FAKULTÄT FÜR MATHEMATIK

DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Mathematics

A Formal Proof of the Incompatibility of *SD*-Efficiency and *SD*-Strategy-Proofness

Author:	Manuel Eberl
Supervisor:	Prof Dr Felix Brandt
Advisor:	Christian Geist, MSc
Date:	19 July 2016

FAKULTÄT FÜR MATHEMATIK

DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Mathematics

A Formal Proof of the Incompatibility of *SD*-Efficiency and *SD*-Strategy-Proofness

Author:	Manuel Eberl
Supervisor:	Prof Dr Felix Brandt
Advisor:	Christian Geist, MSc
Date:	19 July 2016

I hereby declare that this thesis is my own work and that no other sources have been used except those clearly indicated and referenced.

Garching, 19 July 2016 Manuel Eberl

Abstract

In the design of voting rules, there are three intuitively desirable properties that one might reasonably expect such a rule to fulfil:

- A voting rule should treat every voter and any alternative on the ballot equally.
- The result should satisfy the voters as far as possible; i. e. there should be no other result that is obviously better for everyone.
- No voter should be able to obtain an advantage by lying about her preferences.

These intuitively desirable properties have formal counterparts by the name of Anonymity and Neutrality, Efficiency, and Strategy-Proofness, respectively. It is well-known that the last two are in some way in conflict to one another – fulfilling both of them is often not possible or imposes great restrictions.

This work focuses on the setting of randomised voting with weak preferences (i. e. voters may submit preferences with ties), particularly on previous work by Brandl *et al.*, who used computerised search and SMT solvers to prove a conjecture by Aziz *et al.* that no anonymous and neutral randomised voting rule (known as Social Decision Scheme) can fulfil the notions of both SD-Efficiency and SD-Strategy-Proofness. My work consists of a fully mechanised formal proof of this result using the interactive theorem prover Isabelle and, based upon this, a human-readable pen-and-paper proof.

Contents

Acknowledgements

I would like to thank Felix Brandt for finding a topic that encompasses both my tentative interest in Social Choice Theory and my background in theorem proving. I also thank my advisor Christian Geist and my quasi-co-advisor Florian Brandl for their quick and helpful answers to my questions, which were often infused with the trademark pedantry of those socialised in the theorem-proving community.

My thanks also go to Lars Hupel and Kristina Magnussen for their proof-reading services.

1 Introduction

Efficiency and *Strategy-Proofness* are two important qualities of a voting rule: *Efficiency* states that the result should be optimal in the sense that one cannot give one voter a more favourable result without giving another voter a less favourable result, i. e. there is no way to truly improve the result in a way that all voters agree with. *Strategy-Proofness* states that no voter should have an incentive to lie, i. e. it must not be possible to achieve a better result by misrepresenting one's preferences. There are many different variants of Efficiency and Strategy-Proofness, depending on what is considered a better result.

This work focuses on randomised voting rules known as *Social Decision Schemes* (SDS), which do not return a single winner but a probability distribution over possible winners. To someone unfamiliar with Social Choice Theory, this may seem strange – why should the 'best' outcome be chosen randomly? The reason is that choosing a *single* winner deterministically is not always possible in a reasonable way. If half of the voters prefer a over b and the others prefer b over a, who should be the winner? Indeed, the well-known Gibbard–Satterthwaite theorem [Gib73; Bra+16] states that a deterministic voting rule that returns a single winner must exhibit at least one of the following undesirable behaviours if there are at least three alternatives on the ballot:

Dictatorial There is one voter who can determine the winner no matter what the preferences of the remaining voters are.

Imposing There is one alternative which can never win, no matter what the voters do.

Manipulable There is at least one situation where a voter has an incentive to lie.

Randomisation is an obvious way that one may consider to solve this problem: if half of the voters prefer a and the others prefer b, one can simply toss a coin to resolve the tie.

Unfortunately, randomisation does not solve all problems. As Gibbard [Gib77; Nan98] has also shown: if one demands, quite reasonably, that voting rules be *anonymous* (i. e. they treat all voters the same), then the only SDS that satisfies *ex-post*-Efficiency (a relatively weak kind of efficiency) and something known as strong *SD*-Strategy-Proofness is the rule of *Random Dictatorship*. This rule chooses a voter uniformly at random and decides that that voter's most-preferred alternative wins. This shows that even in the randomised setting, Efficiency and Strategy-Proofness are difficult to combine.

In this result by Gibbard, voters are required to have *linear ballots*, i. e. they need to submit their preferences as a list in order of decreasing preference with no ties allowed. In this work, we shall consider a more liberal setting where ties *are* allowed. The goal is to prove a conjecture by Aziz *et al.*: that any anonymous and neutral SDS (i. e. that treats all voters and alternatives equally) in this setting violates either *SD*-Strategy-Proofness or *SD*-Efficiency. *SD*, in this context, stands for *Stochastic Dominance*, which is one particular way to define whether the probability distribution returned by the SDS is preferred to another by a voter or not.

This conjecture was proven by Brandl *et al.* using a computer program that searches the space of preference profiles (i. e. ballots) of four voters and four alternatives and uses an SMT solver to check the consistency of the four conditions – Anonymity, Neutrality, *SD*-Efficiency, and *SD*-Strategy-Proofness – for 'interesting' sets of preference profiles. If an inconsistency is found, that proves that no such SDS can exist, and one can then easily show that no SDS for more voters or alternatives exists.

They did find such a set of profiles, but at that point, the 'proof' is merely of the form that a computer program says 'This is unsatisfiable'. While some SMT solvers *can* output a proof of the unsatisfiability, these proofs can again only be checked effectively by computers, since they are much too large and low-level for humans to read – so in the end, one still has to trust the correctness of the proof checker. This can be made less problematic by using a number of different SMT solvers to verify the result independently, but it is perhaps still not very satisfying to some mathematicians.

However, perhaps more importantly, it must be noted that the process of inspecting a set of profiles, deriving the set of conditions that arise from it, and translating them into the format of SMT was done by an unverified Java program. A bug in this program could easily lead to an incorrect proof, and past experience shows that unverified computer code used in mathematical proofs does often contain bugs that can potentially threaten the soundness of the proof (cf. Flyspeck by Hales *et al.* [Hal+15] and the Lorentz Attractor by Tucker [Tuc99]). The Java program by Brandl *et al.* outputs enough information on each condition for a human to be able to check the correctness of each of them, but considering that the SMT input contains 94 non-trivial conditions, this would still be a time-consuming and error-prone task for a human.

The goal of this project is therefore to address these two problems and increase the confidence in the validity of this proof by

- using the interactive theorem prover Isabelle to develop a fully machine-checked version of the entire proof, including the parts previously done by the Java program, the SMT solver, and informal pen-and-paper reasoning.
- developing a 'human-readable' version of the SMT proof, i. e. a proof that is both detailed and structured enough to enable a human to verify the validity of each step.

