H'(p_j^{\varphi_j}) = H'(p_j)^{\varphi_j} = \{\mu_j^{\varphi_j}\} = H(p_j)^{\varphi_j} = H(p_j^{\varphi_j}) = H(p),$$

as desired. $\square$

Proof of Proposition 4. Assume that F admits a U -symmetric and resolute refinement H . Using Proposition 3, we deduce that, for every $p \in \mathcal{P}$, $H(p) \subseteq F(p) \cap C^U(p)$ and so $F(p) \cap C^U(p) \neq \emptyset$.

Conversely, assume that, for every $p \in \mathcal{P}$, $F(p) \cap C^U(p) \neq \emptyset$. Let $(p_j)_{j=1}^R \in \mathcal{P}^R$ be a system of representatives for the U -orbits in $\mathcal{P}$ and $(\mu_j)_{j=1}^R$ be a sequence of matchings such that, for every $j \in \llbracket R \rrbracket$, $\mu_j \in F(p_j) \cap C^U(p_j) \neq \emptyset$. By Lemma 2 there exists a unique U -symmetric and resolute matching mechanism H on $\mathcal{P}$ such that, for every $j \in \llbracket R \rrbracket$, $H(p_j) = \{\mu_j\}$. Let us prove that H is a refinement of F . Let $p \in \mathcal{P}$ and consider $j \in \llbracket R \rrbracket$ and $\varphi_j \in U$ such that $p = p_j^{\varphi_j}$. Then, using the U -symmetry of H and F , we get

$$H(p) = H(p_j^{\varphi_j}) = H(p_j)^{\varphi_j} = \{\mu_j^{\varphi_j}\} \subseteq F(p_j)^{\varphi_j} = F(p_j^{\varphi_j}) = F(p). \quad \square$$

Appendix C. Semiregular permutation groups

C.1. Semiregular subgroups of G^*

We start this section recalling some definitions from the theory of permutation groups.

Let X be a nonempty and finite set and S be a subgroup of $\text{Sym}(X)$. S is called semiregular if, for every $x \in X$, we have $\text{Stab}_S(x) = \{\text{id}_X\}$. In other words, S is semiregular if the only $\varphi \in S$ fixing at least an element of X is $\varphi = \text{id}_X$.¹⁹ S is called transitive if, for every $x, y \in X$, there exists $s \in S$ such that $s(x) = y$; regular if S is transitive and semiregular. Clearly, S is transitive if and only if S admits a unique orbit on X .

The following proposition describes some general properties of semiregular groups.²⁰

Proposition 11. Let X be a nonempty and finite set and let $S \leq \text{Sym}(X)$ be semiregular. Then, the following facts hold true:

- (i) every orbit of S has size $|S|$;
- (ii) $|S|$ divides $|X|$ and the number of orbits of S is $\frac{|X|}{|S|}$;
- (iii) S is regular if and only if $|S| = |X|$;
- (iv) every subgroup of S is semiregular;
- (v) if $s_1, s_2 \in S$ are such that there exists $x \in X$ with $s_1(x) = s_2(x)$, then $s_1 = s_2$.

Proof. (i) Pick $x \in X$. Then, $|x^S| = \frac{|S|}{|\text{Stab}_S(x)|} = |S|$.

(ii) We know that X is disjoint union of the orbits of S . By (i), each orbit of S has size $|S|$. Thus, we deduce that $|S|$ divides $|X|$ and that the number of orbits of S is $\frac{|X|}{|S|}$.

(iii) Assume that S is regular. Pick $x \in X$. Since S is transitive, we have $x^S = X$. Since $|\text{Stab}_S(x)| = 1$, it follows that $|X| = |x^S| = \frac{|S|}{|\text{Stab}_S(x)|} = |S|$. Conversely, assume that $|S| = |X|$. Pick $x \in X$. Since $|\text{Stab}_S(x)| = 1$, we have $|x^S| = \frac{|S|}{|\text{Stab}_S(x)|} = |S| = |X|$. Thus, $x^S = X$, which says that S is transitive.

¹⁸ The number R depends of course on U and $\mathcal{P}$. We can avoid more precise notation since U and $\mathcal{P}$ are always clear from the context.

¹⁹ The concept of semiregularity is widely considered in the literature of permutation groups. Some recent contributions involving semiregular groups are, for instance, Maynard and Siemons (2002), Bereczky and Maróti (2008), Kovács et al. (2015).

²⁰ Even though Proposition 11 expresses classic and well-established facts, we could not find a reference containing the statements necessary for our scopes. So, for clarity of exposition, we have preferred to state and prove what needed.

(iv) Let $U \leq S$. Then, for every $x \in X$, we have $\text{Stab}_U(x) = U \cap \text{Stab}_S(x) = U \cap \{id_X\} = \{id_X\}$. Thus, U is semiregular.

(v) Let $s_1, s_2 \in S$ and $x \in X$ be such that $s_1(x) = s_2(x)$. Thus, $s_2^{-1}s_1(x) = x$, that is, $s_2^{-1}s_1 \in \text{Stab}_S(x) = \{id_X\}$. As a consequence, $s_2^{-1}s_1 = id_X$, that is, $s_1 = s_2$. $\square$

We emphasize the strong consequence of semiregularity expressed by Proposition 11(v): if two permutations of S coincide on a single element of X , then they coincide on the whole set X .

From here on, we focus on the properties of semiregular subgroups of G^* under the assumption that n is odd.

Proposition 12. *Let n be odd and $S \leq G$ be semiregular. Then, the following facts hold true:*

- (i) every orbit of S is included in W or is included in M ;
- (ii) $|S|$ divides n and there are $\frac{n}{|S|}$ orbits of S included in W and $\frac{n}{|S|}$ orbits of S included in M ;
- (iii) $|S|$ is odd and the number of orbits of S is even.

Proof. (i) Since $S \leq G$, every $\varphi \in S$ takes W in W and M in M . Thus, every orbit of S is included in W or in M .

(ii) By (i), we know that W is union of orbits of S , and M is union of orbits of S . Since S is semiregular, by Proposition 11(i), we know that each orbit of S has size $|S|$. Then we conclude that $|S|$ divides $|W| = |M| = n$ and there are $\frac{n}{|S|}$ orbits of S included in W and $\frac{n}{|S|}$ orbits of S included in M .

(iii). Since n is odd and $|S|$ divides n , we deduce that $|S|$ is odd. Moreover, by Proposition 11(ii), we know that the number of orbits of S is $\frac{2n}{|S|}$, which is even because $|S|$ is odd. $\square$

Proposition 13. *Let n be odd and $S \leq G^*$ be semiregular and such that $S \not\leq G$. Then, the following facts hold true:*

- (i) $|S|$ is even and, for every $z \in I$, $|z^S \cap W| = |z^S \cap M| = \frac{|S|}{2}$;
- (ii) $|S|$ divides $2n$ and the number of orbits of S is odd.

Proof. (i) Let $z \in I$ and prove that $|z^S \cap W| = |z^S \cap M|$. Since $S \not\leq G$ there exists $s \in S \setminus G \subseteq G^* \setminus G$. Since s takes W in M , we can consider the function $\bar{s} : z^S \cap W \rightarrow z^S \cap M$ defined, for every $x \in z^S \cap W$, by $\bar{s}(x) = s(x)$. We have that $\bar{s}$ is injective, because if $x_1, x_2 \in z^S \cap W$ are such that $\bar{s}(x_1) = \bar{s}(x_2)$, then we have that $s(x_1) = s(x_2)$ and thus $x_1 = x_2$. Let us prove that $\bar{s}$ is surjective. First, let us observe that $s^{-1} \in S \setminus G$. Indeed $s^{-1} \in S$ because S is a group. Moreover, $s^{-1} \notin G$ because, being G a group, $s^{-1} \in G$ implies $s \in G$. Consider now $y \in z^S \cap M$ and note that $s^{-1}(y) \in z^S \cap W$ and $\bar{s}(s^{-1}(y)) = ss^{-1}(y) = y$. We conclude then that $\bar{s}$ is a bijection, and so $|z^S \cap W| = |z^S \cap M|$. Using Proposition 11(i), we obtain that

$$\begin{aligned} |S| &= |z^S| = |z^S \cap (W \cup M)| = |(z^S \cap W) \cup (z^S \cap M)| \\ &= |z^S \cap W| + |z^S \cap M| = 2|z^S \cap W|. \end{aligned}$$

Thus, $|S|$ is even and $|z^S \cap W| = |z^S \cap M| = \frac{|S|}{2}$.

