# MIT Open Access Articles

## *Strategy-proofness of the randomized Condorcet voting system*

# Strategy-Proofness of the Randomized Condorcet Voting System

**Lê Nguyên Hoang**

**Abstract** In this paper, we study the strategy-proofness properties of the randomized Condorcet voting system (RCVS). Discovered at several occasions independently, the RCVS is arguably the natural extension of the Condorcet method to cases where a deterministic Condorcet winner does not exists. Indeed, it selects the always-existing and essentially unique Condorcet winner of lotteries over alternatives. Our main result is that, in a certain class of voting systems based on pairwise comparisons of alternatives, the RCVS is the only one to be Condorcet-proof. By Condorcet-proof, we mean that, when a Condorcet winner exists, it must be selected and no voter has incentives to misreport his preferences. We also prove two theorems about group-strategy-proofness. On one hand, we prove that there is no group-strategy-proof voting system that always selects existing Condorcet winners. On the other hand, we prove that, when preferences have a one-dimensional structure, the RCVS is group-strategy-proof.

**Keywords** Social choice · Condorcet winner · Strategy-proofness

## 1 Introduction

Social choice theory consists in choosing an alternative for a group of people whose individual preferences may greatly differ from one another. One of the first mathematicians to address this question was Condorcet (1785). Condorcet argued that an alternative that is preferred to any other by the majority should always be selected. Such an alternative is now known as a *Condorcet winner*. Unfortunately, Condorcet went on proving that a Condorcet winner does not necessarily exist, as he provided an example where the majority prefers $x$ to $y$, $y$ to $z$ and $z$ to $x$. This example is now known as a Condorcet paradox.

MIT, EECS,
77 Massachusetts Ave, Cambridge, MA, USA,
E-mail: lenhoang@mit.edu

It has been the essence of several impossibility theorems since. Namely, first, Arrow (1951) famously derived the impossibility of a "fair" aggregation of the preferences of the individuals into a preference of the group. Second, Gibbard (1973) and Satterthwaite (1975) proved that there is no strategy-proof, anonymous neutral and deterministic voting system. A similar result has been proved by Campbell and Kelly (1998) about the impossibility of combining the Condorcet principle with strategy-proofness for deterministic social choice rules that select one or two alternatives. Third, Gibbard (1977, 1978) proved that random dictatorship was the only strategy-proof, anonymous, neutral and unanimous voting system, assuming voters' preferences satisfy the Von Neumann and Morgenstern (1944) axioms.

Nevertheless, a natural extension of the concept of Condorcet winner to lotteries has been introduced and widely studied by Kreweras (1965), Fishburn (1984), Felsenthal and Machover (1992), Laslier (1997), Laslier (2000), Brandl et al (2016b), and relies on a remarkable existence and near-uniqueness theorem proved independently by Fisher and Ryan (1992) and Laffond et al (1993). Namely, it was proved that, provided there is no tie between any two alternatives, and given a specific but natural extension of majority preferences over candidates to preferences over lotteries, there always is a unique lottery that the majority likes at least as much as any other lottery. We call such a lottery the Condorcet winner of lotteries, or the randomized Condorcet winner. Naturally, it is this randomized Condorcet winner that we propose to select through the randomized Condorcet voting system (RCVS)[1]. The compelling naturalness of the RCVS has been further supported by Brandl et al (2016b) who characterized it as the only voting system satisfying two consistency axioms. What is perhaps most exciting is the recent implementation of the RCVS on the website `https://pnyx.dss.in.tum.de`. In Section 2, we quickly redefine the RCVS and stress its naturalness.

In addition to this naturalness, the RCVS has been proved to possess appealing Pareto-efficiency properties[2]. Indeed, Aziz et al (2013) proved that random dictatorship and RCVS are two extreme points of a tradeoff between Pareto-efficiency and strategy-proofness. Loosely, random dictatorship is, in some sense related to the class of preferences considered[3], more strategy-proof but less Pareto-efficient. Moreover, Aziz et al (2013, 2014) prove that, to a

---

[1] This voting system has been given different names in previous papers, including "game-theory method" in Felsenthal and Machover (1992) which is not to be confused with the slightly different game-theory method by Rivest and Shen (2010), "symmetric two-party competition game equilibrium" in Laslier (2000); Myerson (1996), "maximal lottery" in Fishburn (1984); Aziz et al (2013); Brandl et al (2016b) and "Fishburn's rule" on `https://pnyx.dss.in.tum.de`. Note that some of these papers also study variants where the margin by which an alternative $x$ is preferred to $y$ is taken into account (whereas, here, only the fact that is the majority prefers $x$ matters). Finally, it should be added that the (support of the) RCVS has also been studied under the names "bipartisan set" and "essential set". We believe, however, that our terminology yields greater insight into the nature of this lottery.

[2] A voting system is Pareto-efficiency if there is no lottery $\tilde{x}$ such that everyone likes $\tilde{x}$ at least as much as the selected lottery, and someone strictly prefers $\tilde{x}$ to the selected lottery.

[3] There are several possible ways to extend preferences over alternatives to preferences over lotteries, each leading to its own concepts of strategy-proofness and Pareto-efficiency.

large extent, strategy-proofness and Pareto-efficiency are incompatible, which suggests that the RCVS can hardly be improved upon with respect to such considerations. These results have been further generalized by Brandl et al (2016a).

Unfortunately, the theorem by Gibbard (1977) implies that the RCVS is not strategy-proof for von Neumann - Morgenstern preferences. The proof of this, along with many similar results, relies on the concept of first-order stochastic dominance, which allows to capture the whole diversity of von Neumann - Morgenstern preferences. In particular, the harshness of Gibbard (1977)'s result is precisely due to how constraining first-order stochastic dominance is. Thus, if we relax this condition, we may be able to prove the (thus weaker) strategy-proofness of some voting systems that are not random dictatorships. This is what has been proposed by Bogomolnaia and Moulin (2001) and Balbuzanov (2016), who respectively introduced ordinal efficiency and convex undomination. In this paper, we shall take another path, by studying a very distinct (but still fairly natural) class of preferences based on pairwise comparisons of drawn alternatives, which was previously introduced by Fishburn (1982) and Aziz et al (2015).

The main contribution of this paper is to show that, for this class of pairwise comparison preferences, the RCVS possesses enviable strategy-proofness properties. We prove that the RCVS is Condorcet-proof, in the sense that, when a Condorcet winner exists, the RCVS selects it and no voter has incentives to misreport his preferences. We shall also show that, in a certain class of voting systems based on pairwise comparisons of alternatives, the RCVS is the only one that is Condorcet-proof. These properties are formally stated and derived in Section 3. We shall argue that they are strong indications that the RCVS has key properties that should favor its use over other voting systems.

Next, in Section 4, we study the group strategy-proofness of voting systems. We start with an impossibility result that asserts that no voting system that selects Condorcet winners is group strategy-proof. Next and finally, we restrict ourselves to the cases where alternatives range on a one-dimensional axis, which is mathematically described by two models known as *single-peakedness* and *single-crossing*. It is well-known that, under these models, Condorcet winners are guaranteed to exist (Black (1958); Roberts (1977); Rothstein (1990, 1991); Gans and Smart (1996)). While the median social rule introduced by Moulin (1980) and generalized by Saporiti (2009) guarantees strategy-proofness for one-dimensional preferences, it requires to explicitly and officially locate alternatives on a one-dimensional line, and to forbid voters' ballots to be inconsistent with the assumed corresponding one-dimensional structure of preferences. In many cases, like in politics, this may not be acceptable. However, Penn et al (2011) proved that, when preferences are single-peaked but ballots are not constrained to be single-peaked, a deterministic group-strategy-proof voting system must be dictatorial. We shall prove that, under single-peakedness or single-crossing preferences, the RCVS is group-strategy-proof.

Finally, Section 5 concludes by emphatically recommending the use of the RCVS in practice.

## 2 The Randomized Condorcet Voting System

In this section, we briefly reintroduce the RCVS, which was repeatedly discovered in the literature. We consider a finite set $X$ of alternatives. A preference $\theta \in \mathcal{O}$ is an order[4] over $X$. For simplicity, we shall restrict our analysis to total order preferences, but there is no difficulty in generalizing our results to partial orders. We denote $\theta : x \succ y$ the fact that a voter with preference $\theta$ prefers alternative $x$ to $y$. The anonymous preferences of a population of voters can then be represented as a probability distribution $\tilde{\theta} \in \Delta(\mathcal{O})$ over preferences. Note that this representation of the preferences of a population does not discriminate certain distinct settings, e.g. a population and two copies of this population. However, it has the advantage of modeling as well situations where different voters have different weights, e.g. in a company board of directors. Now, we say that the majority $M_{\tilde{\theta}}$ prefers $x$ to $y$ if more people prefer $x$ to $y$, i.e.

$$M_{\tilde{\theta}} : x \gg y \quad \stackrel{\triangle}{\Longleftrightarrow} \quad \mathbb{P}_{\theta \sim \tilde{\theta}} \left[ \theta : x \succ y \right] > \mathbb{P}_{\theta \sim \tilde{\theta}} \left[ \theta : x \prec y \right],$$

where $\mathbb{P}_{\theta \sim \tilde{\theta}}[\cdot]$ is the probability of an event "$\cdot$" regarding a random voter $\theta$ drawn from the population $\tilde{\theta}$. For convenience of notation, we use probability notations for quantities often rather regarded as frequencies. The line above can equivalently be read as the probability that a random voter prefers $x$ to $y$ is greater than the probability that he prefers $y$ to $x$, or as the fraction of voters who prefer $x$ to $y$ being greater than the fraction of voters who prefer $y$ to $x$.

We shall use the notation "$\geqslant$" instead of "$\gg$" when the right-hand inequality features the greater-or-equal sign "$\geq$".