Both of these goals were achieved, and the formal Isabelle/HOL proof of the impossibility result [Ebe16b] and the required definitions and facts about Social Choice Theory [Ebe16a] are available in the *Archive of Formal Proofs*, which is a peer-reviewed repository of Isabelle/HOL proof developments that is continuously maintained by the Isabelle developers to ensure compatibility with future Isabelle releases despite the extensive changes to the infrastructure and the background theory with every new Isabelle release.

1.1 Related Work

I will now give a – probably incomplete – list of some important related work. In doing so, I will use some terminology that was not defined yet; some of it is defined in Section 3.

Bogomolnaia and Moulin [BM01] proved that anonymity, *SD*-Efficiency and *strong SD*-Strategy-Proofness are incompatible for *Random Assignments*. Since a Random Assignment can be constructed from an SDS (albeit on more alternatives), this implies that these properties are also inconsistent for SDSs.

Aziz *et al.* [ABB13] proved that this also holds for weak *SD*-Strategy-Proofness if restricted to majoritarian SDSs, i. e. SDSs that only depend on the pair-wise majority graph of the preference profile. A stronger result that allows the SDS to depend on the *weighted* majority graph followed [ABB14a], as well as related results for *all* SDSs, but with stronger notions of Efficiency and Strategy-Proofness. [ABB14a]

Brandl *et al.* [BBS16] then proved that there exists no anonymous and neutral SDS for four voters and alternatives that coincides with *Random Dictatorship* on strict preferences and satisfies both *SD*-Efficiency and weak *SD*-Strategy-Proofness; however, the lifting of this result to more than four voters and alternatives requires the additional restriction that the SDS ignores fully indifferent voters. This assumption is not present in the original paper; I discovered that it is necessary while trying to formalise the proof in Isabelle/HOL. The authors have confirmed this issue in personal communication and proposed the solution of adding the assumption about ignoring fully indifferent voters.

Finally, Brandl *et al.* [BBG16] proved the incompatibility of *SD*-Efficiency and weak *SD*-Strategy-Proofness for anonymous and neutral SDSs using SMT solvers – without the additional problematic assumption about Random Dictatorship. Their work forms the basis for this project, as this is the theorem that will be proven formally in this work.

In the course of this work, many important notions from Randomised Social Choice Theory have been developed in Isabelle and some important theorems about them have been proven in a fully formal and machine-checked way – probably for the first time. These developments are also available in the *Archive of Formal Proofs* [Ebe16a] and can be used for similar projects in the future.

1.2 Outline

I will now give a brief outline of the remainder of this thesis: Section 2 describes the tools used in this project: Isabelle/HOL, Z3, and QSopt_ex. Next, Section 3 defines the basic notions from Social Choice Theory that we will use and gives proofs for the basic facts required for the main proof. Section 4 describes the contributions of this work: The formalisation of Social Decision Schemes in Isabelle/HOL in Section 4.1, the Isabelle/HOL proof automation tools that form the verified counterparts to the Java program by Brandl *et al.* in Sections 4.2 and 4.3, and the human-readable proof of the main impossibility result in Section 4.4.

Finally, Section 5 summarises the results that were achieved and the lessons that were drawn from them, and the Appendix gives a list of all the preference profiles required by the proof and the facts derived from them with a justification for each of them.

2 Utilised Tools

I will now give a brief overview of the three tools that were used in this project.

2.1 Isabelle

Isabelle is a generic interactive theorem prover. *Interactive* means that the prover does not find the proof by itself like an automated theorem prover – the user must give it a sequence of steps to follow and the prover's automation fills in the gaps. This allows proofs of more complex theorems that are outside the scope of fully-automated theorem provers. *Generic* means that it supports different kinds of *object logics*, such as first-order logic, higher-order logic, and Zermelo–Fraenkel set theory. However, these days, Isabelle is mostly used in the form of Isabelle/HOL, i. e. with higher-order logic. The HOL of Isabelle/HOL is a typed logic with functions as first-class values that supports a simple form of polymorphism and Haskell-style type classes. Isabelle/HOL also provides many proof automation tools and mechanisms for the definition of e. g. recursive functions, inductive predicates, and recursive datatypes and co-datatypes.

The Isabelle distribution contains a large library of formalised general-purpose mathematics in HOL, including:

- natural numbers, integers, real and complex numbers
- algebraic type classes such as groups, rings, fields, vector spaces
- topology, limits, and infinite sums
- basic number theory and combinatorics
- univariate and multivariate real and complex analysis
- measure theory and probability theory

More specialised results and/or very large formalisations – such as model-checking algorithms, Landau symbols, the Central Limit Theorem – are available in a peer-reviewed online repository known as the *Archive of Formal Proofs* (AFP). Like the Isabelle distribution, the AFP is maintained by the Isabelle developers to ensure that its entries remain compatible with new Isabelle releases despite the fact that both the system itself and the background library change rapidly with each release.

One of the great advantages of Isabelle is the proof language *Isar*, which allows users to write structured, quasi-human-readable proofs instead of proof scripts consisting of proof tactic invocations. The structured style of Isar is much closer to the way a human would write a proof, although most Isar proofs are still far away from being understandable by someone unfamiliar with theorem provers. One reason for this is that many things that are dismissed as trivial in a pen-and-paper proof need to be made explicit in a formal proof, and often, concepts must be defined differently for technical reasons. Still, the reader is encouraged to have a look at the Isabelle/HOL proof of the main result with the Isabelle/jEdit IDE.

2.2 Z3

Z3 is a solver for *Satisfiability Modulo Theories* (SMT). The basic idea of this approach is to extend first-order Boolean satisfiability problems by replacing the Boolean variables in it with expressions in other logics, ideally logics with efficient decision procedures – such as uninterpreted functions or linear arithmetic. In practice, SMT solvers perform well mostly on quantifier-free formulæ. Fortunately, the problems that we shall look at are all quantifier-free linear real arithmetic (QF_LRA).

Z3 is integrated into Isabelle via the *smt* proof method [Böh09], which translates Isabelle/HOL goals into the SMTlib format – with much pre-processing, since Isabelle/HOL supports many features that do not exist in SMT, such as higher-order functions and polymorphism – and attempts to reconstruct an Isabelle proof from the Z3 proof. It should be noted that Z3 is one of the few SMT solvers that can produce proofs. Note that by *Isabelle proof*, we do not mean actual Isabelle proof text: *smt* does not produce Isabelle code; it constructs Isabelle theorems by emulating the Z3 proof rules with basic logical inference. Like the Z3 proofs, these reconstructed proofs are very large and low-level and therefore not human-readable.