(ii) By Proposition 11(ii), we know that $|S|$ divides $2n$. Since n is odd and $|S|$ is even, we conclude that the number of orbits of S , that is $\frac{2n}{|S|}$, is odd. $\square$

We present a basic but useful result about centralizers in G^* .²¹

Proposition 14. *Let $\varphi \in \text{Sym}(I)$ be a $2n$ -cycle. Then, the following facts hold true:*

- (i) $C_{\text{Sym}(I)}(\langle \varphi \rangle) = \langle \varphi \rangle$;
- (ii) if $\varphi \in G^*$, then $C_{G^*}(\langle \varphi \rangle) = \langle \varphi \rangle$;

²¹ Proposition 14(i) is well known, but we could not find an exact reference. So, for the sake of a self-contained exposition, we have preferred to prove it.

(iii) if $\varphi \in G^* \setminus G$ and n is odd, then φ^n is the unique element of order 2 in $C_{G^*}(\langle \varphi \rangle) \cap (G^* \setminus G)$;

(iv) if $\varphi \in G^* \setminus G$ and n is even, then there exists no element of order 2 in $C_{G^*}(\langle \varphi \rangle) \cap (G^* \setminus G)$.

Proof. (i) By the fact that $\langle \varphi \rangle$ is abelian, we immediately get that $C := C_{\text{Sym}(I)}(\langle \varphi \rangle) \geq \langle \varphi \rangle$. Let us prove that C is semiregular. Consider then $z \in I$ and $\psi \in \text{Stab}_C(z)$ and prove that $\psi = id_I$. Given $u \in I$, since $\langle \varphi \rangle$ is transitive, we know that there exists $k \in \llbracket 2n \rrbracket$ such that $u = \varphi^k(z)$. Since $\psi \in C$, we have that $\psi\varphi^k = \varphi^k\psi$. Thus,

$$\psi(u) = \psi\varphi^k(z) = \varphi^k\psi(z) = \varphi^k(z) = u.$$

We conclude then that $\psi = id_I$, as desired. C is also transitive because it contains the transitive group $\langle \varphi \rangle$. Hence, C is regular. By Proposition 11(iii), we deduce that $|C| = 2n$ and hence $C = \langle \varphi \rangle$.

(ii) Let $\varphi \in G^*$. By (i), we have that $C_{G^*}(\langle \varphi \rangle) = G^* \cap C_{\text{Sym}(I)}(\langle \varphi \rangle) = G^* \cap \langle \varphi \rangle = \langle \varphi \rangle$.

(iii) Let $\varphi \in G^* \setminus G$ and n be odd. By (ii) the only element of order 2 in $C_{G^*}(\langle \varphi \rangle)$ is φ^n . Since n is odd we also have that $\varphi^n \in G^* \setminus G$.

(iv) Let $\varphi \in G^* \setminus G$ and n be even. By (ii) the only element of order 2 in $C_{G^*}(\langle \varphi \rangle)$ is φ^n . Since n is even we have that $\varphi^n \in G$ and thus $\varphi^n \notin G^* \setminus G$. $\square$

Let us prove the main result of the section.

Proposition 15. *Let n be odd and $S \leq G^*$ be semiregular. Then, there exists $\varphi \in C_{G^*}(S) \cap (G^* \setminus G)$ such that $|\varphi| = 2$.*

Proof. We have to show that there exists $\varphi \in G^* \setminus G$ satisfying the following two properties:

- (i) for every $s \in S$ and $z \in I$, $\varphi s(z) = s\varphi(z)$;
- (ii) for every $z \in I$, $\varphi\varphi(z) = z$.

We will define φ on I by specifying its definition on the orbits of S on I . To that purpose, we first observe that, given $z, z' \in I$ with $z' \in z^S$, there exists a unique $s \in S$ such that $z' = s(z)$. The existence of $s \in S$ for which $z' = s(z)$ follows directly from the definition of S -orbit of z . Furthermore, by Proposition 11(v), if $s, s' \in S$ are such that $z' = s(z) = s'(z)$, then $s = s'$. This guarantees the uniqueness. As a consequence, given $z \in I$, we can uniquely represent every element of z^S as $s(z)$ where $s \in S$. We will refer to such notable property as the *unique representation property* throughout the proof. The proof is structured in two cases.

Case 1. $S \leq G$.

By Proposition 12(i), we know that every orbit of S is included in W or in M and that there are $r := \frac{n}{|S|}$ orbits of S included in W as well as r orbits of S included in M , for a total of $2r$ orbits. Let $O_1^w, \dots, O_r^w$ be the distinct orbits of S included in W and $O_1^m, \dots, O_r^m$ be the distinct orbits of S included in M . For every $j \in \llbracket r \rrbracket$, let us fix $x_j \in O_j^w$ and $y_j \in O_j^m$. Thus, for every $j \in \llbracket r \rrbracket$, $O_j^w = x_j^S$ and $O_j^m = y_j^S$.

For every $j \in \llbracket r \rrbracket$, we define φ on $x_j^S \cup y_j^S$ by setting, for every $s \in S$, $\varphi(s(x_j)) := s(y_j)$ and $\varphi(s(y_j)) := s(x_j)$. Such a definition is consistent thanks to the unique representation property. Note that, for every $z \in x_j^S$, $\varphi(z) \in y_j^S$ and, for every $z \in y_j^S$, $\varphi(z) \in x_j^S$. Indeed, if $z \in x_j^S$, then $z = s(x_j)$ for some $s \in S$ and $\varphi(z) = \varphi(s(x_j)) = s(y_j) \in y_j^S$. Analogously, if $z \in y_j^S$, then $z = s(y_j)$ for some $s \in S$ and $\varphi(z) = \varphi(s(y_j)) = s(x_j) \in x_j^S$. As a consequence, for every $z \in x_j^S \cup y_j^S$, we have that $\varphi(z) \in x_j^S \cup y_j^S$. Moreover, $\varphi : x_j^S \cup y_j^S \rightarrow x_j^S \cup y_j^S$ is a bijection. In fact, it is sufficient to prove that $\varphi : x_j^S \cup y_j^S \rightarrow x_j^S \cup y_j^S$ is injective. Consider then $z, z' \in x_j^S \cup y_j^S$ such that $\varphi(z) = \varphi(z')$ and prove that $z = z'$. By the property of φ proved before, we must have $z, z' \in x_j^S$ or $z, z' \in y_j^S$. Assume $z, z' \in x_j^S$. By definition of orbit, there exist $s, s' \in S$ such that $z = s(x_j)$ and $z' = s'(x_j)$. Thus, $\varphi(z) = \varphi(z')$ implies $\varphi(s(x_j)) = \varphi(s'(x_j))$ that in turn, by the definition of φ , implies $s(y_j) = s'(y_j)$. By the unique representation property, we deduce that

$s = s'$ and therefore $z = s(x_j) = s'(x_j) = z'$. The case where $z, z' \in y_j^S$ is analogous and thus omitted.

Let us prove that $\varphi \in G^* \setminus G$. It is clear that $\varphi \in \text{Sym}(I)$. Thus, we only need to show that $\varphi(W) = M$. Consider then $x \in W$. We know that there exists $j \in \llbracket r \rrbracket$ such that $x \in x_j^S$. Then, $\varphi(x) \in y_j^S \subseteq M$. That shows $\varphi(W) \subseteq M$ and, since $|W| = |M|$, we deduce $\varphi(W) = M$.