*Example 1* Consider $X = \{x, y, z\}$, and $\tilde{\theta} \in \Delta(\mathcal{O})$ defined by:

$$\mathbb{P}_{\theta \sim \tilde{\theta}} \left[ \theta : x \succ y \succ z \right] = 27/100,$$
$$\mathbb{P}_{\theta \sim \tilde{\theta}} \left[ \theta : z \succ x \succ y \right] = 31/100,$$
$$\mathbb{P}_{\theta \sim \tilde{\theta}} \left[ \theta : y \succ x \succ z \right] = 42/100.$$

We then have $M_{\tilde{\theta}} : x \gg y \gg z \gg x$, which proves that the majority preference $M_{\tilde{\theta}}$ is not transitive and that there is no Condorcet winner. This is the infamous Condorcet paradox.

---

[4] An order is a binary relation that satisfies the following properties, for all $x, y, z \in X$:

- Antisymmetry: if $\theta : x \succeq y$ and $\theta : y \succeq x$, then $x = y$.
- Transitivity: if $\theta : x \succeq y$ and $\theta : y \succeq z$, then $\theta : x \succeq z$.

If, in addition, the order satisfies totality, i.e. $\theta : x \succeq y$ or $\theta : y \succeq x$, then we say that the order is total.

Given the limitations of deterministic voting systems proved by Gibbard (1973), Satterthwaite (1975) and Penn et al (2011), we turn our attention to randomized voting systems, which have been gaining interests in recent years (see, e.g. Ehlers et al (2002); Bogomolnaia et al (2005); Chatterji et al (2014)). Instead of selecting an alternative, a randomized voting system selects a lottery $\tilde{x} \in \Delta(X)$, that is, a probability distribution over alternatives. A crucial difficulty posed by the introduction of randomness in social choice theory is the extension of preferences over deterministic alternatives to preferences over lotteries. To introduce and justify the randomized Condorcet voting system, it turns out to be sufficient to extend the majority preferences. We do this as follows. We say that the majority $M_{\tilde{\theta}}$ prefers a lottery $\tilde{x}$ to a lottery $\tilde{y}$, if the majority more often prefers the alternative drawn by $\tilde{x}$ to the one drawn by $\tilde{y}$, than the other way around, i.e.

$$M_{\tilde{\theta}} : \tilde{x} \gg \tilde{y} \quad \stackrel{\triangle}{\iff} \quad \mathbb{P}_{x \sim \tilde{x}, y \sim \tilde{y}} \left[ M_{\tilde{\theta}} : x \gg y \right] > \mathbb{P}_{x \sim \tilde{x}, y \sim \tilde{y}} \left[ M_{\tilde{\theta}} : x \ll y \right],$$

where, as earlier, the notation $x \sim \tilde{x}$ means that we are drawing $x$ from the probability distribution $\tilde{x}$. This extension of majority preferences to lotteries shares strong similarities with the SSB preferences axiomatized by Fishburn (1982), and even more with the pairwise comparison preferences studied by Aziz et al (2014). We stress, however, that the majority preference $M_{\tilde{\theta}}$ need not be transitive over deterministic alternatives, which is evidently the essence of the Condorcet paradox. Nevertheless, we argue that this extension of majority preferences over alternatives to majority preferences over lotteries is fairly natural, especially given that we assume to only have access to ordinal preferences of the voters.

The definition of majority preferences over lotteries can also be stated in terms of an inequality with matrices. First, for any preferences $\tilde{\theta}$ of the people, let us define the referendum matrix $\mathcal{R}(\tilde{\theta}) \in \mathbb{R}^{X \times X}$ by

$$\mathcal{R}_{xy}(\tilde{\theta}) \triangleq \mathbb{P}_{\theta \sim \tilde{\theta}} [\theta : x \succ y] - \mathbb{P}_{\theta \sim \tilde{\theta}} [\theta : y \succ x].$$

Intuitively, $\mathcal{R}_{xy}(\tilde{\theta})$ counts the relative proportion of voters that prefer $x$ over $y$, and thus, the hypothetical result of a referendum opposing $x$ to $y$.

Now, let us define $A(M_{\tilde{\theta}}) \in \mathbb{R}^{X \times X}$ the skew-symmetric matrix that only remembers the signs of the entries of the referendum matrix. In other words, $A(M_{\tilde{\theta}})$ is defined by

$$A_{xy}(M_{\tilde{\theta}}) = \begin{cases} +1, & M_{\tilde{\theta}} : x \gg y, \\ -1, & M_{\tilde{\theta}} : x \ll y, \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, we can represent any lottery $\tilde{x}$ by a vector $p(\tilde{x}) \in \mathbb{R}^X$ defined by $p_x(\tilde{x}) = \mathbb{P}_{y \sim \tilde{x}}[x = y]$. Then,

$$M_{\tilde{\theta}} : \tilde{x} \gg \tilde{y} \quad \iff \quad p(\tilde{x})^T A(M_{\tilde{\theta}}) p(\tilde{y}) > 0,$$

Like earlier, we shall use the symbol "$\geqq$" when the right-hand side inequality features the greater-or-equal sign.

*Remark 1* The definition of the majority preferences $M_{\tilde{\theta}}$ over lotteries is not to be confused with the fact that a random voter will more likely prefer $\tilde{x}$ to $\tilde{y}$, nor with the fact that a random voter will more likely prefer a random alternative drawn from $\tilde{x}$ to one drawn from $\tilde{y}$.

*Example 2* Let us reconsider Example 1. Recall that $M_{\tilde{\theta}} : x \gg y \gg z \gg x$. Consider the lottery $\tilde{p}$ that assigns probability $2/3$ to $x$ and $1/3$ to $y$, which we shall compare to $z$ (or, equivalently, the lottery $\delta_z$ which assigns probability 1 to $z$). Then, $\mathbb{P}_{p \sim \tilde{p}}[M_{\tilde{\theta}} : p \gg z] = \mathbb{P}_{p \sim \tilde{p}}[p = y] = 1/3$, while $\mathbb{P}_{p \sim \tilde{p}}[M_{\tilde{\theta}} : z \gg p] = \mathbb{P}_{p \sim \tilde{p}}[p = x] = 2/3$. In other words, two out of three times, the majority will prefer the alternative $z$ to the one drawn by $\tilde{p}$, while only one third of the times it will prefer the alternative drawn by $\tilde{p}$ to $z$. Therefore, the majority prefers $z$ to $\tilde{p}$, i.e. $M_{\tilde{\theta}} : z \gg \tilde{p}$.

Finally, we can generalize the concept of Condorcet winners of alternatives to Condorcet winners of lotteries. We say that a lottery $\tilde{x}$ is a randomized Condorcet winner if there is no other lottery that the majority prefers, i.e. such that

$$\forall \tilde{y} \in \Delta(X), \quad M_{\tilde{\theta}} : \tilde{x} \gtrapprox \tilde{y}.$$

This definition of the majority preferences over lotteries then allows to circumvent the Condorcet paradox in a very natural way, which relies on the following restatement of a well-known theorem.

**Theorem 1 (Fisher and Ryan (1992); Felsenthal and Machover (1992); Laffond et al (1993))** *There always exists a randomized Condorcet winner. Plus, if there is no tie between any two alternatives, the randomized Condorcet winner is unique.*

On one hand, the proofs of this theorem are not very constructive nor insightful. For instance, the existence is derived from the minimax theorem by Von Neumann (1928) or the Nash (1951) theorem. On the other hand, though, the randomized Condorcet winner can be efficiently computed. Indeed, the set of randomized Condorcet winners is actually a polytope, whose variables are the probabilities of selecting the different alternatives, and whose constraints assert that the majority must like the randomized Condorcet winners at least as much as any deterministic alternative. Thus, a randomized Condorcet winner can be computed by solving a basic LP with $O(|X|)$ variables and constraints. Naturally, it is this essentially unique randomized Condorcet winner that we propose to select.

**Definition 1** The randomized Condorcet voting system (RCVS) $\mathscr{C} : \Delta(\mathcal{O}) \to \Delta(X)$ selects the randomized Condorcet winner $\mathscr{C}(\tilde{\theta})$ of the majority preferences $M_{\tilde{\theta}}$.[5]

---

[5] In the case where the randomized Condorcet winner is not unique, a randomized Condorcet winner could be randomly selected by the RCVS by maximizing a random linear objective function over the polytope of randomized Condorcet winners.

Note that any deterministic Condorcet winner is a randomized Condorcet winner. Therefore, by the uniqueness property, if a deterministic Condorcet winner exists, then the RCVS selects it deterministically. In any case, by construction, the RCVS has the following characteristic property:

$$\forall \tilde{x} \in \Delta(X), \quad M_{\tilde{\theta}} : \mathscr{C}(\tilde{\theta}) \gtreqqless \tilde{x},$$

that is, the majority always prefers the randomized Condorcet winner at least as much as any lottery. From this property, it is immediate that the RCVS satisfies independence of irrelevant alternatives, in the sense that if an alternative is not in the support of $\mathscr{C}(\tilde{\theta})$, then removing it from the set of alternatives (which only implies reducing the set $\Delta(X)$) does not affect the value of lottery $\mathscr{C}(\tilde{\theta})$.

*Example 3* We reconsider Example 1. Recall that $M_{\tilde{\theta}} : x \gg y \gg z \gg x$, so that there was no deterministic Condorcet winner. In particular, note that $M_{\tilde{\theta}} : c \gg p$ if and only if $(c, p) \in \{(x, y), (y, z), (z, x)\}$. Here, the randomized Condorcet winner $\mathscr{C}(\tilde{\theta})$ is the uniform distribution over $X$. Indeed, let $\tilde{p}$ the lottery that assigns probabilities $p_x$, $p_y$ and $p_z$ to alternatives $x$, $y$ and $z$. Then,

$$
\begin{aligned}
\mathbb{P}_{c \sim \mathscr{C}(\tilde{\theta}), p \sim \tilde{p}} \left[ M_{\tilde{\theta}} : c \gg p \right] &= \mathbb{P}\left[ (c, p) \in \{(x, y), (y, z), (z, x)\} \right] \\
&= \mathbb{P}\left[ (c, p) = (x, y) \right] + \mathbb{P}[(c, p) = (y, z)] + \mathbb{P}[(c, p) = (z, x)] \\
&= \frac{p_y}{3} + \frac{p_z}{3} + \frac{p_x}{3} \\
&= \mathbb{P}\left[ (c, p) = (z, y) \right] + \mathbb{P}[(c, p) = (x, z)] + \mathbb{P}[(c, p) = (y, x)] \\
&= \mathbb{P}\left[ (c, p) \in \{(z, y), (x, z), (y, x)\} \right] \\
&= \mathbb{P}\left[ M_{\tilde{\theta}} : c \ll p \right],
\end{aligned}
$$

where all the probabilities are obtained by drawing $c$ from $\mathscr{C}(\tilde{\theta})$ and $p$ from $\tilde{p}$. This proves that the majority $M_{\tilde{\theta}}$ likes $\mathscr{C}(\tilde{\theta})$ just as much as $\tilde{p}$. In particular, we have $M_{\tilde{\theta}} : \mathscr{C}(\tilde{\theta}) \gtreqqless \tilde{p}$, for any lottery $\tilde{p}$. This is the characteristic property of the RCVS.