2.3 QSOpt_ex

QSopt_ex [Esp06; App+07] is a Linear Programming solver (written in C) that uses exact arithmetic, i. e. it outputs the exact optimal solutions as rational numbers without any rounding errors. It was developed by Applegate *et al.* using their non-exact solver QSopt as a basis and uses a combination of fast, non-exact floating point operations and exact rational computations that use GMP arbitrary-precision rational numbers.

However, I do not use this version of QSopt_ex since I was unable to compile the code. Fortunately, there is a fork by Jon Lund Steffenson [Ste14] that provides a number of improvements, particularly to the build system. I created rudimentary bindings to interface with this version of QSopt_ex from Isabelle/ML by writing the problems into a problem description file in the LP format, invoking QSopt_ex on it, and parsing the result file.

Since the problems arising in the context of this work are very small, a simple Linear Programming solver written directly in Isabelle/ML would be a preferable solution and may be of interest as future work.

2.4 Trustworthiness

In some sense, Isabelle is the only one of the three tools that is still important in the final result: While the development process of the proof required heavy use of the other two external tools – the SMT solver Z3 (see Section 2.2) and the exact Linear Programming solver QSopt_ex (see Section 2.3) – we do *not* have to trust either of them. At any stage of the process, the proofs of the results presented here were fully machine-checked by the Isabelle kernel down to the axioms of the logic:

- Z3 was used in the form of the Isabelle proof method *smt* [Böh09], which translates an Isabelle goal into the SMTlib format, calls Z3, and constructs a (non-human-readable) Isabelle proof from the Z3 proof object. Therefore, proofs using *smt* are no less trustworthy than ordinary Isabelle proofs.

- QSopt_ex is used to solve linear programs arising in the context of Efficiency conditions, both to find and prove the conditions. The optimal assignment of a linear program (corresponding to a lottery of alternatives) is imported into Isabelle as a witness and the proof is then carried out within Isabelle using that witness.

However, even though we do not trust these third-party tools, using them in the Isabelle proof introduces a dependency on them. Since they are not under our control and may become unavailable in the future or change in ways that make them incompatible with the Isabelle interface, I have fully removed all dependencies on these tools in the final proof by

- replacing the *smt* proof with a fully structured Isar proof using 'regular' Isabelle proof methods

- writing down the inefficient supports to be proved along with their witnesses explicitly in the proof document instead of computing them anew every time.

Therefore, while Z3 and QSopt_ex were instrumental in developing the Isabelle proof, the final version of the proof does not require them anymore.

As for Isabelle, its trustworthiness is due to the following principle: Simply put, the only part of Isabelle that can produce theorems is the *inference kernel*. Any fact that is proven at any point needs to be reduced to basic inferences or axioms of the object logic (HOL in our case) and this is checked by the kernel. All of Isabelle's sophisticated proof automation machinery as well as the automation that was developed in this thesis is essentially untrusted code; a bug in one of these components can never lead to inconsistencies.

The inference kernel is still a sizeable piece of software, but certainly much smaller and more rigorously-tested than the remainder of Isabelle. Also, over the course of the last two decades, some Isabelle developers have attempted to prove the relative consistency of the Isabelle kernel (modulo possible implementation mistakes); the most recent one is the work by Kunčar and Popescu [Kun15; KP15].

3 Preliminaries

Let us now turn to the concepts of Social Choice Theory that are required to state and prove the main result. Everything in this section is essentially Social Choice Theory folklore; all of the results are well-known and were not invented by me. However, in most cases, the Isabelle/HOL formalisation is probably the first formal and machine-checked version of the definitions and theorems.

Now, first of all, we need to define the basic setting for the remainder of this work: What assumptions do we have about the alternatives, the voters (which will, from now on, be called *agents*) and their preferences?

We will consider *elections*[1] consisting of an *agenda* – a non-empty finite set of *alternatives* – and an *electorate* – a non-empty finite set of *agents*. Each agent has *preferences* over the alternatives, which are modelled as relations. The goal is now to devise a *voting rule* that looks at the combined preferences of all the agents (known as a preference profile) and determines the *winning alternative*.

As mentioned in the introduction, in this work, we shall focus on a particular class of randomised voting rules known as *Social Decision Schemes*. These return a *lottery* of alternatives, i. e. a discrete probability distribution over winning alternatives. I will use $\Delta(A)$ to denote the set of lotteries over the set A.

We denote the set of agents with $N = \{1 \ldots n\}$ and the set of alternatives with A and $|A| = m$. Preference profiles are written as R, and the preference relation of the i-th candidate in a profile R is written as $\succeq_{R(i)}$, where $x \succeq_{R(i)} y$ means 'x is at least as good as y in the opinion of voter i.' In our setting, the relations $\succeq_{R(i)}$ will always be required to be *total preorders*, i. e.

Reflexive: $x \succeq_{R(i)} x$ for any $x \in A$.

Transitive: if $x \succeq_{R(i)} y$ and $y \succeq_{R(i)} z$ for any $x, y, z \in A$, then also $x \succeq_{R(i)} z$.

Total: for any $x, y \in A$, at least one of $x \succeq_{R(i)} y$ and $y \succeq_{R(i)} x$ holds.

Note that we consider *weak preferences*, so the relations do *not* have to be antisymmetric, i. e. $x \succeq_{R(i)} y$ and $y \succeq_{R(i)} x$ may both hold even if $x \neq y$.

If $x \succeq_{R(i)} y$ and $y \succeq_{R(i)} x$, we say that i is *indifferent* between x and y and write this as $x \sim_{R(i)} y$. Since $\sim_{R(i)}$ is an equivalence relation, it gives rise to equivalence classes, which we call the *indifference classes* of $R(i)$.

It is obvious that any finite total preorder can be written uniquely as a *weak ranking*: a list of its indifference classes in order of decreasing preference (i. e. best alternatives first). This format will be used to specify preference profiles both in this work and in the formal Isabelle/HOL proof text.

[1] The term *election* is rather non-standard, but it was convenient in the formalisation: It is simply the combination of an electorate and an agenda. It does not yet contain the preferences of the agents or a voting rule.

3.1 Anonymity and Neutrality

The most obvious demand that one may have of a voting rule is that it is not biased, i. e. it should treat all agents and all alternatives the same. This is captured formally as the requirement that permuting the agents or alternatives does not change the result. For the agents, this is called *Anonymity*; for the alternatives, it is called *Neutrality*.