Let us prove that φ satisfies (i). Consider $s \in S$ and $z \in I$, and let us show that $\varphi s(z) = s\varphi(z)$. If $z \in W$, there exists $j \in \llbracket r \rrbracket$ such that $z \in x_j^S$. Then, $z = s'(x_j)$ for some $s' \in S$. By definition of φ , we then have $\varphi s(z) = \varphi s s'(x_j) = s s'(y_j)$ and $s\varphi(z) = s\varphi(s'(x_j)) = s s'(y_j)$; therefore $\varphi s(z) = s\varphi(z)$, as desired. If $z \in M$, the argument is completely analogous and thus omitted.

Let us finally prove that φ satisfies (ii). Consider $z \in I$. If $z \in W$, there exists $j \in \llbracket r \rrbracket$ such that $z \in x_j^S$. Let $s \in S$ be such that $z = s(x_j)$. Thus

$$\varphi\varphi(z) = \varphi\varphi s(x_j) = \varphi s(y_j) = s(x_j) = z.$$

If $z \in M$, the argument is completely analogous and thus omitted.

Case 2. $S \not\leq G$.

Let $O_1, \dots, O_r$ be the orbits of S , where $r \in \mathbb{N}$. By Proposition 13(i), we know that $|S|$ is even and that, for every $j \in \llbracket r \rrbracket$, $|O_j \cap W| = |O_j \cap M| = \frac{|S|}{2}$. Since 2 divides $|S|$, by Cauchy theorem, there exists $s^* \in S$ such that $|s^*| = 2$. Let us prove that $s^* \in G^* \setminus G$. Indeed, by Proposition 11(iv), $\langle s^* \rangle$ is semiregular. Assume, by contradiction, that $\langle s^* \rangle \leq G$. Then, since n is odd, we can apply Proposition 12(iii) to $\langle s^* \rangle$ and deduce that $|\langle s^* \rangle| = |s^*| = 2$ is odd, a contradiction. For every $j \in \llbracket r \rrbracket$, let us fix $x_j \in O_j \cap W$ and set $y_j := s^*(x_j) \in O_j \cap M$. Note that, for every $j \in \llbracket r \rrbracket$, $x_j = s^*(y_j)$.

For every $j \in \llbracket r \rrbracket$, we define φ on x_j^S by setting, for every $s \in S$, $\varphi s(x_j) := s(y_j)$. Such a definition is consistent thanks to the unique representation property. Note that, for every $z \in x_j^S$, $\varphi(z) \in x_j^S$. Indeed, consider $z \in x_j^S$. Then $z = s(x_j)$ for some $s \in S$ and $\varphi(z) = \varphi s(x_j) = s(y_j) = s s^*(x_j) \in x_j^S$. Moreover, $\varphi : x_j^S \rightarrow x_j^S$ is a bijection. In order to prove that fact it is sufficient to prove that $\varphi : x_j^S \rightarrow x_j^S$ is injective. Consider then $z, z' \in x_j^S$ such that $\varphi(z) = \varphi(z')$. We know that there are $s, s' \in S$ such that $z = s(x_j)$ and $z' = s'(x_j)$. Thus, $\varphi(z) = \varphi(z')$ is equivalent to $\varphi s(x_j) = \varphi s'(x_j)$ that in turn is equivalent to $s(y_j) = s'(y_j)$. By the unique representation property, we deduce that $s = s'$; therefore $z = s(x_j) = s'(x_j) = z'$. Thus, we conclude that $\varphi : x_j^S \rightarrow x_j^S$ is injective and then bijective.

We show that $\varphi \in G^* \setminus G$. It is immediate to prove that $\varphi \in \text{Sym}(I)$. Thus, it remains to show that $\varphi(W) = M$. Consider then $z \in W$ and prove that $\varphi(z) \in M$. We know that there exists $j \in \llbracket r \rrbracket$ such that $z \in x_j^S$. Let $s \in S$ be such that $z = s(x_j)$. Since $z, x_j \in W$, we have that $s \in G$. Then, since $y_j \in M$, we have that $\varphi(z) = s(y_j) \in M$. That shows that $\varphi(W) \subseteq M$ and, since $|W| = |M|$, we deduce $\varphi(W) = M$.

We next prove that φ satisfies (i). Consider then $s \in S$ and $z \in I$, and show that $\varphi s(z) = s\varphi(z)$. Let $j \in \llbracket r \rrbracket$ be such that $z \in x_j^S$. Then $z = s'(x_j)$ for some $s' \in S$. By definition of φ , we then have $\varphi s(z) = \varphi s s'(x_j) = s s'(y_j)$ and $s\varphi(z) = s\varphi(s'(x_j)) = s s'(y_j)$; therefore $\varphi s(z) = s\varphi(z)$, as desired. Thus, (i) is proved.

We finally prove that φ satisfies (ii). Consider $z \in I$. We know that there exists $j \in \llbracket r \rrbracket$ such that $z \in x_j^S$. Let $s \in S$ be such that $z = s(x_j)$. Thus $\varphi\varphi(z) = \varphi\varphi s(x_j) = \varphi s(y_j) = \varphi s s^*(x_j) = s s^*(y_j) = s(x_j) = z$. $\square$

C.2. Semiregularity of the G^* -stabilizers

In this section, we analyze the G^* -stabilizers of preference profiles, with the main purpose to show that they are always semiregular subgroups of G^* , as stated in the next proposition.

Proposition 16. *Let $p \in \mathcal{P}$. Then, $\text{Stab}_{G^*}(p)$ is a semiregular subgroup of G^* .*

Proof. First, let us prove that, for every $\varphi \in \text{Stab}_{G^*}(p)$,

$$T_\varphi = [b^{(r)}], \text{ with } b = |\varphi|. \quad (14)$$

Consider $\varphi \in \text{Stab}_{G^*}(p) \cap G$. Then φ takes the set W into W and the set M into M . As a consequence, each orbit of φ on I is included in one of the sets W and M . Let $x_1, \dots, x_k, y_1, \dots, y_h$ be representatives of the orbits of φ on I , where $k, h \geq 1$, $x_1, \dots, x_k \in W$ and $y_1, \dots, y_h \in M$. Let us set, for every $j \in \llbracket k \rrbracket$, $b_j := |x_j^{(\varphi)}|$ and, for every $i \in \llbracket h \rrbracket$, $c_i := |y_i^{(\varphi)}|$. Pick $j \in \llbracket k \rrbracket$. Since $\text{Stab}_{G^*}(p) \cap G$ is a group, we have that $\varphi^{b_j} \in \text{Stab}_{G^*}(p) \cap G$, and then, by (5), we deduce

$$\varphi^{b_j} p(x_j) = p(\varphi^{b_j}(x_j)). \quad (15)$$

Using the fact that x_j is fixed by φ^{b_j} , (15) implies $\varphi^{b_j} p(x_j) = p(x_j)$. Since $p(x_j) \in \mathbf{L}(M)$, by Lemma 1, we get that, for every $y \in M$, $\varphi^{b_j}(y) = y$. Consider now $v \in \text{Sym}(M)$ defined, for every $y \in M$, by $v(y) = \varphi(y)$. For every $y \in M$, we have that $v^{b_j}(y) = \varphi^{b_j}(y) = y$. Thus, $v^{b_j} = \text{id}_M$ which implies $|v|$ divides b_j . Moreover, $y_1, \dots, y_h \in M$ are representatives of the orbits of v on M and, for every $i \in \llbracket h \rrbracket$, we have $y_i^{(v)} = y_i^{(\varphi)}$. As a consequence, for every $i \in \llbracket h \rrbracket$, $c_i = |y_i^{(v)}|$ divides $|v|$. Thus, for every $i \in \llbracket h \rrbracket$, c_i divides b_j . Pick now $i \in \llbracket h \rrbracket$. A completely analogous argument allows us to prove also that, for every $j \in \llbracket k \rrbracket$, b_j divides c_i . Thus, for every $j \in \llbracket k \rrbracket$ and $i \in \llbracket h \rrbracket$, b_j divides c_i and c_i divides b_j , and therefore $b_j = c_i$. Thus, the parts of φ are equal to each other and all equal to $|\varphi|$. That proves (14).