*Example 4* As another example, assume $X = \{x, y, z_1, z_2, z_3\}$ and $M_{\tilde{\theta}} : x \gg y \gg z_i \gg x$ for all $i \in \{1, 2, 3\}$, and that $M_{\tilde{\theta}} : z_1 \gg z_2 \gg z_3 \gg z_1$. Then the randomized Condorcet winner assigns probability $1/3$ to $x$ and $y$, and probability $1/9$ to each $z_i$ for $i \in \{1, 2, 3\}$.

## 3 Condorcet-Proofness

As claimed in the introduction, the RCVS has appealing strategy-proofness properties. In this section, we shall prove some of these properties. Namely, we will show that the RCVS is Condorcet-proof, which means that, when a deterministic Condorcet winner exists, the RCVS selects it and no voter has then incentive to misreport his preferences. Moreover, we will prove that the RCVS

is the only voting system to have this property in a class of voting systems
based on pairwise comparisons. To formalize these properties, we first intro-
duce the preferences and strategies that the definition of Condorcet-proofness
relies on.


### 3.1 Preferences and Strategies

While our preferences are so far well-defined over $X$, we need to determine
how they extend to pairwise comparisons of lotteries. There is not a unique
way to perform such an extension. In this paper, we do so as follows. We say
that a voter with preference $\theta \in \mathcal{O}$ prefers lottery $\tilde{x}$ to $\tilde{y}$ if he is more likely
to prefer an alternative drawn by $\tilde{x}$ to one drawn by $\tilde{y}$, than the other way
around, i.e.

$$\theta : \tilde{x} \succeq \tilde{y} \quad \overset{\triangle}{\Longleftrightarrow} \quad \mathbb{P}_{x \sim \tilde{x}, y \sim \tilde{y}} [\theta : x \succ y] \geq \mathbb{P}_{x \sim \tilde{x}, y \sim \tilde{y}} [\theta : x \prec y].$$

These preferences are the pairwise comparison extensions introduced by Aziz
et al (2014). They are particular cases of the SSB preferences axiomatized by
Fishburn (1982)[6]. Note that they are nontransitive[7] and thus do not satisfy
the axioms by Von Neumann and Morgenstern (1944). This explains why the
Gibbard (1977) theorem does not apply to our setting. Nevertheless, they can
be considered risk-neutral, in the sense that, if $\theta : x \succ y \succ z$, if $\tilde{w}$ is the
uniform distribution over $\{x, y, z\}$ and if $w$ is drawn from $\tilde{w}$, then $\theta$ is equally
likely to prefer $w$ over $\tilde{w}$ than the other way around. In practice, voters might
be more risk-averse than that, in which case the RCVS will turn out to be all
the more Condorcet-proof.

A helpful feature of such preferences is that they are perfectly determined
by their restriction to preferences over alternatives. In particular, combined to
the revelation principle derived by Gibbard (1973), this implies that, without
loss of generality, we can restrict ourselves to the analysis of voting systems
whose ballots are the total orders over $X$.

Now, in an actual election, the voters have the option of voting any ballot,
including those that do not represent their actual preferences. We capture
this by introducing the concept of strategies. Intuitively, a strategy of the
population tells how each voter, given his preferences, will vote. More formally,
a strategy $s$ of the population is a mapping $s : \mathcal{O} \to \Delta(\mathcal{O})$, where $s(\theta)$ is the
mix of ballots chosen by voters of preference $\theta$. A more relevant way to interpret
this mix of ballots is to regard it as the way the set of voters with preference
$\theta$ will spread its votes among the different possible ballots. What is more, we
extend the domain of $s$ to the set $\Delta(\mathcal{O})$ by $s(\tilde{\theta}) \triangleq \mathbb{E}[s(\tilde{\theta})]$, so that $s$ is now a
function $\mathcal{O} \to \Delta(\mathcal{O})$. Then, given the preferences $\tilde{\theta}$ of the people, $s(\tilde{\theta})$ are the
ballots of the people when they follow strategy $s$.

---

[6] A preference $\theta$ over lotteries is SSB if there exists a skew-symmetric matrix $\phi(\theta) \in \mathbb{R}^{X \times X}$
such that $\theta : \tilde{x} \succ \tilde{y}$ if and only if $p(\tilde{x})^T \phi(\theta) p(\tilde{y}) > 0$, where $p(\tilde{x}) \in \mathbb{R}^X$ is the vector of the
probabilities of the lottery $\tilde{x}$. In our case, $\phi_{xy}(\theta) \triangleq 1$ if $\theta : x \succ y$, and $-1$ otherwise.

[7] See, e.g. Grime (2010), for examples on such nontransitivity.

Now, the strategy $s$ determines a partition of the voters into two subsets $\mathsf{Truthful}(s)$ and $\mathsf{Manipulator}(s)$ defined by

$$\mathsf{Truthful}(s) = \{\theta \in \mathcal{O} \mid s(\theta) = \delta_\theta\},$$
$$\mathsf{Manipulator}(s) = \{\theta \in \mathcal{O} \mid s(\theta) \neq \delta_\theta\},$$

where $\delta_\theta$ is the Dirac distribution on $\theta$. Finally, the truthful strategy $s^{truth}$ is evidently defined by $s^{truth}(\theta) = \delta_\theta$ for all $\theta \in \mathcal{O}$. Equivalently, a strategy $s$ is truthful when $\mathsf{Truthful}(s) = \mathcal{O}$.

## 3.2 Condorcet-proofness of the RCVS

We can now define formally what we mean by Condorcet-proofness. Recall that a voting system $\mathscr{V}$ inputs the ballots of the population $\tilde{a} \in \Delta(\mathcal{O})$ and outputs a lottery $\mathscr{V}(\tilde{a}) \in \Delta(X)$. When the population with preferences $\tilde{\theta}$ is truthful, the ballots are $\tilde{a} = \tilde{\theta}$. When the population plays strategy $s$, its ballots are $\tilde{a} = s(\tilde{\theta})$.

**Definition 2** A voting system $\mathscr{V} : \Delta(\mathcal{O}) \rightarrow \Delta(X)$ is Condorcet-proof if, whenever preferences $\tilde{\theta}$ of the people yield a deterministic Condorcet winner $x$, the voting system $\mathscr{V}$ selects $x$ and there is no preference $\theta$ such that individuals with preference $\theta$ have incentives to misreport their preferences altogether, i.e.

$$\forall \tilde{\theta}, \left(\exists x, \forall y, M_{\tilde{\theta}} : x \gg y\right) \Longrightarrow \begin{cases} \mathscr{V}(\tilde{\theta}) = \delta_x, \\ \mathsf{Manipulator}(s) = \{\theta\} \Rightarrow \theta : \mathscr{V}(s(\tilde{\theta})) \preceq \mathscr{V}(\tilde{\theta}). \end{cases}$$

In other words, a Condorcet-proof voting system is a Condorcet method that prevents manipulations when a deterministic Condorcet winner exists. Therefore, Condorcet-proofness does not entirely include strategy-proofness. It only includes strategy-proofness for certain population preferences $\tilde{\theta}$. Note, in addition, that this strategy-proofness is slightly stronger than the more usual dominant-strategy-proofness from the literature. Indeed, here, we allow for more than one voter to deviate from truthfulness. However, we do require is that all the voters that do deviate from truthfulness have the same preference. Thus, Condorcet-proofness can be regarded as a weaker version of the stronger group-Condorcet-proofness we shall discuss later on, which imposes no restriction on the set of manipulators.

The following key theorem has been sketched by Peyre (2012c) in a popularization article. Here, we provide a rigorous proof.

**Theorem 2 (Peyre (2012c))** *The RCVS is Condorcet-proof.*

First note that, as we already said it earlier, the RCVS does select deterministic Condorcet winners whenever they exist. Therefore, all we need to prove is the strategy-proofness part. Now, we prove an insightful lemma. Loosely, it says that, when misreporting their preferences, manipulators can only switch pairwise majority preferences that they agree with.

**Lemma 1** *Assume* $\mathsf{Manipulator}(s) = \{\theta\}$ *and* $M_{\tilde{\theta}} : x \gg y$. *The two following implications hold:*

- *If* $\theta : y \succ x$, *then* $M_{s(\tilde{\theta})} : x \gg y$.
- *If* $M_{s(\tilde{\theta})} : y \gg x$, *then* $\theta : x \succ y$.