Definition 1 (Anonymity)**.** *An SDS f is anonymous if, for any permutation $\pi : N \to N$:*

$$f(R \circ \pi) = f(R)$$

Definition 2 (Permuting Relations and Profiles)**.** *For a relation $\succeq$ on A and a permutation $\sigma : A \to A$, we define the* permuted relation $\succeq^\sigma$ *as:*

$$x \succeq^\sigma y \longleftrightarrow \sigma^{-1}(x) \succeq \sigma^{-1}(y)$$

It is clear that if $\succeq$ is a (total) preorder, then $\succeq^\sigma$ is again a (total) preorder.

For a finite total preorder, the weak ranking of $\succeq^\sigma$ can easily be obtained from the weak ranking of $\succeq$ by renaming all elements with σ; e. g. for $\sigma = (a\ b\ c\ d)$ and $\succeq = (\{a\}, \{b\}, \{c, d\})$, we have $\succeq^\sigma = (\{b\}, \{c\}, \{d, a\})$.

For a preference profile $R = (R(1) \dots R(n))$ and a permutation σ of the alternatives, we then define the permuted profile $R^\sigma = (R(1)^\sigma \dots R(n)^\sigma)$.

Definition 3 (Neutrality)**.** *We say that an SDS f is neutral if, for any permutation $\sigma : A \to A$ and any alternative $x \in A$:*

$$f(R^\sigma)(\sigma(x)) = f(R)(x)$$

i. e. when renaming the alternatives, the output lottery is the same as the original lottery, but with all alternatives renamed accordingly.

3.2 Pareto Preference

An interesting situation in an election is when all agents agree on something: If all agents think that x is at least as good as y, we say that x is (weakly) *Pareto-preferred* to y. Formally:

Definition 4 (Pareto preference)**.** *For a preference profile R, we define the Pareto-preference relation as:*

$$x \succeq_{\mathit{Pareto}(R)} y \longleftrightarrow \forall i \in N.\ x \succeq_{R(i)} y$$

The strict part of this relation is also interesting: $x \succ_{\mathit{Pareto}(R)} y$ means that all agents think that x is at least as good as y, and at least one agent thinks that x is strictly better than y. We than say that x is *strongly Pareto-preferred* to y, or that y is *Pareto-dominated* by x. We also call y a *Pareto loser*. Intuitively, a Pareto loser is an undesirable outcome in an election, since one can make one agent better off without making any other agent worse off by simply returning the Pareto-dominating alternative instead.

More generally, one can see *Pareto* as a function that sends a family of preorders (i. e. a tuple/set/multiset of preorders) to a single preorder. This view will be convenient for the definition of *SD*-Efficiency.

The Pareto preorder of a family of preorders is *not* total, even for a family of total preorders – unless the family agrees on everything, which is surely too much to expect.

3.3 Stochastic Dominance

For the definition of the concepts of Efficiency and Strategy-Proofness, we will require a way to determine whether an agent prefers one outcome of the election to another. Since our outcomes are not single alternatives, but *lotteries over alternatives*, we need a way to lift the agents' preferences over alternatives to preferences over lotteries. Essentially, we are looking for a function that sends a preorder on a set A to a preorder on $\Delta(A)$. Such a function is called a 'lottery extension':

One such lottery extension is *Stochastic Dominance* (*SD*). The informal definition of this is the following:

> 'A lottery p is considered at least as good as a lottery q if for all alternatives $x \in A$, the probability of getting a result that is at least as good as x in p is greater than or equal to the probability of getting something at least as good as x in q.'

More formally:

Definition 5 (Stochastic Dominance)**.** *For a given preorder $\succeq$ on A, we define the associated Stochastic Dominance preorder $SD(\succeq) \subseteq \Delta(A) \times \Delta(A)$ as*

$$p \succeq_{SD} q \longleftrightarrow \forall x{\in}A.\ \mathrm{P}_p(\{y \in A \mid y \succeq x\}) \geq \mathrm{P}_q(\{y \in A \mid y \succeq x\})$$

Utilitarian View on Stochastic Dominance. It turns out that this definition is, in fact, equivalent to another perhaps more intuitive definition using utility functions. A utility function assigns to any alternative a real number that indicates how much utility the agent derives from this alternative. A higher utility corresponds to a more preferred alternative.

Definition 6. *A von Neumann–Morgenstern (vNM) utility function for alternatives A is a function $u : A \to \mathbb{R}$. We say that u is consistent w. r. t. a preference relation $\succeq$ if*

$$x \succeq y \longleftrightarrow u(x) \geq u(y)\ .$$

In particular, note that the preference is strict iff the inequality on u is strict, and there is an indifference between two alternatives iff they have the same utility.

The informal formulation of the utilitarian view of Stochastic Dominance is then [ABB14b]:

> 'A lottery p is considered at least as good as a lottery q if for *all* von Neumann–Morgenstern utility functions u consistent with $\succeq$, the expected utility w. r. t. p is at least as high as the expected utility w. r. t. q.'

Formally:

Theorem 1 (Utilitarian view of Stochastic Dominance)**.** *Let A be a finite non-empty set, $\succeq$ a total preorder on A, and vNM($\succeq$) $\subseteq \mathbb{R}^A$ the set of all vNM utility functions consistent with $\succeq$. Then:*

$$p \succeq_{SD} q \longleftrightarrow \forall u{\in}vNM(\succeq).\ \mathrm{E}_p[u] \geq \mathrm{E}_q[u]$$

To prove this, we first prove the following auxiliary fact on expected utilities and indifference classes:

Lemma 2. *Let $\succeq$ be a total preorder on the finite non-empty set A, $p{\in}\Delta(A)$, and u a vNM utility function that is consistent with $\succeq$. Furthermore, let $I_i \dots I_l$ be the weak ranking of $\succeq$, i. e. the descending sequence of its indifference classes. Then:*

$$\mathrm{E}_p[u] = u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}(u(I_i) - u(I_{i+1}))$$

Proof. First of all, note that the expressions $u(I_i)$ are well-defined, since all alternatives in an indifference class have the same utility. For an alternative $y{\in}A$, we write $y \succeq I_i$ to mean 'y is at least as good as the alternatives in I_i'. Note that if $i < l$, we have $y \succeq I_i \longleftrightarrow y \succ I_{i+1}$. The proof is then a simple telescoping argument:

$$\begin{aligned}
\mathrm{E}_p[u] &= \sum_{x\in A} p(x)u(x) = \sum_{i=1}^{l} \mathrm{P}_p(I_i)u(I_i) = \\
&= \sum_{i=1}^{l} \mathrm{P}_p(\{y{\in}A \mid y \succeq I_i\} \setminus \{y{\in}A \mid y \succ I_i\})u(I_i) = \\
&= \sum_{i=1}^{l} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}u(I_i) - \sum_{i=1}^{l} \mathrm{P}_p\{y{\in}A \mid y \succ I_i\}u(I_i) = \\
&= \underbrace{\mathrm{P}_p\{y{\in}A \mid y \succeq I_l\}}_{=1} u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}u(I_i) - \\
&\qquad \underbrace{\mathrm{P}_p\{y{\in}A \mid y \succ I_0\}}_{=0} u(I_0) + \sum_{i=2}^{l} \mathrm{P}_p\{y{\in}A \mid y \succ I_i\}u(I_i) = \\
&= u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}u(I_i) - \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid \underbrace{y \succ I_{i+1}}_{y \succeq I_i}\}u(I_{i+1})
\end{aligned}$$

$$= u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}(u(I_i) - u(I_{i+1}))$$