Consider now $\varphi \in \text{Stab}_{G^*}(p) \cap (G^* \setminus G)$. Let $T_\varphi = [b_1, \dots, b_r]$, where $r \in \mathbb{N}$ and $b_j \in \mathbb{N}$ for all $j \in \llbracket r \rrbracket$. Observe that a permutation in $G^* \setminus G$ takes W into M and M into W . Thus, every orbit of φ on I contains at least an element in W and an element in M . Moreover, the number of women and men in an orbit is the same. As a consequence, we have that, for every $j \in \llbracket r \rrbracket$, $b_j \geq 2$ and b_j is even. Let $z_1, \dots, z_r \in I$ be representatives of the orbits of φ on I such that, for every $j \in \llbracket r \rrbracket$, $|z_j^{(\varphi)}| = b_j$. Pick $j \in \llbracket r \rrbracket$. Since $\text{Stab}_{G^*}(p)$ is a group, we have that $\varphi^{b_j} \in \text{Stab}_{G^*}(p)$, and then, by (5), we deduce that, for every $z \in I$,

$$\varphi^{b_j} p(z) = p(\varphi^{b_j}(z)). \quad (16)$$

Consider $x \in z_j^{(\varphi)} \cap W$. Then, x is fixed by φ^{b_j} , and thus (16) implies $\varphi^{b_j} p(x) = p(x)$. Since $p(x) \in \mathbf{L}(M)$, by Lemma 1, we deduce that, for every $y \in M$, $\varphi^{b_j}(y) = y$. Consider now $y \in z_j^{(\varphi)} \cap M$. Then y is fixed by φ^{b_j} , and thus (16) implies $\varphi^{b_j} p(y) = p(y)$. Since $p(y) \in \mathbf{L}(W)$, by Lemma 1, we deduce that, for every $x \in W$, $\varphi^{b_j}(x) = x$. It follows that $\varphi^{b_j} = \text{id}_I$. As a consequence, $|\varphi|$ divides b_j . Since we know that b_j divides $|\varphi|$, we conclude that $|\varphi| = b_j$. Since that holds true for any $j \in \llbracket r \rrbracket$, we obtain that the parts in T_φ are equal to each other and all equal to $|\varphi|$. That proves (14).

Let us finally prove that $S := \text{Stab}_{G^*}(p) \leq \text{Sym}(I)$ is a semiregular subgroup of G^* . We need to prove that, for every $z \in I$, $\text{Stab}_S(z) = \{\text{id}_I\}$. Assume, by contradiction, that there exist $z \in I$ and $\varphi \in S \setminus \{\text{id}_I\}$ such that $\varphi(z) = z$. By the fact that $\varphi \in S \setminus \{\text{id}_I\}$ and by (14), we deduce that $T_\varphi = [b^{(r)}]$, with $b = |\varphi| \geq 2$. But such a permutation does not fix any element of I , a contradiction. $\square$

We now describe, up to group isomorphisms, the whole family of stabilizers when $n = 3$. That description helps the reader to understand the many possibilities that can arise and the fact that the description of the stabilizers is not, in general, an immediate task.

Let $n = 3$ and consider $p \in \mathcal{P}$. By Propositions 16 and 11(ii), we know that the size of $\text{Stab}_{G^*}(p)$ divides 6 and hence it belongs to the set $\{1, 2, 3, 6\}$. As a consequence, up to isomorphisms, we have $\text{Stab}_{G^*}(p) \in \{\{\text{id}_I\}, C_2, C_3, C_6, \text{Sym}(\llbracket 3 \rrbracket)\}$. Interestingly, all those cases can arise. Indeed, consider the following preference profiles

$$p_1 = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 4 & 4 & 1 & 1 & 1 \\ 5 & 5 & 5 & 2 & 2 & 3 \\ 6 & 6 & 6 & 3 & 3 & 2 \\ \hline \end{array}, \quad p_2 = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 4 & 4 & 1 & 1 & 1 \\ 5 & 5 & 5 & 2 & 2 & 2 \\ 6 & 6 & 6 & 3 & 3 & 3 \\ \hline \end{array}.$$

$$p_3 = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 5 & 6 & 2 & 3 & 1 \\ \hline 5 & 6 & 4 & 1 & 2 & 3 \\ \hline 6 & 4 & 5 & 3 & 1 & 2 \\ \hline \end{array}, \quad p_4 = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ \hline 5 & 6 & 4 & 2 & 3 & 1 \\ \hline 6 & 4 & 5 & 3 & 1 & 2 \\ \hline \end{array},$$

$$p_5 = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ \hline 5 & 6 & 4 & 3 & 1 & 2 \\ \hline 6 & 4 & 5 & 2 & 3 & 1 \\ \hline \end{array}.$$

A computation shows that

$$\text{Stab}_{G^*}(p_1) = \{id_I\},$$

$$\text{Stab}_{G^*}(p_2) = \langle (14)(25)(36) \rangle \cong C_2,$$

$$\text{Stab}_{G^*}(p_3) = \langle (123)(456) \rangle \cong C_3,$$

$$\text{Stab}_{G^*}(p_4) = \langle (153426) \rangle \cong C_6,$$

$$\text{Stab}_{G^*}(p_5) = \{id_I, (123)(456), (132)(465), (14)(26)(35), (15)(24)(36), (16)(25)(34)\} \cong \text{Sym}(\llbracket 3 \rrbracket).$$

In light of Proposition 4, preference profiles with large stabilizers are crucial for establishing impossibility results. Indeed, if $p_1, p_2 \in \mathcal{P}$ are such that $\text{Stab}_{G^*}(p_1) \supseteq \text{Stab}_{G^*}(p_2)$, by (10), we get that $C^U(p_1) \subseteq C^U(p_2)$, for all $U \leq G^*$. As a consequence, $C^U(p_1) \cap F(p_1) \subseteq C^U(p_2) \cap F(p_2)$ and so p_1 is a better candidate than p_2 to get $C^U(p_1) \cap F(p_1) = \emptyset$.

By Propositions 16 and 11(ii), we know that the size of a stabilizer cannot be larger than $2n$. Propositions 17 and 18 shows that such an upper bound can be reached by a stabilizer that is cyclic. Moreover, in the odd case, an additional property can also be satisfied.

Proposition 17. *There exists $p \in \mathcal{P}$ such that $\text{Stab}_{G^*}(p)$ is generated by a $2n$ -cycle.*

Proof. Consider the $2n$ -cycle $\varphi := (1 \ n+1 \ 2 \ n+2 \ \dots \ n \ 2n) \in G^*$. We are going to exhibit $p \in \mathcal{P}$ such that $\text{Stab}_{G^*}(p) = \langle \varphi \rangle$. Note that φ is a $2n$ -cycle and $\varphi \in G^* \setminus G$. Thus $\varphi^2 \in G$ and clearly $\varphi^2 = \sigma\nu$, where $\sigma := (1 \ 2 \ \dots \ n) \in G_W$ and $\nu := (n+1 \ n+2 \ \dots \ 2n) \in G_M$. Note that $|\sigma| = |\nu| = n$; for every $x \in W$, $\sigma(x) = \varphi^2(x)$; for every $y \in M$, $\nu(y) = \varphi^2(y)$.