*Proof* Let us prove the first implication. We assume $\theta : y \succ x$. Then, the manipulator $\theta$ cannot increase the number of ballots that favor $y$ to $x$. Indeed,

$$
\begin{aligned}
\mathbb{P}_{a \sim s(\tilde{\theta})} \left[ a : y \succ x \right] &= \mathbb{E}_{\hat{\theta} \sim \tilde{\theta}} \left[ \mathbb{P}_{a \sim s(\hat{\theta})} \left[ a : y \succ x \right] \right] \\
&= \mathbb{E}_{\hat{\theta} \sim \tilde{\theta}} \left[ \mathbb{P}_{a \sim s(\hat{\theta})} \left[ a : y \succ x \right] \, \Big| \, \hat{\theta} \neq \theta \right] \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} \neq \theta \right] \\
&\qquad + \mathbb{P}_{a \sim s(\theta)} \left[ a : y \succ x \right] \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} = \theta \right] \\
&\leq \sum_{\substack{a : y \succ x \\ a \neq \theta}} \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} = a \right] + \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} = \theta \right] \\
&= \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} : y \succ x \right],
\end{aligned}
$$

where we used the fact that $s(\hat{\theta}) = \delta_{\hat{\theta}}$ for $\hat{\theta} \neq \theta$, and that $\mathbb{P}_{a \sim s(\theta)} \left[ a : y \succ x \right] \leq 1$. A similar computation shows that $\mathbb{P}_{a \sim s(\tilde{\theta})} \left[ a : x \succ y \right] \geq \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} : x \succ y \right]$. Thus,

$$
\begin{aligned}
M_{\tilde{\theta}} : x \gg y \quad &\Longleftrightarrow \quad \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} : x \succ y \right] > \mathbb{P}_{\hat{\theta} \sim \tilde{\theta}} \left[ \hat{\theta} : y \succ x \right] \\
&\Longrightarrow \quad \mathbb{P}_{a \sim s(\tilde{\theta})} \left[ a : x \succ y \right] > \mathbb{P}_{a \sim s(\tilde{\theta})} \left[ a : y \succ x \right] \\
&\Longleftrightarrow \quad M_{s(\tilde{\theta})} : x \gg y,
\end{aligned}
$$

which is the first implication of the lemma. The second implication is essentially the contraposition, using in addition the fact that if $M_{\tilde{\theta}} : x \gg y$ implies that $x \neq y$, and thus, if $\theta : x \succeq y$, then $\theta : x \succ y$. $\qquad\square$

We can now prove the theorem.

*Proof (Theorem 2)* Assume that the preferences $\tilde{\theta}$ of the people yield a Condorcet winner $x \in X$ and that $\mathsf{Manipulator}(s) = \{\theta\}$. Using the fundamental property of the RCVS for $s(\tilde{\theta})$ and the previous lemma, we have

$$
\begin{aligned}
M_{s(\tilde{\theta})} &: \mathscr{C}(s(\tilde{\theta})) \gg x \\
&\Longleftrightarrow \quad \mathbb{P}_{y \sim \mathscr{C}(s(\tilde{\theta}))} \left[ M_{s(\tilde{\theta})} : y \gg x \right] \geq \mathbb{P}_{y \sim \mathscr{C}(s(\tilde{\theta}))} \left[ M_{s(\tilde{\theta})} : x \gg y \right] \\
&\Longrightarrow \quad \mathbb{P}_{y \sim \mathscr{C}(s(\tilde{\theta}))} \left[ \theta : x \succ y \right] \geq \mathbb{P}_{y \sim \mathscr{C}(s(\tilde{\theta}))} \left[ \theta : y \succ x \right] \\
&\Longleftrightarrow \quad \theta : x \succeq \mathscr{C}(s(\tilde{\theta})),
\end{aligned}
$$

which proves that the manipulator $\theta$ does not gain by misreporting his preferences. $\qquad\square$

3.3 Near-Uniqueness

Condorcet-proofness is a very restrictive property, and it is a remarkable fact that the RCVS satisfies it. Indeed, in this section, we shall prove that any Condorcet-proof tournament-based[8] voting system must agree with the RCVS for a wide range of inputs. To do so, we first defined what a tournament-based voting system is. Recall that the referendum matrix measured the margins by which any alternative is preferred to any other alternative, while the skew-symmetric matrix $A(M_{\tilde{\theta}})$ computes the signs of the referendum matrix.

**Definition 3** A pairwise (respectively, tournament-based) voting system is a voting system whose outcome is entirely determined by the referendum matrix (respectively, by the signs of the entries of the referendum matrix).

Moreover, let us define the $\ell_1$-norm of the referendum matrix by

$$||\mathcal{R}(\tilde{\theta})||_1 \triangleq \sum_{x,y \in X} |\mathcal{R}_{xy}(\tilde{\theta})|.$$

We can now state the uniqueness result.

**Theorem 3** *A Condorcet-proof pairwise voting system must agree with the RCVS for all preferences $\tilde{\theta}$ of the people such that $||\mathcal{R}(\tilde{\theta})||_1 < 2$ and $\mathcal{R}_{xy}(\tilde{\theta}) \neq 0$ for all $x \neq y$. In particular, the RCVS is the only Condorcet-proof tournament-based voting system.*

*Proof* The proof is given in Appendix A. □

While the theorem indicates a sort of uniqueness of Condorcet-proof voting systems, at least in a neighborhood of the uniform distribution, I have not succeeded in characterizing these Condorcet-proof voting systems. I suspect them not to be unique though. My intuition is that some referendum matrices $R$ are so extreme that only a few ballots $\tilde{a}$ that could have led to them, in which case strategy-proofness may not be restrictive enough to impose the uniqueness of the choice of $\mathcal{V}(\tilde{a})$.

Two intuitive remarks can be added though to hint at the fact that this theorem encompasses more cases than it seems to. First, ballots that almost yield deterministic Condorcet winners are intuitively those that could likely have been results of manipulations without which a deterministic Condorcet winner existed. Therefore, quite likely, it will be necessary to impose many constraints on the outcomes of these ballots to prevent possible manipulations. This suggests that Condorcet-proofness imposes the winning lottery for such ballots to be at least quite similar to the randomized Condorcet winner. Second, if we add the constraint that the voting system must satisfy independence of irrelevant alternatives, then there will likely be only a handful of

---

[8] The terminology of tournaments is widely used in social choice theory, e.g. see Laslier (1997). It corresponds to a (sometimes weighted) directed graph whose nodes are alternatives, and with an arc from $x$ to $y$ if the majority prefers $x$ to $y$. Equivalently, the graph can be represented by the referendum matrix we use here.

alternatives that actually matter. This means that Condorcet-proofness must apply to a small induced graph, for which the assumptions of Theorem 3 are more likely to apply.

To illustrate the rareness of Condorcet-proof voting systems, let us present an example of a Condorcet method which fails to be Condorcet-proof.

*Example 5* In the last decades, Schulze (2011) introduced a seductive deterministic voting system based on weighted tournaments. Weighted tournaments can be represented as weighted directed graphs whose nodes are alternatives. We then draw an arcs from $x$ to $y$, if the majority prefers $x$ to $y$, and we assign a weight to the arc proportional to $\mathcal{R}_{xy}(\tilde{\theta})$. Note that a deterministic Condorcet winner in this setting is a node with no incoming arc. When there is such a node, Schulze proposes to select this node. This means that the Schulze method is a Condorcet method. When no deterministic Condorcet winner exists, however, Schulze proposes to remove the arcs of the weighted tournament which have the smallest weights until the tournament yields a Condorcet winner.

Unfortunately, the Schulze method fails to be strategy-proof even when a deterministic Condorcet winner exists, and even in the simplified setting where preferences assumed both single-crossing and single-peaked[9]. To see this, consider $x < y < z$ three alternatives and preferences defined by

$$\theta_1 : x \succ y \succ z, \qquad \theta_2 : y \succ x \succ z, \qquad \theta_3 : y \succ z \succ x, \qquad \theta_4 : z \succ y \succ x. \tag{1}$$

Consider 15 voters whose preferences $\tilde{\theta} \in \Delta(\mathcal{O})$ are

$$15\,\tilde{\theta} = 7\theta_1 + 3\theta_2 + 3\theta_3 + 2\theta_4. \tag{2}$$

Given these preferences, $y$ is the Condorcet winner of $\tilde{\theta}$, and the one that the Schulze method selects. But now consider that manipulators $\theta_1$ choose ballot $s(\theta_1) = \delta_a$, where $a : x \succ z \succ y$, and that other voters are truthful (i.e. $\mathsf{Manipulator}(s) = \{\theta_1\}$). Then,

$$15\,s(\tilde{\theta}) = 7a + 3\theta_2 + 3\theta_3 + 2\theta_4. \tag{3}$$

We now have a Condorcet paradox $M_{s(\tilde{\theta})} : y \gg x \gg z \gg y$. This is illustrated in Figure 1.

At this point, the Schulze method consists in removing the arc with the lowest weight, which is the arc from $y$ to $x$. This leaves $x$ with no incoming arc, leading to the election of $x$. Since manipulators $\theta_1$ indeed prefer $x$ to $y$, they benefit from conspiring, which proves that the Schulze method is not strategy-proof even highly structured preferences.

---

[9] We give definitions to single-crossing and single-peakedness later on.

**Fig. 1** On the left is the tournament of the preferences, where $y$ is Condorcet winner. The arrow from $y$ to $x$ corresponds to the majority preference $M_{\tilde{\theta}} : y \gg x$. On the right is the tournament of the ballots, for which the Schulze method elects $x$. Weights are the surplus of voters that prefer one alternative to another.

## 4 Group-Condorcet-Proofness

Strategy-proofness as defined so far is restricted to a class of single-minded voters deviating from truthfulness. A stronger form of strategy-proofness may be desirable in settings where voters can easily communicate and plot more complex group strategies. This leads us to the concept of group strategy-proofness, which has for instance been studied in Saporiti (2009) and Penn et al (2011).

**Definition 4** A voting system $\mathscr{V} : \Delta(\mathcal{O}) \to \Delta(X)$ is group-Condorcet-proof if, whenever preferences $\tilde{\theta}$ of the people yield a Condorcet winner $x$, the voting system $\mathscr{V}$ selects $x$ and no subset of voters has strict incentives to collectively misreport their preferences, i.e. for all such $\tilde{\theta}$, we have $\mathscr{V}(\tilde{\theta}) = \delta_x$ and

$$\forall s \neq s^{truth}, \exists \theta \in \mathsf{Manipulator}(s), \quad \theta : \mathscr{V}(s(\tilde{\theta})) \preceq \mathscr{V}(\tilde{\theta}).$$

Group strategy-proofness is sometimes regarded as too strong a requirement. One contribution of this paper is to back this intuition, with the following impossibility theorem.