□

We can now prove Theorem 1:

Proof.
For the ⟶ direction, assume $p \succeq_{SD} q$ as defined initially. Let $I_1, \ldots, I_l$ be the weak ranking of $\succeq$. We then have:

$$\mathrm{E}_p[u] \overset{\text{Lemma 2}}{=} u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_p\{y{\in}A \mid y \succeq I_i\}(u(I_i) - u(I_{i+1})) \overset{p\ \succeq_{SD}\ q}{\geq}$$
$$\geq u(I_l) + \sum_{i=1}^{l-1} \mathrm{P}_q\{y{\in}A \mid y \succeq I_i\}(u(I_i) - u(I_{i+1})) \overset{\text{Lemma 2}}{=} \mathrm{E}_q[u]$$

Now, for the ⟵ direction, assume

$$\forall u{\in}\mathit{vNM}(\succeq).\ \mathrm{E}_p[u] \geq \mathrm{E}_q[u]\ . \tag{$*$}$$

Let $x \in A$. We now need to show that

$$\mathrm{P}_p\{y \in A \mid y \succeq x\} \geq \mathrm{P}_q\{y \in A \mid y \succeq x\}\ .$$

Ideally, we would like to choose the utility function

$$u(y) := \begin{cases} 1 & \text{if } y \succeq x \\ 0 & \text{otherwise} \end{cases}$$

since the expected value of u is then precisely the probability that $y \succeq x$. However, this u is *not* consistent with $\succeq$, since u assigns the same utility of 1 to all alternatives that are at least as good as x and the same probability 0 to all those that are not, i. e. alternatives that are ranked equally with x receive the same utility as alternatives that are strictly better than x.

The idea now is to make u consistent with $\succeq$ by introducing a small bias towards better alternatives and letting the magnitude of this bias tend to 0. To do this, we consider the weak ranking $I_1 \ldots I_l$ of $\succeq$ and define $i(y)$ to be the index of y in the weak ranking, i. e. the unique i such that $y \in I_i$. Now define the family of utilities

$$u_\varepsilon(y) := u(y) + \varepsilon(l - i(y))$$

for any $\varepsilon > 0$. It is clear that this is a vNM utility function that is consistent with $\succeq$. Then:

$$\begin{aligned}
\mathrm{P}_q\{y \in A \mid y \succeq x\} &\le \sum_{y \succeq x} q(y) + \varepsilon \sum_{y \in A} (l - i(y)) q(y) = \mathrm{E}_q[u_\varepsilon] \overset{(*)}{\le} \\
&\le \mathrm{E}_p[u_\varepsilon] = \sum_{y \succeq x} p(y) + \varepsilon \sum_{y \in A} (l - i(y)) p(y) \le \sum_{y \succeq x} p(y) + \varepsilon \cdot l = \\
&= \mathrm{P}_p\{y \in A \mid y \succeq x\} + \varepsilon \cdot l
\end{aligned}$$

Since l is fixed and this holds for all $\varepsilon > 0$, we can conclude

$$\mathrm{P}_p\{y \in A \mid y \succeq x\} \ge \mathrm{P}_q\{y \in A \mid y \succeq x\}$$

by letting ε tend to 0. □

A non-trivial consequence of this is the following interpretation of 'not strictly *SD*-preferred':

Theorem 3. *Let A be a finite non-empty set, $\succeq$ a total preorder on A, then:*

$$p \not\succ_{SD} q \longleftrightarrow \exists u \in vNM(\succeq).\ \mathrm{E}_p[u] \le \mathrm{E}_q[u]$$

Proof. Omitted since this fact is not required for the results in this work. (There is, however, a machine-checked Isabelle proof) □

Corollary 4.

$$\begin{aligned}
p \not\succeq_{SD} q &\longleftrightarrow \exists u \in vNM(\succeq).\ \mathrm{E}_p[u] < \mathrm{E}_q[u] \\
p \succ_{SD} q &\longleftrightarrow \forall u \in vNM(\succeq).\ \mathrm{E}_p[u] > \mathrm{E}_q[u] \\
p \parallel_{SD} q &\longleftrightarrow \exists u_1, u_2 \in vNM(\succeq).\ \mathrm{E}_p[u_1] > \mathrm{E}_q[u_1] \wedge \mathrm{E}_p[u_2] < \mathrm{E}_q[u_2]
\end{aligned}$$

where $\parallel$ denotes incomparability.

These theorems and corollaries now imply the following justification of the concept of Stochastic Dominance: If we assume that agents have utility functions and attempt to maximise their expected utility, the agent will always choose p over q if $p \succ_{SD} q$ holds.

Note the characterisation of $\parallel_{SD}$ in Corollary 4. This shows that *SD* is usually *not* total, even if the original preorder on alternatives was total.

Example 1. *For the set of alternatives $A = \{a, b, c\}$ and the preference order $a \succ b \succ c$, the lotteries b and $1/2\, a + 1/2\, c$ are incomparable.*

Singleton lotteries and *SD*. We can also prove the following interesting special case of Stochastic Dominance where one of the lotteries is a singleton lottery (i. e. its support consists of only one alternative):

Corollary 5. *Let $\succeq$ be a preorder on the (not necessarily finite and possibly empty) set A. Let p be a lottery on A and $x \in A$. Then*

$$x \succeq_{SD} p \longleftrightarrow \forall y \in \text{supp}(p).\ x \succeq y$$
$$p \succeq_{SD} x \longleftrightarrow \forall y \in \text{supp}(p).\ y \succeq x$$

where the x on the left-hand side of the equivalence is the singleton lottery that returns x almost-surely.

Proof. Omitted. (As always, there is an Isabelle/HOL proof) □

3.4 Efficiency

We now define the notion of *Efficiency*. The intuition behind Efficiency is the following: if the outcome p (in our case: a lottery) of an election is such that there exists another outcome q that is strictly 'better' – in some specific sense – then the voting rule should not have returned p in the first place, since there are obviously better choices (such as q).

The question is: What does it mean for one lottery to be better than another? There are a number of ways to define this.