Define, for every $x \in W$,

$$p(x) := [\nu^{x-1}(n+1), \dots, \nu^{x-1}(2n)] \in \mathbf{L}(M),$$

and, for every $y \in M$,

$$p(y) := [\sigma^y(1), \dots, \sigma^y(n)] \in \mathbf{L}(W).$$

In order to prove that $\varphi \in \text{Stab}_{G^*}(p)$, we show that, for every $z \in I$, we have

$$\varphi p(z) = p(\varphi(z)). \quad (17)$$

Let us consider then $z \in I$. Assume first that $z \in W$. Then

$$\begin{aligned} \varphi p(z) &= \varphi[\nu^{z-1}(n+1), \dots, \nu^{z-1}(2n)] = \varphi[\varphi^{2z-2}(n+1), \dots, \varphi^{2z-2}(2n)] \\ &= [\varphi^{2z-1}(n+1), \dots, \varphi^{2z-1}(2n)]. \end{aligned}$$

On the other hand, we also have

$$\begin{aligned} p(\varphi(z)) &= p(n+z) = [\sigma^{n+z}(1), \dots, \sigma^{n+z}(n)] = [\sigma^z(1), \dots, \sigma^z(n)] \\ &= [\varphi^{2z}(1), \dots, \varphi^{2z}(n)] = [\varphi^{2z-1}\varphi(1), \dots, \varphi^{2z-1}\varphi(n)] \\ &= [\varphi^{2z-1}(n+1), \dots, \varphi^{2z-1}(2n)], \end{aligned}$$

and hence (17) follows.

Assume next that $z \in M$. Then, we have

$$\varphi p(z) = \varphi[\sigma^z(1), \dots, \sigma^z(n)] = \varphi[\varphi^{2z}(1), \dots, \varphi^{2z}(n)]$$

$$= [\varphi^{2z}(n+1), \dots, \varphi^{2z}(2n)].$$

In particular, we have $\varphi p(2n) = [n+1, \dots, 2n]$. On the other hand, for $n+1 \leq z < 2n$, we also have

$$p(\varphi(z)) = p(z-n+1) = [\nu^{z-n}(n+1), \dots, \nu^{z-n}(2n)]$$

$$= [\nu^z(n+1), \dots, \nu^z(2n)] = [\varphi^{2z}(n+1), \dots, \varphi^{2z}(2n)].$$

Finally, observe that $p(\varphi(2n)) = p(1) = [n+1, \dots, 2n] = \varphi p(2n)$. Thus, (17) is proved.

Now from $\text{Stab}_{G^*}(p) \geq \langle \varphi \rangle$, we deduce that $2n$ divides $|\text{Stab}_{G^*}(p)|$. By Propositions 16 and 11, we know that $|\text{Stab}_{G^*}(p)|$ divides $2n$ and so $\text{Stab}_{G^*}(p) = \langle \varphi \rangle$. $\square$

Proposition 18. *Let n be odd. Then there exists $p \in \mathcal{P}$ such that $\text{Stab}_{G^*}(p)$ is generated by a $2n$ -cycle $\varphi \in G^*$ with the property that, for every $z \in I$, $\text{Rank}_{p(z)}(\varphi^n(z)) = n$.*

Proof. Let $n \geq 3$ be odd. Consider the $2n$ -cycle $\varphi := (1 \ n+1 \ 2 \ n+2 \ \dots \ n \ 2n) \in G^*$. Note that, for every $x \in W$, we have $\varphi(x) = x+n$; for every $y \in M$, $\varphi(y)$ is equal to the unique element in $[y-n+1]_n \cap \llbracket n \rrbracket$.

We claim that, for every $x \in W$ odd, $\varphi^x(1) = n + \frac{x+1}{2} \in M$. We prove that by finite induction on x . Surely $\varphi(1) = n + \frac{1+1}{2} = n+1$. Assume that the thesis holds for an odd $x \leq n-2$ and show it for the next odd, that is, for $x+2$. Observe also that every $x \in W$ satisfies $\frac{x+1}{2} < \frac{x+3}{2} \leq n$, because $n \geq 3$. Those arithmetic considerations and the inductive assumption imply then that

$$\begin{aligned} \varphi^{x+2}(1) &= \varphi^2 \varphi^x(1) = \varphi^2 \left(n + \frac{x+1}{2} \right) = \varphi \left(\frac{x+1}{2} + 1 \right) = \varphi \left(\frac{x+3}{2} \right) \\ &= n + \frac{x+3}{2}, \end{aligned}$$

which concludes the proof of the claim. As a consequence, using the fact that n is odd, we get $\varphi^n(1) = \frac{3n+1}{2}$.

We claim next that, for every $x \in W$, $\varphi^{2(x-1)}(1) = x$. We prove that by finite induction on x , for $x \in W$. If $x = 1$, then $\varphi^{2(1-1)}(1) = \varphi^0(1) = id_I(1) = 1$. Assume that the thesis holds for $x \leq n-1$. Then, we have

$$\varphi^{2x}(1) = \varphi^2 \varphi^{2(x-1)}(1) = \varphi^2(x) = \varphi(n+x) = x+1,$$

and hence the thesis holds for $x+1$.

Define now $p \in \mathcal{P}$ as follows. Let $p(1) = \left[y_1, \dots, y_{n-1}, y_{n-1}, \frac{3n+1}{2} \right]$, where $y_1, \dots, y_{n-1} \in M$ are such that $M = \left\{ y_1, \dots, y_{n-1}, \frac{3n+1}{2} \right\}$. Define then, for every $x \in W$, $p(x) = \varphi^{2(x-1)}p(1)$ and, for every $y \in M$, $p(y) = \varphi^{2y-2n-1}p(1)$. We show that $\varphi \in \text{Stab}_{G^*}(p)$, that is, for every $z \in I$, we have

$$\varphi p(z) = p(\varphi(z)). \quad (18)$$

Let us consider $z \in I$. Assume first that $z \in W$. Then we have

$$\varphi p(z) = \varphi \varphi^{2(z-1)}p(1) = \varphi^{2z-1}p(1).$$

On the other hand, we also have

$$p(\varphi(z)) = p(n+z) = \varphi^{2(n+z)-2n-1}p(1) = \varphi^{2z-1}p(1),$$

and so (18) is satisfied.

Assume next that $z \in M$. Then, we have

$$\varphi p(z) = \varphi \varphi^{2z-2n-1}p(1) = \varphi^{2z-2n}p(1).$$

In particular, $\varphi p(2n) = p(1)$. On the other hand, we also have that $p(\varphi(z))$ equals the preferences, with respect to p , of the only individual in the set $[z-n+1]_n \cap \llbracket n \rrbracket$. Indeed, if $z = 2n$ that gives $p(\varphi(2n)) = p(1)$; if $n+1 \leq z \leq 2n-1$, that gives

$$p(\varphi(z)) = p(z-n+1) = \varphi^{2(z-n+1-1)}p(1) = \varphi^{2z-2n}p(1).$$

Hence (18) is proved.

Let now $z \in I$. We have to show that $\text{Rank}_{p(z)}(\varphi^n(z)) = n$. Assume first that $z \in W$. By definition of p and by the properties observed for φ , we have that

$$\text{Rank}_{p(z)}\left(\varphi^{2(z-1)}\left(\frac{3n+1}{2}\right)\right) = n,$$

and

$$\varphi^{2(z-1)}\left(\frac{3n+1}{2}\right) = \varphi^{2(z-1)}\varphi^n(1) = \varphi^n\varphi^{2(z-1)}(1) = \varphi^n(z).$$

Therefore, $\text{Rank}_{p(z)}(\varphi^n(z)) = n$. Assume next that $z \in M$. Observe that $\varphi^n \in G^* \setminus G$ and $|\varphi^n| = 2$. Consider then $x \in W$ such that $z = \varphi^n(x)$ and $x = \varphi^n(z)$. Since $\varphi^n \in \text{Stab}_{G^*}(p)$, we know that $p(z) = p(\varphi^n(x)) = \varphi^n p(x)$. Since $x \in W$, we know that $\text{Rank}_{p(x)}(\varphi^n(x)) = n$. Thus, we conclude that

$$\text{Rank}_{p(z)}(\varphi^n(z)) = \text{Rank}_{p(z)}(x) = \text{Rank}_{\varphi^n p(x)}(\varphi^n \varphi^n(x)) = \text{Rank}_{p(x)}(\varphi^n(x)) = n.$$

Now, from $\text{Stab}_{G^*}(p) \geq \langle \varphi \rangle$, we deduce that $2n$ divides $|\text{Stab}_{G^*}(p)|$. By Propositions 16 and 11, we know that $|\text{Stab}_{G^*}(p)|$ divides $2n$. As a consequence, $\text{Stab}_{G^*}(p) = \langle \varphi \rangle$. $\square$

Appendix D. Proofs of the results of Sections 4.3 and 5

In this section, we finally prove the results stated in Section 4.3 and Section 5. The proofs proposed strongly rely on the results proved in Appendix C.