**Theorem 4** *There is no group-Condorcet-proof voting system.*

*Proof* The proof only requires 4 alternatives and 7 voters, among whom only 2 need to be assumed to be manipulators. Let $X = \{w, x, y, z\}$ and the ballots:

$$a_1 : x \succ y \succ z \succ w, \qquad a_2 : z \succ x \succ y \succ w, \qquad (4)$$

$$a_3 : x \succ w \succ y \succ z, \qquad a_4 : y \succ w \succ z \succ x, \qquad a_5 : z \succ w \succ x \succ y. \qquad (5)$$

We define the ballots of the people by

$$7\tilde{a} = a_1 + a_2 + a_3 + 2a_4 + 2a_5,$$

which means that 1 out of the 7 voters voted $a_1$, 1 voted $a_2$, and so on.

The weighted tournament of the ballots is depicted in Figure 1, where weights have to be divided by 7, along with the referendum matrix $\mathcal{R}(\tilde{a})$.

Let $\mathscr{V}$ be a group-Condorcet-proof voting system. We will show that, for any choice of $\mathscr{V}(\tilde{a}) \in \Delta(X)$, the ballots $\tilde{a}$ could have been produced by manipulators who had incentives to misreport their preferences, even when there
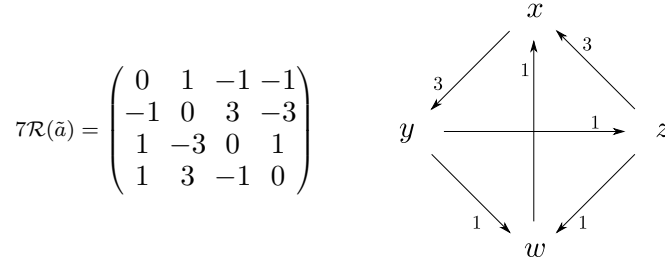
$$7\mathcal{R}(\tilde{a}) = \begin{pmatrix} 0 & 1 & -1 & -1 \\ -1 & 0 & 3 & -3 \\ 1 & -3 & 0 & 1 \\ 1 & 3 & -1 & 0 \end{pmatrix}$$



**Table 1** Pairwise comparisons of ballots $\tilde{a}$.

was a Condorcet winner for the preferences. This will show that $\mathscr{V}$ cannot exist. To do so, let us denote $p_v = \mathbb{P}_{\hat{v} \sim \mathscr{V}(\tilde{a})}[\hat{v} = v]$ for all $v \in X$.

Now, consider $\theta_y : z \succ w \succ y \succ x$, and the preferences $\tilde{\theta}_y \in \Delta(\mathcal{O})$ of the people defined by

$$7\tilde{\theta}_y = a_1 + a_2 + a_3 + 2a_4 + 2\theta_y.$$

In other words, we are investigating the case where the two $\theta_y$ voters were manipulators and voted $a_5$ instead of $\theta_y$. We have $7\mathcal{R}_{yx}(\tilde{\theta}_y) = 1 > 0$, yielding $M_{\tilde{\theta}_y} : y \gg x$. Plus, like for $M_{\tilde{a}}$, we have $M_{\tilde{\theta}_y} : y \gg z$ and $M_{\tilde{\theta}_y} : y \gg w$. Thus, $y$ is Condorcet winner of $\tilde{\theta}_y$. To make sure that the two $\theta_y$ did not have incentives to conspire, we must have $\theta_y : \mathscr{V}(\tilde{a}) \preceq y$. This means that $p_w + p_z \leq p_x$.

We then investigate a similar manipulation by $\theta_z : x \succ w \succ z \succ y$ when the preferences of the people are $\tilde{\theta}_z$ defined by

$$7\tilde{\theta}_z = a_1 + a_2 + \theta_z + 2a_4 + 2a_5.$$

Similarly to above, we verify that $z$ is the Condorcet winner of $\tilde{\theta}_z$. Strategy-proofness then implies that $p_w + p_x \leq p_y$.

Now consider $\theta_x : y \succ x \succ w \succ z$ and $\tilde{\theta}_x$ defined by

$$7\tilde{\theta}_x = a_1 + a_2 + a_3 + 2\theta_x + 2a_5.$$

Alternative $x$ is the Condorcet winner of $\tilde{\theta}_x$, implying $p_y \leq p_w + p_z$.

Before going further, let us find out the implication of the three inequalities we have seen so far. Using successively the second, third and first inequalities yields:

$$p_w + p_x \leq p_y \leq p_w + p_z \leq p_x.$$

This leads to $p_w \leq 0$, and, since probabilities are non-negative, $p_w = 0$. It then follows that $p_x = p_y = p_z = 1/3$. This determines uniquely the lottery that $\mathscr{V}(\tilde{a})$ must be to guarantee individual Condorcet-proofness. Interestingly, this is precisely the lottery prescribed by the RCVS.

However, we can show that this lottery is not compatible with group-Condorcet-proofness. Indeed, consider $\theta_w^1 : x \succ y \succ w \succ z$ and $\theta_w^2 : z \succ x \succ w \succ y$ and $\tilde{\theta}_w$ defined by

$$7\tilde{\theta}_w = \theta_w^1 + \theta_w^2 + a_3 + 2a_4 + 2a_5.$$

Now, $w$ is the Condorcet winner of $\tilde{\theta}_w$. But since we have $2/3 = p_x + p_y > p_z = 1/3$ and $2/3 = p_x + p_z > p_y = 1/3$, both manipulators $\theta_w^1$ and $\theta_w^2$ had incentives to conspire. Thus $\mathscr{V}$ is not group-Condorcet-proof, which proves the theorem. $\qquad\square$

### 4.1 Median Voter

In practice, many social choice settings yield a natural one-dimensional structure, e.g. in politics. This means that alternatives can be located on a one-dimensional line, and that the preferences of voters are somehow consistent with the way alternatives are located on the line. The one-dimensionality of alternatives can be represented by a total order relation on $X$, where $x < y$ means that $x$ is "on the left" of $y$. However, in the literature, we find two distinct definitions of the consistency of preferences with respect to the left-right structure of alternatives.

**Definition 5** The set $\mathcal{O}^{SP}$ of single-peaked preferences is the set of preferences $\theta$ such that, denoting $x^*(\theta)$ the favorite alternative of $\theta$, we have

$$(y < x < x^*(\theta) \quad \text{or} \quad x^*(\theta) < x < y) \quad \implies \quad \theta : x \succ y,$$

for any two alternatives $x$ and $y$.

A set $\mathcal{O}^{SC}$ of preferences is single-crossing if there is an order relation "$<$" on $\mathcal{O}^{SC}$ such that, whenever $x_1 < x_2$ and $\theta_1 < \theta_2$, we have

$$\left(\theta_1 : x_2 \succ x_1 \Rightarrow \theta_2 : x_2 \succ x_1\right) \quad \text{and} \quad \left(\theta_2 : x_1 \succ x_2 \Rightarrow \theta_1 : x_1 \succ x_2\right).$$

These two definitions are incompatible, in the sense that there are single-crossing sets of preferences that do not satisfy single-peakedness, and the set of single-peaked preferences is not single-crossing. However, under any of these two assumptions, we can define the concept of a median voter[10]. The well-known median voter theorem then holds.

**Theorem 5 (Black (1958); Dummett and Farquharson (1961); Roberts (1977); Rothstein (1990, 1991); Gans and Smart (1996))** *If preferences are single-peaked or single-crossing and yield a median voter, then the median voter's favorite alternative is the Condorcet winner.*

Note that Black (1958) proved that this allows a majority of the people to secure the selection of the Condorcet winner. In other words, if the majority agrees to select the Condorcet winner, no one outside the majority can modify the outcome. This property is called stability. Dummett and Farquharson (1961) showed that it still held even if we slightly weaken the single-peakedness

---

[10] In the case of single-peakedness, the median voter is ill-defined, but the favorite alternative of the median voter is well-defined, by considering the partial order on voters derived by the left-right order between their favorite alternatives.

assumption. However, stability is weaker than strategy-proofness, which requires that no one, within the majority or not, can manipulate the vote to obtain a better alternative. As pointed out by Penn et al (2011), the apparent simplicity of the theorem above vanishes as we involve strategy-proofness. Indeed, Penn et al (2011) proved that a deterministic group-strategy-proof voting system must be dictatorial even when preferences are assumed single-peaked.

Now, Moulin (1980) did propose a strategy-proof voting system for single-peaked preferences called the median rule, and Saporiti (2009) did prove the group-strategy-proofness for single-crossing preferences of a variant of the median rule. However, to do so, alternatives must officially and unambiguously be located on the left-right line, and voters must be forbidden from voting ballots that are inconsistent with this left-right line. In fact, the mere concept of the median voter requires assuming that everyone agrees on how alternatives range on the left-right line. In many cases, e.g. politics, even when alternatives and preferences mostly have some hidden left-right structure, alternatives may refuse to be located on this left-right line, and voters may refuse to be forbidden from casting non-single-crossing or non-single-peaked ballots.

Formally, this would require to define a voting system $\mathscr{V} : \Delta(\Theta) \to \Delta(X)$, even though we believe or know the support of $\tilde{\theta}$ to be restricted to $\mathcal{O}^{SP}$ or some $\mathcal{O}^{SC}$. In particular, manipulations may still produce ballots $s(\tilde{\theta})$ whose support is not limited to $\mathcal{O}^{SP}$ or some $\mathcal{O}^{SC}$, in which case a decision $\mathscr{V}(s(\tilde{\theta}))$ still needs to be made.

This subtle difficulty to design strategy-proof voting systems even under one-dimensional preferences renders methods by Moulin (1980) and Saporiti (2009) inapplicable in our setting. Meanwhile, we have seen in Example 5 that the Schulze method fails to be strategy-proof even when preferences are both single-peaked and single-crossing. This makes the following result all the more remarkable.

**Theorem 6** *When the support of the preferences $\tilde{\theta}$ is single-peaked or single-crossing, the RCVS is group Condorcet-proof.*

The proof is given in Appendix B.