3.4.1 *Ex-Post*-Efficiency

One obvious case where a lottery can be considered inefficient is when it contains Pareto losers: By definition, if x is a Pareto loser, there is another alternative y such that all agents consider y to be at least as good as x and at least one voter considers y to be strictly better than x. Therefore, simply returning y instead of x yields an outcome that can reasonably be described as strictly better for that one agent and at least as good for all other agents.

Definition 7. *A lottery is called ex-post-efficient if it has no Pareto losers in its support. An SDS is called ex-post efficient if, for any preference profile R, it returns a lottery that is ex-post-efficient w. r. t. R.*

3.4.2 *SD*-Efficiency

Another natural way to compare lotteries is to use lottery extensions. Recall that a lottery extension lifts an agent's preference relation on *alternatives* to a preference relation on *lotteries*. If we now combine all of these preference relations on lotteries into a single relation, we can compare two results of an election. The obvious choice for this is Pareto dominance – i. e. we consider a lottery at least as good as another when *all* agents agree that this is the case. This can be captured formally as follows:

Definition 8 (*SD*-Efficiency)**.** *A lottery p is called SD-efficient w. r. t. a profile R if*

$$\nexists q \in \Delta(A).\ q \succ_{\mathit{Pareto}(SD \circ R)} p\ .$$

(Recall that R is a function that maps an agent to her preference relation, and $SD$is a function that maps a relation to a relation on lotteries. Then $SD \circ R$ is a family of preorders on lotteries, and Pareto is a function that sends families of preorders to preorders.)

Stated more explicitly, this means:

$$\nexists q{\in}\Delta(A).\ (\forall i{\in}N.\ q \succeq_{SD(R(i))} p) \wedge (\exists i{\in}N.\ q \succ_{SD(R(i))} p)\ .$$

An SDS is then called SD-efficient if, for any preference profile R, it returns a lottery that is SD-efficient w. r. t. R.

Corollary 4 then implies the following characterisation of SD-Efficiency:

Corollary 6. *A lottery p is SD-efficient iff there exists no other lottery q that yields at least the same expected utility for all agents and strictly more utility for at least one agent, no matter what their utility functions are.*

In other words: For any other lottery q, either

- *q yields less expected utility for at least one agent and one particular utility function, or*
- *p and q yield the same expected utility for all agents, no matter what their utility functions are (i. e. p and q are equivalent modulo the indifference classes of the agents).*

***SD*-Efficiency and supports.** An interesting property of SD-efficiency is that it does not depend on the exact probabilities of the lottery at all, but only on the support of the lottery. To show this, we first look at the following characterisation of SD-inefficiency:

Theorem 7. *Let R be a preference profile and $p \in \Delta(A)$ an SD-inefficient lottery w. r. t. R. Then all lotteries $p' \in \Delta(A)$ with supp$(p') \supseteq$ supp(p) are also SD-inefficient w. r. t. R.*

Proof. Since p is inefficient, there exists a lottery q with $q \succ_{\mathit{Pareto}(SD \circ R)} p$. We let

$$\varepsilon := \min \left\{ \frac{p'(x)}{p(x) - q(x)} \,\middle|\, x \in A, p(x) > q(x) \right\}\ .$$

Note that the set is non-empty since $p \neq q$. Next, we define

$$q'(x) := p'(x) - \varepsilon(p(x) - q(x))\ .$$

Since $\operatorname{supp}(p) \subseteq \operatorname{supp}(p')$ and A is finite, it is clear that $\varepsilon > 0$. We then have $q'(x) \geq 0$: if $p(x) \leq q(x)$, this is obvious; if $p(x) > q(x)$, we have, by construction, $\varepsilon(p(x) - q(x)) \leq p'(x)$ and therefore also $q'(x) \geq 0$. Moreover, we have

$$\sum_{x \in A} q'(x) = \sum_{x \in A} p'(x) - \varepsilon \sum_{x \in A} p(x) + \varepsilon \sum_{x \in A} q(x) = 1 - \varepsilon + \varepsilon = 1$$

Therefore, $q'(x)$ is a well-defined lottery. For any vNM utility function u, the expected utility w. r. t. q' is:

$$\mathrm{E}_{q'}[u] = \mathrm{E}_{p'}[u] + \varepsilon(\mathrm{E}_q[u] - \mathrm{E}_p[u]) \tag{$*$}$$

Since $q \succsim_{\mathit{Pareto}(SD \circ R)} p$, we know that for any agent i and any vNM utilities u consistent with $R(i)$, $\mathrm{E}_q[u] \geq \mathrm{E}_p[u]$. Therefore, due to $\varepsilon > 0$ and $(*)$, we also have $\mathrm{E}_{q'}[u] \geq \mathrm{E}_{p'}[u]$ and therefore $q' \succsim_{\mathit{Pareto}(SD \circ R)} p'$.

Moreover, since $q \not\precsim_{\mathit{Pareto}(SD \circ R)} p$, there exists an agent i and a vNM utility u consistent with $R(i)$ such that $\mathrm{E}_q[u] > \mathrm{E}_p[u]$. With $\varepsilon > 0$ and $(*)$, we then have $\mathrm{E}_{q'}[u] > \mathrm{E}_{p'}[u]$ and therefore $q' \not\precsim_{\mathit{Pareto}(SD \circ R)} p'$. In conclusion, we have shown that $q' \succ_{\mathit{Pareto}(SD \circ R)} p'$ and therefore p' is not SD-efficient w. r. t. R. □

Corollary 8. *A lottery $p \in \Delta(A)$ is SD-efficient iff all lotteries with the same support are SD-efficient.*

Definition 9 (SD-Efficiency of supports)**.** *Corollary 8 justifies speaking of efficient and inefficient supports. We call a support SD-efficient (resp. SD-inefficient) if the lotteries with this support are SD-efficient (resp. SD-inefficient).*

***SD*-Efficiency and *ex-post*-Efficiency.** We can now also examine how SD-Efficiency relates to Pareto losers and *ex-post*-Efficiency:

Corollary 9. *Given a preference profile R and an alternative x, the following four statements are equivalent:*

(*a*) *x is a Pareto loser.*

(*b*) *The singleton lottery x is SD-inefficient.*

(*c*) *$\{x\}$ is an SD-inefficient support.*

(*d*) *All supports that include x are SD-inefficient.*

In particular, this shows that the singleton SD-inefficient supports are precisely those that consist of a single Pareto loser. We can therefore decide the SD-efficiency of singleton supports particularly easily by checking whether the alternative is a Pareto loser.

Proof. To show (a) ⇒ (b), suppose x is a Pareto loser. Then there exists some y such that $y \succ_{\mathit{Pareto}(R)} x$ and therefore, using Corollary 5, also $y \succ_{\mathit{Pareto}(SD \circ R)} x$. Therefore, the singleton lottery x is SD-inefficient.