First, note that, using (10), we have that, for every preference profile $p \in \mathcal{P}$,

$$C^{G^*}(p) = \{\mu \in C_{G^*}(\text{Stab}_{G^*}(p)) \cap (G^* \setminus G) : |\mu| = 2\}. \quad (19)$$

Proof of Theorem 1. Assume first that n is even and prove that there exists no resolute and G^* -symmetric matching mechanism. By Proposition 17, there exists $p \in \mathcal{P}$ such that $\text{Stab}_{G^*}(p) = \langle \varphi \rangle$, where φ is a $2n$ -cycle. By Corollary 2, we complete the proof by showing that $C^{G^*}(p) = \emptyset$. By Proposition 14(iv), recalling (19), we immediately have that $C^{G^*}(p) = \emptyset$.

Assume now that n is odd and prove that there exists a resolute and G^* -symmetric matching mechanism. By Corollary 2, it is sufficient to show that, for every $p \in \mathcal{P}$, $C^{G^*}(p) \neq \emptyset$. Let $p \in \mathcal{P}$ and let $S := \text{Stab}_{G^*}(p)$. By Proposition 16, S is semiregular. Thus, recalling (19) and Proposition 15, we immediately get $C^{G^*}(p) \neq \emptyset$. $\square$

Proof of Proposition 5. Assume that n is odd. By Proposition 4, it is sufficient to show that there exists $p \in \mathcal{P}$ such that $C^{G^*}(p) \cap MO(p) = \emptyset$. Since n is odd, by Proposition 18, we know that there exists $p \in \mathcal{P}$ such that $\text{Stab}_{G^*}(p) = \langle \varphi \rangle$, where $\varphi \in G^*$ is a $2n$ -cycle such that, for every $z \in I$, $\text{Rank}_{p(z)}(\varphi^n(z)) = n$. By Proposition 14(iii), we have that the unique element of order 2 in $C_{G^*}(\langle \varphi \rangle) \cap (G^* \setminus G)$ is φ^n . However, $\varphi^n \notin MO(p)$ and thus, recalling (19), we get $C^{G^*}(p) \cap MO(p) = \emptyset$. $\square$

In order to prove Theorem 3, we first need two preliminary results.

Proposition 19. Let $\varphi \in \mathcal{M}$. Then $\{\varphi^\nu \in \text{Sym}(I) : \nu \in G_M\} = \mathcal{M}$.

Proof. By Proposition 7, we know that $\{\varphi^\nu \in \text{Sym}(I) : \nu \in G_M\} \subseteq \mathcal{M}$. Consider now $\mu \in \mathcal{M}$. Define $\nu \in G_M$ by $\nu(x) = x$, for all $x \in W$, and $\nu(y) = \mu\varphi^{-1}(y)$, for all $y \in M$. Note that $\varphi^{-1} = \varphi$, $\mu^{-1} = \mu$. Moreover, $\nu^{-1}(x) = x$, for all $x \in W$, and $\nu^{-1}(y) = \varphi\mu^{-1}(y)$, for all $y \in M$. Then, we have that $\varphi^\nu = \mu$. Indeed, let $z \in I$. If $z \in W$, then

$$\varphi^\nu(z) = \nu\varphi\nu^{-1}(z) = \nu\varphi(z) = \mu\varphi^{-1}\varphi(z) = \mu(z).$$

If $z \in M$, then

$$\varphi^\nu(z) = \nu\varphi\nu^{-1}(z) = \nu\varphi\varphi\mu^{-1}(z) = \nu\mu^{-1}(z) = \nu\mu(z) = \mu(z).$$

Thus $\mu \in \{\varphi^\nu \in \text{Sym}(I) : \nu \in G_M\}$. $\square$

Proposition 20. Let $\varphi, \mu \in \mathcal{M}$. Then $\varphi\mu = \mu\varphi$ if and only if there exists $\nu \in G_M$ with $|\nu| \leq 2$ such that $\mu = \varphi^\nu$.

Proof. Assume that there exists $\nu \in G_M$ with $|\nu| \leq 2$ such that $\mu = \varphi^\nu$. Note that $\varphi = \varphi^{-1}$ and $\nu = \nu^{-1}$. We have to prove that, for every $z \in I$, $\varphi\mu(z) = \mu\varphi(z)$. Let $z \in I$. If $z \in W$, then

$$\varphi\mu(z) = \varphi\varphi^\nu(z) = \varphi\nu\varphi\nu^{-1}(z) = \varphi\nu\varphi(z) = \varphi\nu^{-1}\varphi(z) = \nu\varphi\nu^{-1}\varphi(z) = \mu\varphi(z).$$

If $z \in M$, then

$$\begin{aligned} \varphi\mu(z) &= \varphi\varphi^\nu(z) = \varphi\nu\varphi\nu^{-1}(z) = \varphi\varphi\nu^{-1}(z) = \nu^{-1}(z) = \nu(z) \\ &= \nu\varphi\varphi(z) = \nu\varphi\nu^{-1}\varphi(z) = \mu\varphi(z). \end{aligned}$$

Conversely, assume that $\varphi\mu = \mu\varphi$. By Proposition 19, we know that there exists $\nu \in G_M$ such that $\mu = \varphi^\nu$. Suppose, by contradiction, that $|\nu| \geq 3$. Then the cycle decomposition of ν contains a k -cycle γ , with $k \geq 3$, moving only men. Let $S \subseteq M$ be the support of γ and let $y_0 \in S$. Then $|S| = k$, $S = y_0^{(\gamma)}$, and $\gamma(y_0) \neq y_0$. We have that

$$\varphi\mu(y_0) = \varphi\nu\varphi\nu^{-1}(y_0) = \varphi\varphi\nu^{-1}(y_0) = \nu^{-1}(y_0) = \gamma^{-1}(y_0),$$

and

$$\mu\varphi(y_0) = \nu\varphi\nu^{-1}\varphi(y_0) = \nu\varphi\varphi(y_0) = \nu(y_0) = \gamma(y_0).$$

Since $\varphi\mu = \mu\varphi$, we must have $\gamma^{-1}(y_0) = \gamma(y_0)$. Thus, we deduce $\gamma^2(y_0) = y_0$ and so $\{y_0, \gamma(y_0)\} = y_0^{(\gamma)}$. It follows that $S = \{y_0, \gamma(y_0)\}$ and therefore $k = 2$, a contradiction. $\square$

Proof of Theorem 3. Let $\varphi \in \mathcal{M}$. Since WPO is a G^* -symmetric matching mechanism, we have that WPO is a $\langle \varphi \rangle$ -symmetric matching mechanism. By Proposition 4, it is sufficient to show that, for every $p \in \mathcal{P}$, $C^{(\varphi)}(p) \cap WPO(p) \neq \emptyset$. Consider then $p \in \mathcal{P}$. Since $|\varphi| = 2$, the only subgroups of $\langle \varphi \rangle$ are the trivial subgroup $\{id_I\}$ and $\langle \varphi \rangle$ itself. Thus, $\text{Stab}_{(\varphi)}(p) \in \{\{id_I\}, \langle \varphi \rangle\}$. If $\text{Stab}_{(\varphi)}(p) = \{id_I\}$, then $C^{(\varphi)}(p) = \mathcal{M}$; therefore $C^{(\varphi)}(p) \cap WPO(p) = WPO(p) \neq \emptyset$. Assume then that $\text{Stab}_{(\varphi)}(p) = \langle \varphi \rangle$. By Proposition 20, we know that

$$C^{(\varphi)}(p) = \{\mu \in \mathcal{M} : \exists \nu \in G_M \text{ with } |\nu| \leq 2 \text{ such that } \mu = \varphi^\nu\}.$$