## 5 Conclusion

In this paper, we have unveiled some remarkable strategy-proof properties of the RCVS. Namely, we have proved the RCVS is Condorcet-proof, and that, in a large class of voting systems, it is the only one to be Condorcet-proof. Moreover, when preferences are one-dimensionsal, it is even group-Condorcet-proof. We have shown this to be a remarkable property by proving that, in the general case, there is no group-Condorcet-proof voting system. Given that, in addition, the RCVS is a natural and easily computable extension of Condorcet's ideas, it is tempting to assume that, considering Condorcet' philosophical take on social choice theory, his wide use of probability theory in diverse problems, and

his concern of strategy-proofness, "he would have endorsed [the RCVS] enthusiastically", as already noted by Felsenthal and Machover (1992). For these reasons, we end this paper by emphatically advocating its use in practice.

# References

Arrow K (1951) Individual values and social choice. Nueva York: Wiley 24

Aziz H, Brandt F, Brill M (2013) On the tradeoff between economic efficiency and strategy proofness in randomized social choice. In: Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems, pp 455–462

Aziz H, Brandl F, Brandt F (2014) On the incompatibility of efficiency and strategyproofness in randomized social choice. In: Proceedings of 28th Association for the Advancement of Artificial Intelligence Conference, pp 545–551

Aziz H, Brandl F, Brandt F (2015) Universal pareto dominance and welfare for plausible utility functions. Journal of Mathematical Economics 60:123–133

Balbuzanov I (2016) Convex strategyproofness with an application to the probabilistic serial mechanism. Social Choice and Welfare 46(3):511–520

Black D (1958) The Theory of Committees and Elections. Cambridge, England, Cambridge University Press

Bogomolnaia A, Moulin H (2001) A new solution to the random assignment problem. Journal of Economic theory 100(2):295–328

Bogomolnaia A, Moulin H, Stong R (2005) Collective choice under dichotomous preferences. Journal of Economic Theory 122(2):165–184

Brandl F, Brandt F, Geist C (2016a) Proving the incompatibility of efficiency and strate- gyproofness via smt solving. In: Proceedings of the 25th International Joint Conference on Artificial Intelligence (IJCAI), AAAI Press, pp 116–122

Brandl F, Brandt F, Seedig HG (2016b) Consistent probabilistic social choice. Econometrica 84(4):1839–1880

Campbell DE, Kelly JS (1998) Incompatibility of strategy-proofness and the condorcet principle. Social Choice and Welfare 15(4):583–592

Chatterji S, Sen A, Zeng H (2014) Random dictatorship domains. Games and Economic Behavior 86:212–236

Condorcet MJANdC (1785) Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix. L'Imprimerie Royale

Dummett M, Farquharson R (1961) Stability in voting. Econometrica: Journal of the Econometric Society pp 33–43

Ehlers L, Peters H, Storcken T (2002) Strategy-proof probabilistic decision schemes for one-dimensional single-peaked preferences. Journal of Economic Theory 105(2):408–434

Felsenthal DS, Machover M (1992) After two centuries, should Condorcet's voting procedure be implemented? Behavioral Science 37(4):250–274

Fishburn PC (1982) Nontransitive measurable utility. Journal of Mathematical Psychology 26(1):31–67

Fishburn PC (1984) Probabilistic social choice based on simple voting comparisons. The Review of Economic Studies pp 683–692

Fisher DC, Ryan J (1992) Optimal strategies for a generalized "scissors, paper, and stone" game. The American Mathematical Monthly 99(10):935–942

Gans JS, Smart M (1996) Majority voting with single-crossing preferences. Journal of Public Economics 59(2):219–237

Gibbard A (1973) Manipulation of voting schemes: a general result. Econometrica: Journal of the Econometric Society pp 587–601

Gibbard A (1977) Manipulation of schemes that mix voting with chance. Econometrica: Journal of the Econometric Society pp 665–681

Gibbard A (1978) Straightforwardness of game forms with lotteries as outcomes. Econometrica: Journal of the Econometric Society pp 595–614

Grime J (2010) Non-transitive dice. URL `http://singingbanana.com/dice/article.htm`

Kreweras G (1965) Aggregation of preference orderings. In: Mathematics and Social Sciences I: Proceedings of the Seminars of Menthon-Saint-Bernard, France (1–27 July 1960) and of Gösing, Austria (3–27 July 1962), pp 73–79

Laffond G, Laslier JF, Le Breton M (1993) The bipartisan set of a tournament game. Games and Economic Behavior 5(1):182–201

Laslier JF (1997) Tournament solutions and majority voting. 7, Springer Verlag

Laslier JF (2000) Aggregation of preferences with a variable set of alternatives. Social Choice and Welfare 17(2):269–282

Moulin H (1980) On strategy-proofness and single peakedness. Public Choice 35(4):437–455

Myerson RB (1996) Fundamentals of social choice theory. Center for Mathematical Studies in Economics and Management Science, Northwestern University, URL `http://home.uchicago.edu/rmyerson/research/schch1.pdf`

Nash J (1951) Non-cooperative games. Annals of Mathematics pp 286–295

Penn EM, Patty JW, Gailmard S (2011) Manipulation and single-peakedness: A general result. American Journal of Political Science 55(2):436–449

Peyre R (2012a) Et le vainqueur du second tour est... Images des Mathématiques, CNRS, URL `http://images.math.cnrs.fr/Et-le-vainqueur-du-second-tour-est.html`

Peyre R (2012b) La démocratie, objet détude mathématique. Images des Mathématiques, CNRS, URL `http://images.math.cnrs.fr/La-democratie-objet-d-etude.html`

Peyre R (2012c) La quête du graal électoral. Images des Mathématiques, CNRS, URL http://images.math.cnrs.fr/La-quete-du-Graal-electoral.html

Rivest RL, Shen E (2010) An optimal single-winner preferential voting system based on game theory. In: Proc. of the 3rd Intl. Workshop on Computational Social Choice (COMSOC), Citeseer, pp 399–410

Roberts KW (1977) Voting over income tax schedules. Journal of Public Economics 8(3):329–340

Rothstein P (1990) Order restricted preferences and majority rule. Social Choice and Welfare 7(4):331–342

Rothstein P (1991) Representative voter theorems. Public Choice 72(2-3):193–212

Saporiti A (2009) Strategy-proofness and single-crossing. Theoretical Economics 4(2):127–163

Satterthwaite MA (1975) Strategy-proofness and arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions. Journal of Economic Theory 10(2):187–217

Schulze M (2011) A new monotonic, clone-independent, reversal symmetric, and condorcet-consistent single-winner election method. Social Choice and Welfare 36(2):267–303

Von Neumann J (1928) Die zerlegung eines intervalles in abzählbar viele kongruente teilmengen. Fundamenta Mathematicae 11(1):230–238

Von Neumann J, Morgenstern O (1944) Theory of games and economic behavior. Princeton University Press

## A Proof of Theorem 3

First, we notice that $\Delta(\mathcal{O})$ can be regarded as the simplex of $\mathbb{R}^{\mathcal{O}}$, and that the map $\mathcal{R} : \Delta(\mathcal{O}) \to \mathbb{R}^{X \times X}$ can be uniquely extended to a linear map $\mathcal{R} : \mathbb{R}^{\mathcal{O}} \to \mathbb{R}^{X \times X}$. This linear map has the two following properties.

**Lemma 2** *The image of $\mathcal{R}$ coincides with the space of skew-symmetric matrices*[11].

*Proof* It is straightforward to see that the image of $\mathcal{R}$ is included in the space of skew-symmetric matrices. Reciprocally, to show the equality, we need only show that any element of the canonical basis of skew-symmetric matrices is in the image of referendum. Such an element $R \in \mathbb{R}^{X \times X}$ is of the form $R_{xy} = -R_{yx} = 1$ for some two different alternatives $x, y \in X$, and $R_{vw} = 0$ in any other case. Denote $v_1, \ldots, v_n$ the other alternatives. We define $\tilde{\theta} \in \mathbb{R}^{\mathcal{O}}$ by $\tilde{\theta} = (\theta_1 + \theta_2)/2$, where

$$\theta_1 : x \succ y \succ v_1 \succ \ldots \succ v_n \quad \text{and} \quad \theta_2 : v_n \succ \ldots \succ v_1 \succ x \succ y.$$

We then have $\mathcal{R}_{vw}(\tilde{\theta}) = 0$ if $(v, w) \notin \{(x, y), (y, x)\}$ and $\mathcal{R}_{xy}(\tilde{\theta}) = -\mathcal{R}_{yx}(\tilde{\theta}) = 1$, which proves that $R = \mathcal{R}(\tilde{\theta})$. □

**Lemma 3** $\mathcal{R}(\Delta(\mathcal{O}))$ *contains all skew-symmetric matrices of $\ell_1$-norm at most 2.*

---

[11] A skew-symmetric matrix $R$ is a matrix whose transposition $R^T$ equals its opposite $-R$, i.e. $R^T = -R$

*Proof* In the proof of Lemma 2, we showed that each element of the canonical basis is the image $\mathcal{R}(\tilde{\theta})$ of some preferences $\tilde{\theta} \in \Delta(\mathcal{O})$ of the people. Yet, such elements of the canonical basis are of $\ell_1$-norm 2. Since $\mathcal{R}$ is linear and $\Delta(\mathcal{O})$ convex, $\mathcal{R}(\Delta(\mathcal{O}))$ therefore contains all convex combinations of the elements of the canonical basis of skew-symmetric matrices. Plus, since, for any two distinct matrices of the canonical basis, the norm of the sum is the sum of the norms, all skew-symmetric matrices of $\ell_1$-norm 2 are images by $\mathcal{R}$ of some preferences of $\Delta(\mathcal{O})$. Plus, the uniform distribution $\tilde{u} \in \Delta(\mathcal{O})$ on all ballots is trivially in the kernel of $\mathcal{R}$. A convex combination involving $\tilde{u}$ then enables to obtain any skew-symmetric matrix of $\ell_1$-norm at most 2. □

We still need another lemma before proving the theorem.