Conversely, to show (b) ⇒ (a), suppose x is SD-inefficient. Then there exists a lottery $q \in \Delta(A)$ such that $q \succ_{\mathit{Pareto}(SD \circ R)} x$. Using Corollary 5, this implies that $y \succ_{\mathit{Pareto}(R)} x$ holds for all $y \in \mathrm{supp}(q)$. Since the support of a lottery must be non-empty, there is at least one such y and therefore y strictly Pareto-dominates x.

We have thus shown the equivalence of (a) and (b). The equivalence of (b), (c), and (d) is an instance of Theorem 7 and Corollary 8. □

This directly implies that *SD*-Efficiency is a stronger notion than *ex-post*-Efficiency:

Corollary 10. *Any SD-efficient SDS f is also ex-post-efficient.*

Proof. This follows directly from the previous corollary: if x is a Pareto loser and x were in the support of $f(R)$, then $f(R)$ would be *SD*-inefficient. □

The essence of *SD*-efficiency. To summarise: Given a preference profile R, we can break down the consequences of *SD*-efficiency for an SDS f to requiring that the support of $f(R)$ is not one of the (finitely many) inefficient supports. This can be simplified even more, since any superset of an inefficient support is also inefficient: We must require that $f(R)$ not be a superset of any inclusion-minimal inefficient support, i. e. that for each inefficient support X, there exists an $x \in X$ such that $f(R)(x) = 0$.

For any given preference profile R, *SD*-efficiency of f therefore boils down to a finite number of conditions, each of which is of the form $f(R)(x_1) = 0 \vee \ldots \vee f(R)(x_n) = 0$. However, what is still missing is a way to actually *compute* these inclusion-minimal inefficient supports. To do this, we can use the following observation:

Observation 1. *The SD-Inefficiency of a support B is equivalent to the SD-Inefficiency of the uniform distribution $\mathcal{U}(B)$. Moreover, $\mathcal{U}(B)$ is inefficient iff there exists some $q \in \Delta(A)$ such that, for each agent $i \in N$ and each alternative $x \in A$, the inequality*

$$\mathrm{P}_q\{y \in A \mid y \succeq_{R(i)} x\} \geq \mathrm{P}_{\mathcal{U}(B)}\{y \in A \mid y \succeq_{R(i)} x\}$$

holds, and at least one of those inequalities needs to be strict. This can be expressed by introducing a slack variable $r_{i,x}$ for each inequality and requiring that all slack variables be non-negative and their sum be positive.

Whether or not this is possible can be decided by solving the following linear program and checking whether the optimal solution is non-zero:

$$\begin{aligned}
\text{maximise} \quad & \sum_{i\in N}\sum_{x\in A} r_{i,x} \quad \text{over } q_x \text{ for } x\in A \text{ and } r_{i,x} \text{ for } i\in N, x\in A \\
\text{such that} \quad & \forall x\in A.\ q_x \geq 0 \quad \text{and} \quad \sum_{x\in A} q_x = 1 \\
\text{and} \quad & \forall i\in N.\ \forall x\in A.\ r_{i,x} \geq 0 \\
\text{and} \quad & \forall i\in N.\ \forall x\in A.\ \sum_{y \succeq_{R(i)} x} q_y = r_{i,x} + \frac{|\{y \in B \mid y \succeq_{R(i)} x\}|}{|B|}
\end{aligned}$$

In fact, any such (not necessarily optimal) solution of this linear program is an easy-to-check certificate for the SD-Inefficiency of B if its value is non-zero; conversely, any optimal solution with a value of 0 is a certificate for the SD-Efficiency of B (combined with a solution to the dual program).

We can actually reduce this a little more: instead of considering every alternative $x \in A$ for every agent $i \in N$, it suffices to consider one alternative from each indifference class for every agent $i \in N$, and we can ignore the least-preferred indifference class for each agent, since the inequalities simplify to $1 \leq 1$ for least-preferred elements. We therefore have $k - 1$ equations for every agent, where k is the number of indifference classes of that agent.

This effectively reduces deciding the SD-Efficiency of a support to a linear program, which can be solved easily using a Linear Programming solver. One can then find all inclusion-minimal SD-inefficient supports by starting with a single alternative and adding alternatives until the support thus obtained becomes inefficient.

Example 2. *Consider the following preference profile:*

$$R: \quad \{b,d\},\{a,c\} \qquad \{c,d\},\{a,b\} \qquad a,b,\{c,d\} \qquad a,c,\{b,d\}$$

By solving the corresponding linear programs, we find that the only inclusion-minimal SD-inefficient support is $\{b,c\}$. For illustration, the linear program[2] *corresponding to the support $\{b,c\}$ is:*

$$\begin{aligned}
\text{maximise} \quad & r_{1,1} + r_{2,1} + r_{3,1} + r_{3,2} + r_{4,1} + r_{4,2} \\
\text{such that} \quad & q_a + q_b + q_c + q_d = 1 \\
\text{and} \quad & q_b + q_d = r_{1,1} + {}^1\!/_2 \\
\text{and} \quad & q_c + q_d = r_{2,1} + {}^1\!/_2 \\
\text{and} \quad & q_a = r_{3,1} \\
\text{and} \quad & q_a + q_b = r_{3,2} + {}^1\!/_2 \\
\text{and} \quad & q_a = r_{4,1} \\
\text{and} \quad & q_a + q_c = r_{4,2} + {}^1\!/_2
\end{aligned}$$

Note the correspondence of each of the equations (except for the first) to an indifference class of an agent.

[2] Note that, by convention, all variables in a Linear Programming problem are implicitly assumed to be non-negative unless other bounds are specified explicitly.

The same problem written in the LP format is:

```
MAXIMIZE
    r1_1 + r2_1 + r3_1 + r3_2 + r4_1 + r4_2
SUBJECT TO
    qa + qb + qc + qd = 1
    - r1_1 + 2 qb + 2 qd = 1
    - r2_1 + 2 qc + 2 qd = 1
    - r3_1 + 2 qa = 0
    - r3_2 + 2 qa + 2 qb = 1
    - r4_1 + 2 qa = 0
    - r4_2 + 2 qa + 2 qc = 1
END
```

The (abridged) solution that QSOpt_ex outputs is:

```
status = OPTIMAL
status OPTIMAL
Value = 2
VARS:
r4_1 = 1
r3_1 = 1
qd = 1/2
qa = 1/2
```

Note that all variables not present in the solution have value 0 by convention. The witness lottery is therefore $1/2a + 1/2d$. *We can conclude that* $\{b, c\}$ *is inefficient and* $f(R)(b) = 0 \lor f(R)(c) = 0$.