In particular, $\varphi \in C^{(\varphi)}(p)$. Let $y_1 \in M$ be the first ranked man in $p(1)$. If $\varphi(1) = y_1$, then $\varphi \in C^{(\varphi)}(p) \cap WPO(p) \neq \emptyset$. If $\varphi(1) = y_0 \neq y_1$, consider $\nu = (y_0 y_1) \in G_M$. Note that $|\nu| = 2$ and that $\varphi^\nu(1) = \nu\varphi(1) = \nu(y_0) = y_1$. Thus, $\varphi^\nu \in C^{(\varphi)}(p) \cap WPO(p) \neq \emptyset$. $\square$

Proof of Theorem 4. Assume $n = 2$ and let $\varphi \in \mathcal{M}$. We have that $\mathcal{M} = \{\mu_1, \mu_2\}$, where $\mu_1 := (13)(24)$ and $\mu_2 := (14)(23)$. Note that $\mu_1\mu_2 = \mu_2\mu_1$. Thus, for every $p \in \mathcal{P}$, we have that $C^{(\varphi)}(p) = \mathcal{M}$. As a consequence, for every $p \in \mathcal{P}$, $C^{(\varphi)}(p) \cap ST(p) = ST(p) \neq \emptyset$. Then, by Proposition 4, we conclude that there exists a resolute, stable and $\langle \varphi \rangle$ -symmetric matching mechanism. $\square$

Proof of Theorem 5. Assume $n \geq 3$ and let $\varphi \in \mathcal{M}$. Define, for every $x \in W = \llbracket n \rrbracket$, $y_x := \varphi(x)$. Then, $M = \{y_x : x \in \llbracket n \rrbracket\}$. Let $p \in \mathcal{P}$ be defined by

$$p(1) = [y_2, y_3, y_1, (y_4), \dots, (y_n)], \quad p(y_1) = [2, 3, 1, (4), \dots, (n)],$$

$$p(2) = [y_3, y_1, y_2, (y_4), \dots, (y_n)], \quad p(y_2) = [3, 1, 2, (4), \dots, (n)],$$

$$p(3) = [y_1, y_2, y_3, (y_4), \dots, (y_n)], \quad p(y_3) = [1, 2, 3, (4), \dots, (n)],$$

and, for every $x \in \llbracket n \rrbracket$ with $x \geq 4$, if any,

$$p(x) = \sigma^{x-1}[y_1, y_2, y_3, (y_4), \dots, (y_n)], \quad p(y_x) = \sigma^{x-1}[1, 2, 3, (4), \dots, (n)],$$

where $\sigma = (12 \dots n)(y_1 y_2 \dots y_n)$. It is immediate to check that $p^\varphi = p$, and thus $\varphi \in \text{Stab}_{G^*}(p)$. Using Proposition 4, we complete the proof by showing that $C^{(\varphi)}(p) \cap ST(p) = \emptyset$. Let $\gamma_1, \dots, \gamma_6 \in \text{Sym}(I)$ be defined by

$$\gamma_1 = (1 y_1)(2 y_2)(3 y_3), \quad \gamma_2 = (1 y_1)(2 y_3)(3 y_2) \quad \gamma_3 = (1 y_2)(2 y_1)(3 y_3),$$

$$\gamma_4 = (1 y_3)(2 y_2)(3 y_1), \quad \gamma_5 = (1 y_2)(2 y_3)(3 y_1), \quad \gamma_6 = (1 y_3)(2 y_1)(3 y_2),$$

and let $\gamma^* = (4 y_4) \cdots (n y_n) \in \text{Sym}(I)$ if $n \geq 4$, while $\gamma^* = id_I$ if $n = 3$. For every $i \in \llbracket 6 \rrbracket$, set $\mu_i = \gamma_i \gamma^* \in \mathcal{M}$. Note that $\varphi = \mu_1$ and that

$$\{\mu \in \mathcal{M} : \forall x \in \llbracket n \rrbracket \text{ with } x \geq 4, \mu(x) = y_x\} = \{\mu_1, \dots, \mu_6\}.$$

It is simple to verify that $ST(p) \subseteq \{\mu_1, \dots, \mu_6\}$. Indeed, consider $\mu \in \mathcal{M} \setminus \{\mu_1, \dots, \mu_6\}$. Then, there exists $x \in \llbracket n \rrbracket$ with $x \geq 4$ such that $\mu(x) \neq y_x$. Thus, μ is blocked by (x, y_x) and so $\mu \notin ST(p)$. Observe now that μ_1 is blocked by $(1, y_2)$; μ_2 is blocked by $(1, y_3)$; μ_3 is blocked by $(3, y_2)$; μ_4 is blocked by $(2, y_1)$. As a consequence, $ST(p) \subseteq \{\mu_5, \mu_6\}$. However, $C^{(\varphi)}(p) \cap \{\mu_5, \mu_6\} = \emptyset$ because both μ_5 and μ_6 do not commute with $\varphi \in \text{Stab}_{G^*}(p)$. Indeed, $\mu_5 \varphi(1) = \gamma_5 \gamma^*(y_1) = \gamma_5(y_1) = 3$ and $\varphi \mu_5(1) = \varphi \gamma_5(1) = 2$, and so $\mu_5 \varphi(1) \neq \varphi \mu_5(1)$; $\mu_6 \varphi(1) = \gamma_6 \gamma^*(y_1) = \gamma_6(y_1) = 2$ and $\varphi \mu_6(1) = \varphi \gamma_6(1) = \varphi(y_3) = 3$, and so $\mu_6 \varphi(1) \neq \varphi \mu_6(1)$. As a consequence, we also have that $C^{(\varphi)}(p) \cap ST(p) = \emptyset$ and this completes the proof. $\square$

Proof of Theorem 6. Suppose by contradiction that there exists a resolute, G^* -symmetric and Pareto optimal generalized matching mechanisms F . Let us denote by $\bar{\mathcal{P}}_*$ the set of the generalized preference profiles $\bar{p}$ such that, for every $x \in W$ and $y \in M$, $y \succ_{\bar{p}(x)} x$ and $x \succ_{\bar{p}(y)} y$. Thus, we have that $\bar{p} \in \bar{\mathcal{P}}_*$ if, for every individual, being unmatched is the worst possible option.

We claim that, for every $\bar{p} \in \bar{\mathcal{P}}_*$, $\bar{F}(\bar{p}) \subseteq \mathcal{M}$. Indeed, assume by contradiction that there exists $\bar{p} \in \bar{\mathcal{P}}_*$ and $\bar{\mu} \in \bar{\mathcal{M}} \setminus \mathcal{M}$ such that $\bar{F}(\bar{p}) = \{\bar{\mu}\}$. Thus, there exists $z \in I$ such that $\bar{\mu}(z) = z$. If $\bar{\mu} = id_I$, then, considering any $x \in W$, $y \in M$ and $\bar{\mu}' = (xy) \in \bar{\mathcal{M}}$, we have that $\bar{\mu}'(x) = y \succ_{\bar{p}(x)} x = \bar{\mu}(x)$, $\bar{\mu}'(y) = x \succ_{\bar{p}(y)} y = \bar{\mu}(y)$, and $\bar{\mu}'(z) = \bar{\mu}(z) = z$ for all $z \in I \setminus \{x, y\}$. In particular, $\bar{\mu}$ is not Pareto optimal for $\bar{p}$, and $\bar{F}$ is not Pareto optimal, a contradiction. If $\bar{\mu} \neq id_I$, then the properties of $\bar{\mu}$ guarantees that $\bar{\mu}$ is product of 2-cycles whose support contains an element of W and an element of M . As a consequence, the set $J = \{z \in I : \bar{\mu}(z) = z\}$ is nonempty and contains at least an element of W and at least an element of M . Consider then $x \in W \cap J$, $y \in M \cap J$ and $\bar{\mu}' = (xy)\bar{\mu} \in \bar{\mathcal{M}}$. We have that $\bar{\mu}'(x) = y \succ_{\bar{p}(x)} x = \bar{\mu}(x)$, $\bar{\mu}'(y) = x \succ_{\bar{p}(y)} y = \bar{\mu}(y)$, and $\bar{\mu}'(z) = \bar{\mu}(z)$ for all $z \in I \setminus \{x, y\}$. In particular, $\bar{\mu}$ is not Pareto optimal for $\bar{p}$, and $\bar{F}$ is not Pareto optimal, a contradiction.