**Lemma 4** *Let the preferences $\tilde{\theta} \in \Delta(\mathcal{O})$, the ballots $\tilde{a} \in \Delta(\mathcal{O})$ and a subset $\mathcal{C} \subset \mathcal{O}$ of manipulators. Then, there exists a strategy $s \in S$ such that $s(\tilde{\theta}) = \tilde{a}$ and $\mathsf{Manipulator}(s) = \mathcal{C}$ if and only if $\mathbb{P}_{\tilde{\theta}}[\mathcal{D}] \leq \mathbb{P}_{\tilde{a}}[\mathcal{D}]$ for all subsets $\mathcal{D} \subset \mathcal{O} - \mathcal{C}$. In particular, if $X$ is finite, this condition amounts to $\mathbb{P}_{\tilde{\theta}}(\tilde{\theta} = a) \leq \mathbb{P}_{\tilde{a}}(\tilde{a} = a)$ for all $a \notin \mathcal{C}$.*

*Proof* First notice that $\tilde{\theta}$ could have produced $\tilde{a}$ with a set $\mathcal{C}$ of manipulators if and only if there exists a strategy $s$ such that $\mathsf{Manipulator}(s) = \mathcal{C}$ and $s(\tilde{\theta}) = \tilde{a}$. Consider that we indeed have $s(\tilde{\theta}) = \tilde{a}$, and let us prove the direct implication of the lemma. Let $\mathcal{D} \subset \mathcal{O} - \mathcal{C}$. Then,

$$\mathbb{P}_{\tilde{a}}[\mathcal{D}] = \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\right] = \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\Big|\tilde{\theta} \in \mathcal{D}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{D}] + \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\Big|\tilde{\theta} \notin \mathcal{D}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{O} - \mathcal{D}].$$

But since $\mathcal{D} \cap \mathcal{C} = \emptyset$, for all $\theta \in \mathcal{D}$, we have $\theta \notin \mathcal{C}$. Thus, $s(\theta) = s^{truth}(\theta) = \delta_\theta$. Thus, $\mathbb{P}_{s(\theta)}[\mathcal{D}] = 1$. Thus, the expression above simplifies to

$$\mathbb{P}_{\tilde{a}}[\mathcal{D}] = \mathbb{P}_{\tilde{\theta}}[\mathcal{D}] + \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\Big|\tilde{\theta} \notin \mathcal{D}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{O} - \mathcal{D}].$$

Therefore, $\mathbb{P}_{\tilde{a}}[\mathcal{D}] \geq \mathbb{P}_{\tilde{\theta}}[\mathcal{D}]$, hence proving the direct implication.

Reciprocally, if $\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] = 0$, then the inequality $\mathbb{P}_{\tilde{\theta}}[\mathcal{D}] \geq \mathbb{P}_{\tilde{a}}[\mathcal{D}]$ implies $\tilde{\theta} = \tilde{a}$. Thus, $s^{truth}(\tilde{\theta}) = \tilde{a}$, which proves that $\tilde{\theta}$ could have produced $\tilde{a}$ with the set $\mathcal{C}$ of manipulators. Otherwise, $\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] \neq 0$. We define $s : \mathcal{C} \to \Delta(\mathcal{O})$ by $\mathbb{P}_{s(\theta)}[\mathcal{C} - \{\theta\}] = 0$,

1. $\forall \mathcal{E} \subset \mathcal{C}, \mathbb{P}_{s(\theta)}[\mathcal{E}] = \mathbb{P}_{\tilde{a}}[\mathcal{E}]/\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]$.
2. $\forall \mathcal{D} \subset \mathcal{O} - \mathcal{C}, \mathbb{P}_{s(\theta)}[\mathcal{D}] = \left(\mathbb{P}_{\tilde{a}}[\mathcal{D}] - \mathbb{P}_{\tilde{\theta}}[\mathcal{D}]\right)/\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]$.

Assuming $\mathbb{P}_{\tilde{\theta}}[\mathcal{D}] \leq \mathbb{P}_{\tilde{a}}[\mathcal{D}]$ for all supsets $\mathcal{D} \supset \mathcal{O} - \mathcal{C}$, the probabilities we have defined here are all non-negative. It is straightforward to see that the additivity of the probability is satisfied. Plus,

$$\mathbb{P}_{\tilde{\theta}}[\mathcal{O}] = \mathbb{P}_{\tilde{\theta}}[\mathcal{C}] + \mathbb{P}_{\tilde{\theta}}[\mathcal{O} - \mathcal{C}] = \frac{\mathbb{P}_{\tilde{a}}[\mathcal{C}]}{\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]} + \frac{\mathbb{P}_{\tilde{a}}[\mathcal{O} - \mathcal{C}] - \mathbb{P}_{\tilde{\theta}}[\mathcal{O} - \mathcal{C}]}{\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]} = 1.$$

Therefore, $s(\theta)$ is a well-defined probability, and $s$ a well-defined strategy of support $\mathcal{C}$. Plus, for $\mathcal{D} \subset \mathcal{O} - \mathcal{C}$,

$$\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}] = \mathbb{P}_{\tilde{\theta}}[\mathcal{D}] + \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\Big|\tilde{\theta} \in \mathcal{C}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] + \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{D}]\Big|\tilde{\theta} \notin \mathcal{C} \cup \mathcal{D}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{O} - \mathcal{C} \cup \mathcal{D}]$$

$$= \mathbb{P}_{\tilde{\theta}}[\mathcal{D}] + \frac{\mathbb{P}_{\tilde{a}}[\mathcal{D}] - \mathbb{P}_{\tilde{\theta}}[\mathcal{D}]}{\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]}\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] = \mathbb{P}_{\tilde{a}}[\mathcal{D}],$$

and, similarly for any $\mathcal{E} \subset \mathcal{C}$, we have

$$\mathbb{P}_{s(\tilde{\theta})}[\mathcal{E}] = \mathbb{E}_{\tilde{\theta}}\left[\mathbb{P}_{s(\tilde{\theta})}[\mathcal{E}]\Big|\tilde{\theta} \in \mathcal{C}\right]\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] = \frac{\mathbb{P}_{\tilde{a}}[\mathcal{E}]}{\mathbb{P}_{\tilde{\theta}}[\mathcal{C}]}\mathbb{P}_{\tilde{\theta}}[\mathcal{C}] = \mathbb{P}_{\tilde{a}}[\mathcal{E}].$$

These two equalities prove that $s(\tilde{\theta}) = \tilde{a}$, which is what we had to prove. □

We can now prove Theorem 3.

*Proof (Theorem 3)* By contradiction, assume that $\mathscr{V}$ disagrees with the RCVS $\mathscr{C}$ for some referendum matrix $R$ of $\ell_1$-norm less than 2. Let us consider ballots $a_{vw}^+, a_{vw}^- \in \mathcal{O}$ defined by

$$a_{vw}^+ : v \succ w \succ x_1 \succ \ldots \succ x_n \quad \text{and} \quad a_{vw}^- : x_n \succ \ldots \succ x_1 \succ v \succ w.$$

Like in the proof of Lemma 2, the choices of $x_1, \ldots, x_n$ are irrelevant. What matters to us is the fact that $\mathcal{R}(a_{vw}^+ + a_{vw}^-)$ is a skew-symmetric matrix of the canonical basis. In particular, the referendum matrix $R$ that the pairwise voting system is based on can be obtained from the ballots $\tilde{a}$ defined by

$$\tilde{a} = \frac{1}{2} \sum_{v,w:R_{vw}>0} R_{vw} a_{vw}^+ + \frac{1}{2} \sum_{v,w:R_{vw}>0} R_{vw} a_{vw}^- + \delta \tilde{u},$$

where $\delta = 1 - \frac{1}{2}\|R\|_1$. By assumption on $R$, we have $\delta > 0$.

Since, by assumption, $R_{xy} \neq 0$ for all $x \neq y$, the ballots $\tilde{a}$ yields a unique randomized Condorcet winner. Therefore, the fact that $\mathscr{V}$ disagrees with $\mathscr{C}$ on $R$ implies that $\mathcal{V}(\tilde{a})$ is not the randomized Condorcet winner of $\tilde{a}$. In other words, there must be some alternative $x \in X$ that the majority $M_{\tilde{a}}$ strictly prefers to $\mathcal{V}(\tilde{a})$. Denoting $Z = \{z_1, \ldots, z_n\}$ and $Y = \{y_1, \ldots, y_m\}$ the sets of alternatives that the majority $M_{\tilde{a}}$ respectively prefers $x$ to $(M_{\tilde{a}} : x \gg z)$ and prefers to $x$ $(M_{\tilde{a}} : y \gg x)$, this means that $\mathbb{P}_{\mathscr{V}(\tilde{a})}[Z] > \mathbb{P}_{\mathscr{V}(\tilde{a})}[Y]$. Evidently, by definitions of sets $Y$ and $Z$, we have $R_{yx} > 0$ and $R_{xz} > 0$ for all $y \in Y$ and $z \in Z$.

We then define the preference $\theta \in \mathcal{O}$ of manipulators by

$$\theta : z_1 \succ \ldots \succ z_n \succ x \succ y_1 \succ \ldots \succ y_m.$$

Notice that we have $\theta : \mathcal{V}(\tilde{a}) \succ x$. We can now define the preferences $\tilde{\theta} \in \Delta(\mathcal{O})$ of the people by

$$\tilde{\theta} = \frac{1}{2} \sum_{\substack{M_{\tilde{a}}:v\gg w \\ (v,w)\notin Y\times\{x\}}} R_{vw}(a_{vw}^+ + a_{vw}^-) + \frac{1}{2}\sum_{y\in Y} R_{yx} a_{yx}^+ + \left(\epsilon + \frac{1}{2}\sum_{y\in Y} R_{yx}\right)\theta + (\delta - \epsilon)\tilde{u},$$

with $0 < \epsilon < \delta$. Importantly, any ballot $a \in \mathcal{O}$ except $\theta$ is more frequent in $\tilde{a}$ than in $\tilde{\theta}$. Thus, by Lemma 4, manipulators $\theta$ can have produced the ballots $\tilde{a}$. Moreover, we have:

$$\forall z \in Z, \quad \mathcal{R}_{xz}(\tilde{\theta}) = R_{xz} + \frac{1}{2}\sum_{y\in Y} R_{yx} \; -\epsilon - \frac{1}{2}\sum_{y\in Y} R_{yx} = R_{xz} \; -\epsilon,$$

$$\forall y \in Y, \quad \mathcal{R}_{xy}(\tilde{\theta}) = \qquad -\frac{1}{2}\sum_{y\in Y} R_{yx} \; +\epsilon + \frac{1}{2}\sum_{y\in Y} R_{yx} = \qquad +\epsilon.$$

Recall that $R_{xz} > 0$ for all $z \in Z$, hence we can choose $\epsilon$ smaller than all $R_{xz}$. By doing so, we guarantee that $\mathcal{R}_{xz}(\tilde{\theta})$ and $\mathcal{R}_{xy}(\tilde{\theta})$ are positive for all $z \in Z$ and $y \in Y$. Thus, $x$ is a Condorcet winner for $\tilde{\theta}$. Yet, by creating ballots $\tilde{a}$, manipulators $\theta$ have obtained strictly better, as we have seen that $\theta : \mathcal{V}(\tilde{a}) \succ x$. This shows that $\mathscr{V}$ is not Condorcet-proof. This proves that a Condorcet-proof pairwise voting system must agree with the RCVS whenever $\|\mathcal{R}(\tilde{\theta})\|_1 < 2$.

The uniqueness of Condorcet-proof tournament-based voting system is then immediately derived by considering any skew-symmetric matrix $R^0$, and by dividing each entry by the $\ell_1$-norm of the matrix, hence yielding a skew-symmetric matrix $R$ of norm 1 to which the previous part applies. $\qquad\square$

## B Proof of Theorem 5

We first prove the following lemma about the structure of the set of manipulators when preferences are one-dimensional.

**Lemma 5** *When preferences are single-peaked or single-crossing with a unique median voter, manipulators must either be all strictly on the left or all strictly on the right of the median voter.*

*Proof* Let $\mathscr{V}$ a voting system. Denote $x$ the Condorcet winner of the single-peaked preferences $\tilde{\theta} \in \Delta(\mathcal{O})$. Denote $Z$ and $Y$ the sets of alternatives that are respectively on the left and on the right of $x$. Now, consider a strategy $s$. We denote $s(\tilde{\theta}) = \tilde{a}$. The strict incentive to conspire means that

$$\forall \theta \in \mathsf{Manipulator}(s), \quad \theta : \mathscr{V}(\tilde{a}) \succ x.$$

If preferences are single-peaked or single-crossing and $\theta \in \mathsf{Manipulator}(s)$ is on the right of the median voter, we know that $\theta : x \succ z$ for all $z \in Z$. Indeed, if preferences are single-peaked, this is due to $\theta$'s ideal point being on the right of $x$. And if preferences are single-crossing, this is because $x$ cannot be switched with a left alternative as we look preferences on the right of the median voter. Since the median voter ranked $x$ better than any $z \in Z$, all voters on its right must do so too.

Thus, $\{z \in X \mid \theta : x \succ z\} \supset Z$, and, as a result, $\{y \in X \parallel \theta : y \succ x\} \subset Y$. Therefore,

$$0 < \mathbb{P}_{v \sim \mathscr{V}(\tilde{a})} [\theta : v \succ x] - \mathbb{P}_{v \sim \mathscr{V}(\tilde{a})} [\theta : v \prec x] \le \mathbb{P}_{\mathscr{V}(\tilde{a})}[Y] - \mathbb{P}_{\mathscr{V}(\tilde{a})}[Z].$$

Therefore, we have $\mathbb{P}_{\mathscr{V}(\tilde{a})}[Y] > \mathbb{P}_{\mathscr{V}(\tilde{a})}[Z]$. But if $\theta \in \mathsf{Manipulator}(s)$ is on the left of the median voter, we must have the opposite inequality. Both cases cannot occur simultaneously, which proves that all manipulators must be on the same side of the left-right spectrum with regards to the median voter. This proves the lemma. $\qquad\square$

We can now prove Theorem 5. The proof slightly differs depending on the assumption of one-dimensionality of preferences that is considered. For clarity, we write the proofs of the two cases in separate blocks.

*Proof (Theorem 5 for single-peakedness preferences)* Let $\mathscr{C}$ denote the randomized Condorcet voting system. We use the same notations $x, \tilde{\theta}, Y, Z, s$ and $\tilde{a}$ as in the proof of Lemma 5. Without loss of generality, we can assume that manipulators are all strictly on the right of the median voter.

Let $z \in Z$. As we have seen in the previous proof, we have $\theta : x \succ z$ for all $\theta \in \mathsf{Manipulator}(s)$. Since manipulators agree with $M_{\tilde{\theta}} : x \gg z$ for $z \in Z$, according to Lemma 1, they cannot invert these pairwise comparisons. Therefore, $M_{\tilde{a}} : x \gg z$. Yet, for manipulators to gain by conspiring, $\mathscr{C}(\tilde{a})$ must differ from $x$, which means that there must be some $y \in Y$ such that $M_{\tilde{a}} : y \gg x$. Let $y^*$ the most leftist alternative that the majority of ballots prefers to $x$, i.e.

$$y^* = \min\{y \in Y \mid M_{\tilde{a}} : y \gg x\},$$

where the minimum corresponds to the order relation "$<$" on alternatives. We denote $Y_- \triangleq \{y_- \in Y \mid x < y_- < y^*\}$ and $Y_+ \triangleq Y - Y_- = \{y_+ \in Y \mid y^* \le y_+\}$.

Since $x$ is Condorcet winner of $\tilde{\theta}$, we know that $M_{\tilde{\theta}} : x \gg y^*$. Thus, manipulators must have inverted the majority preference of $x$ over $y^*$. Since, according to Lemma 1, manipulators can only invert arcs they agree with, this means that there must be a manipulator $\theta \in \mathsf{Manipulator}(s)$ who agrees with $M_{\tilde{\theta}} : x \gg y^*$. This manipulator thus thinks $\theta : x \succ y^*$. We will show that assuming that he had incentive to conspire leads to a contradiction.

On one hand, by definition of $y^*$, we have $M_{\tilde{a}} : x \gg y$ for all $y \in Y_-$, i.e.

$$Y_- \subset \{w \in X \mid M_{\tilde{a}} : x \gg w\} \quad \text{and} \quad \{w \in X \mid M_{\tilde{a}} : w \gg x\} \subset Z \cup Y_+.$$

Combining this with the property $M_{\tilde{a}} : \mathscr{C}(\tilde{a}) \geqslant x$ satisfied by the randomized Condorcet voting system yields

$$\begin{aligned} \mathbb{P}_{\mathscr{C}(\tilde{a})}[Y_-] &\leq \mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[M_{\tilde{a}} : x \gg w\right] \\ &\leq \mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[M_{\tilde{a}} : w \gg x\right] \\ &\leq \mathbb{P}_{\mathscr{C}(\tilde{a})}\left[Z \cup Y_+\right]. \end{aligned}$$

On the other hand, strict incentives to conspire for $\theta$ imply that

$$\mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[\theta : w \succ x\right] > \mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[\theta : x \succ w\right].$$

Since $\theta : x \succ y^*$, we know that the ideal point of $\theta$ is necessarily on the left of $y^*$. As a result, for $y \in Y_+$, we have $\theta : x \succ y^* \succ y$. Therefore,

$$\left\{w \in X \mid \theta : x \succ w\right\} \supset Z \cup Y_+ \quad \text{and} \quad Y_- \supset \left\{w \in X \mid \theta : w \succ x\right\},$$

which leads to $\mathbb{P}_{\mathscr{C}(\tilde{a})}[Y_-] > \mathbb{P}_{\mathscr{C}(\tilde{a})}\left[Z \cup Y_+\right]$. This contradicts equation (**??**), and proves the theorem for single-peaked preferences. □

*Proof (Theorem 5 for single-crossing preferences)* We reuse the same notations $x, \tilde{\theta}, Y, Z, s$ and $\tilde{a}$ as in the proof of Lemma 5. Let $\theta_m$ the median voter. Lemma 5 allows us to assume without loss of generality that the manipulators are all on the right of $\theta_m$, i.e. $\theta > \theta_m$ for all $\theta \in \mathsf{Manipulator}(s)$. Then, we have, once again, $M_{\tilde{a}} : x \gg z$ for all $z \in Z$.

Let now $\theta = \min \mathsf{Manipulator}(s)$ the most leftist manipulator. Denote $Y^+$ and $Y^-$ defined by

$$Y^+ = \{y \in Y \mid \theta : y \succ x\} \quad \text{and} \quad Y^- = \{y \in Y \mid \theta : x \succ y\}.$$

Contrary to the proof for single-peakedness, $Y^+$ now corresponds to the alternatives some manipulators prefer to $x$, as the sign " $+$ " now refers to $\theta$'s preference rather than the left-right line of alternatives.

Let $y^+ \in Y^+$. Since for any $\theta' \in \mathsf{Manipulator}(s)$, we have $\theta < \theta'$, single-crossing implies that $\theta' : y^+ \succ x$. Therefore, manipulators all disagree with the majority preference $M_{\tilde{\theta}} : x \gg y^+$, and hence, by Lemma 5, cannot invert it. Therefore, $M_{\tilde{a}} : x \gg y^+$. Since this holds for all $y^+ \in Y^+$, we have

$$Y^+ \subset \{w \in X \mid M_{\tilde{a}} : x \gg w\} \quad \text{and} \quad \{w \in X \mid M_{\tilde{a}} : w \gg x\} \subset Z \cup Y^-.$$

Yet, the fundamental property of the RCVS applied to $x$ then implies

$$\begin{aligned} \mathbb{P}_{\mathscr{C}(\tilde{a})}[Y^+] &\leq \mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[M_{\tilde{a}} : x \gg w\right] \\ &\leq \mathbb{P}_{w \sim \mathscr{C}(\tilde{a})}\left[M_{\tilde{a}} : w \gg x\right] \\ &\leq \mathbb{P}_{\mathscr{C}(\tilde{a})}\left[Z \cup Y^-\right]. \end{aligned}$$

But this contradicts the strict incentives for $\theta$ to conspire, i.e. $\mathbb{P}_{\mathscr{C}(\tilde{a})}[Y^+] > \mathbb{P}_{\mathscr{C}(\tilde{a})}\left[Z \cup Y^-\right]$. Thus, we reach the same conclusion for single-crossing preferences as we did for single-peaked ones. □