Consider now $\Phi : \mathcal{P} \rightarrow \bar{\mathcal{P}}_*$ that associates with any $p \in \mathcal{P}$ the unique element $\Phi(p)$ of $\bar{\mathcal{P}}_*$ such that: for every $x \in W$ and $y_1, y_2 \in M$, $y_1 \succ_{\Phi(p)(x)} y_2$ if and only if $y_1 \succ_{p(x)} y_2$; for every $y \in M$ and $x_1, x_2 \in W$, $x_1 \succ_{\Phi(p)(y)} x_2$ if and only if $x_1 \succ_{p(y)} x_2$; for every $x \in W$ and $y \in M$, $y \succ_{\Phi(p)(x)} x$ and $x \succ_{\Phi(p)(y)} y$. Having in mind the tables representing the elements of $\mathcal{P}$ and $\bar{\mathcal{P}}$, $\Phi(p)$ is built from the table associated with p by simply adding at the bottom of each column the name of the corresponding individual. It can be easily shown that Φ is a bijection and that, for every $p \in \mathcal{P}$ and $\varphi \in G^*$, $\Phi(p^\varphi) = \Phi(p)^\varphi$.

Let us consider the matching mechanism F defined, for every $p \in \mathcal{P}$, by $F(p) = \bar{F}(\Phi(p))$. It is a cumbersome exercise to show that F is resolute, G^* -symmetric and Pareto optimal. Such a fact, by means of Proposition 1, contradicts Theorem 2. $\square$

Data availability

No data was used for the research described in the article.

References

- Abdulkadiroğlu, A., Sönmez, T., 2003. School choice: A mechanism design approach. *Am. Econ. Rev.* 93, 729–747.
 Bartholdi, L., Hann-Caruthers, W., Josyula, M., Tamuz, O., Yariv, L., 2021. Equitable voting rules. *Econometrica* 89, 563–589.

- Berczky, Á., Maròti, A., 2008. On groups with every normal subgroup transitive or semiregular. *J. Algebra* 319, 1733–1751.
 Bubboloni, D., Gori, M., 2014. Anonymous and neutral majority rules. *Soc. Choice Welf.* 43, 377–401.
 Bubboloni, D., Gori, M., 2015. Symmetric majority rules. *Math. Social Sci.* 76, 73–86.
 Bubboloni, D., Gori, M., 2016. Resolute refinements of social choice correspondences. *Math. Social Sci.* 84, 37–49.
 Bubboloni, D., Gori, M., 2021. Breaking ties in collective decision-making. *Decis. Econ. Finance* 44, 411–457.
 Bubboloni, D., Gori, M., 2025. A generalization to networks of Young's characterization of the Borda rule. *Ann. Oper. Res.* <http://dx.doi.org/10.1007/s10479-025-06593-w>.
 Cooper, F., Manlove, D., 2020. Algorithms for new types of fair stable matchings. In: 18th International Symposium on Experimental Algorithms (SEA 2020). *Leibniz International Proceedings in Informatics (LIPIcs)*, Volume 160. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 20:1–20:13.
 Doğan, O., Giritligil, A.E., 2015. Anonymous and neutral social choice: existence results on resoluteness. Murat Sertel Center for Advanced Economic Studies, Working paper series 2015-01.
 Endriss, U., 2020. Analysis of one-to-one matching mechanisms via SAT solving: Impossibilities for universal axioms. In: The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI-20). pp. 1–8.
 Eğecioğlu, Ö., 2009. Uniform generation of anonymous and neutral preference profiles for social choice rules. *Monte Carlo Methods Appl.* 15, 241–255.
 Eğecioğlu, Ö., Giritligil, A.E., 2013. The impartial, anonymous, and neutral culture model: a probability model for sampling public preference structures. *J. Math. Sociol.* 37, 203–222.
 Gale, D., Shapley, L.S., 1962. College admissions and the stability of marriage. *Am. Math. Mon.* 69, 9–15.
 Gusfield, D., Irving, R.W., 1989. The Stable Marriage Problem: Structure and Algorithms. The MIT Press.
 Halaburda, H., 2010. Unravelling in two-sided matching markets and similarity of preferences. *Games Econ. Behav.* 69, 365–393.
 Kivinen, S., 2023. On the manipulability of equitable voting rules. *Games Econ. Behav.* 141, 286–302.
 Kivinen, S., 2024. Equitable, neutral, and efficient voting rules. *J. Math. Econom.* 115, 103061.
 Klaus, B., Klijn, F., 2006. Procedurally fair and stable matching. *Econom. Theory* 27, 431–447.
 Knuth, D.E., 1976. *Mariages Stables Et Leurs Relations Avec D'Autres Problèmes Combinatoires*. Les Presses de l'Université de Montreal, Montreal.
 Kovács, I., Malnič, A., Marušič, D., Miklavčič, Š., 2015. Transitive group actions: (im)primitivity and semiregular groups. *J. Algebraic Combin.* 41, 867–885.
 Masarani, F., Gokturk, S.S., 1989. On the existence of fair matching algorithms. *Theory and Decision* 26, 305–322.
 Maynard, P., Siemons, J., 2002. On the reconstruction index of the permutation groups: semiregular groups. *Aequationes Math.* 64, 218–231.
 Milne, J.S., 2021. Group theory. Available at www.jmilne.org/math/CourseNotes/GT.pdf.
 Miyagawa, E., 2002. Strategy-proofness and the core in house allocation problems. *Games Econ. Behav.* 38, 347–361.
 Nizamogullari, D., Özkal-Sanver, İ., 2014. Characterization of the core in full domain marriage problems. *Math. Social Sci.* 69, 34–42.
 Özkal-Sanver, İ., 2004. A note on gender fairness in matching problems. *Math. Social Sci.* 47, 211–217.
 Robinson, D.J.S., 1996. *A Course in the Theory of Groups*. Graduate Texts in Mathematics 80. Springer New York.
 Romero-Medina, A., 2001. “Sex-equal” stable matchings. *Theory and Decision* 150, 197–212.
 Root, J., Bade, S., 2023. Royal processions: Incentives, efficiency and fairness in two-sided matching. In: *Proceedings of the 24th ACM Conference on Economics and Computation*. p. 1077, Full version of the paper at <https://arxiv.org/abs/2301.13037>.
 Roth, A.E., 1984. The evolution of the labor market for medical interns and residents: a case study in game theory. *J. Political Econ.* 92, 991–1016.
 Roth, A.E., 1991. A natural experiment in the organization of entry-level labor markets: Regional markets for new physicians and surgeons in the United Kingdom. *Am. Econ. Rev.* 81, 415–440.
 Roth, M.A., 1990. *Two-Sided Matchings. A Study in Game-Theoretic Modeling and Analysis*. Cambridge University Press.
 Sasaki, H., Toda, M., 1992. Consistency and characterization of the core of two-sided matching problems. *J. Econom. Theory* 56, 218–227.