3.5 Strategy-Proofness

Strategy-Proofness is again motivated by a very simple intuitive demand: No agent should be able to obtain a better result for herself by misrepresenting her preferences. There are two ways to capture this intuition formally:

- The outcome that an agent obtains when she submits her true preferences is always at least as good as the outcome that she gets with the manipulated preferences.
- The outcome that an agent obtains when she submits manipulated preferences is never strictly better than the outcome that she gets if she submits her true preferences.

While these two formulations sound equivalent, there is a subtle difference: Recall that lottery extensions are typically *not* total. In particular, Stochastic Dominance, which we will use, is not total and therefore 'at least as good as' is a much stronger statement than 'not worse'. In fact, recall Theorems 1 and 3:

$$p \succeq_{SD} q \longleftrightarrow \forall u \in vNM(\succeq).\ \mathrm{E}_p[u] \geq \mathrm{E}_q[u]$$
$$p \not\prec_{SD} q \longleftrightarrow \exists u \in vNM(\succeq).\ \mathrm{E}_p[u] \geq \mathrm{E}_q[u]$$

In other words: p is *at least as good* as q (w. r. t. SD) iff p yields at least as much expected utility than q no matter what the agents utility function is. On the other hand, p is already considered *no worse* than q (w. r. t. SD) iff p yields at least as much expected utility than q for *at least one* utility function. The first formulation is therefore considerably stronger than the second one.

This leads to the following two notions of Strategy-Proofness:

Definition 10. *For a preference profile R, we write $R[i := \succeq']$ for the profile obtained from R by replacing the preferences of agent i with the alternative preference relation $\succeq'$.*

Then, we say that an SDS f is strongly strategy-proof if for all preference profiles R, all agents i, and any total preorder $\succeq'$:

$$f(R) \succeq_{SD(R(i))} f(R[i := \succeq'])$$

We say that f is weakly strategy-proof (or just strategy-proof) if for all preference profiles R, all agents i, and any total preorder $\succeq'$:

$$f(R) \not\prec_{SD(R(i))} f(R[i := \succeq'])$$

As explained before, these notions can be stated more intuitively as:

> 'No agent can obtain more expected utility by misrepresenting her preferences . . .
>
> . . . no matter what her utility function is (in case of strong Strategy-Proofness).
>
> . . . for at least one particular utility function (in case of weak Strategy-Proofness).'

3.6 Lifting

We will now explore how an SDS for a given set of agents and alternatives can be lowered to an SDS for a smaller set of agents and alternatives – and consequently, how impossibility results for SDSs for a certain number of agents and alternatives can be lifted to more agents and alternatives.

Suppose we have an electorate N_2 and an agenda A_2. Now fix some arbitrary sub-electorate N_1 of N_2 and some sub-agenda A_1 of A_2. All of these must, of course, be non-empty.

Definition 11 (Lifting Preference Profiles)**.** *Let R be a preference profile of N_1 and A_1. We now define the lifted preference profile $\bar{R}$ such that*

- *all agents in N_1 have the same preferences w. r. t. A_1 as they do in R.*
- *all agents in N_1 strictly prefer every alternative in A_1 to every alternative in $A_2 \setminus A_1$.*
- *all agents in N_1 are indifferent between all alternatives in $A_2 \setminus A_1$.*
- *all agents in $N_2 \setminus N_1$ are indifferent between all alternatives.*

This lifting mechanism has the following convenient properties:

Lemma 11.

(a) *For any permutation π of N_1, we have $\overline{R \circ \pi} = \bar{R} \circ \pi$.*

(b) *For any permutation σ of A_1, we have $\overline{R^\sigma} = \bar{R}^\sigma$.*

(c) *The Pareto losers of $\bar{R}$ are the Pareto losers of R plus all alternatives in $A_2 \setminus A_1$.*

(d) *For every agent i in N_1 and any $p, q \in \Delta(A_1)$, we have $p \succeq_{SD(\bar{R}(i))} q \longleftrightarrow p \succeq_{SD(R(i)} q$.*

(e) *For every agent i in $N_2 \setminus N_1$ and any $p, q \in \Delta(A_2)$, we have $p \sim_{SD(\bar{R}(i)} q$.*

(f) *Therefore, if a lottery $p \in \Delta(A_1)$ is SD-efficient w. r. t. $\bar{R}$, it is also in $\Delta(A_2)$ and SD-efficient w. r. t. R.*[3]

Proof. All of these facts follow rather directly from the definitions, so the exact proofs will not be printed here. □

We can now use lifting of profiles to lower an SDS for N_2 and A_2 to one for N_1 and A_1:

Lemma 12 (Lowering SDSs)**.** *Let f be an ex-post-efficient SDS for N_2 and A_2. We define $\bar{f}(R) := f(\bar{R})$.*

To show that this is well-defined, we must show that $\bar{f}(R) \in \Delta(A_1)$, i. e. for any preference profile R on N_1 and A_1, no alternative from $A_2 \setminus A_1$ is in the support of $\bar{f}(R) = f(\bar{R})$. This is obviously the case, since the alternatives in $A_2 \setminus A_1$ are Pareto losers w. r. t. $\bar{R}$ and f is ex-post-efficient.

We still need to justify that Anonymity / Neutrality / ex-post-Efficiency / SD-Efficiency / SD-Strategy-Proofness carry over. This follows easily from Lemma 11, so the exact proofs will be omitted here.

Corollary 13 (Lifting Impossibility Results)**.** *Consider an impossibility result for m agents and n alternatives involving ex-post-Efficiency or SD-Efficiency and possibly involving Anonymity / Neutrality / SD-Strategy-Proofness, i. e. 'There exists no ex-post- / SD-efficient SDS on m agents and n alternatives that fulfils a given subset of the previously named properties.'*

Then there exists no such SDS for m' agents and n' alternatives for any $m' \geq m$, $n' \geq n$.

[3] This 'if' is actually an 'iff', but the other direction is not as obvious. However, a formal Isabelle/HOL proof of both directions exists.

4 Main Impossibility Result

4.1 Background Theory

I will now describe how the concepts defined in Section 3 were formalised in Isabelle/HOL. All of these concepts and the theorems about them are available in the *Archive of Formal Proofs* [Ebe16a] and can be used for similar projects in the future. The current formalisation focuses on weak preferences and Stochastic Dominance, but it is flexible enough to be extended to other preference domains and lottery extensions.

The flexibility is due to the heavy use of the Isabelle feature of *locales* [Bal14]. These are named contexts with certain fixed variables and assumptions. The user can then make definitions and prove theorems containing these variables and using these assumptions. A locale can be *instantiated* by giving concrete values for its fixed variables and proving that the locale assumptions hold on these values. Upon doing this, the user gains access to all the locale theorems, instantiated with the concrete values of the interpretation.

The standard example for locales are algebraic structures such as monoids: a monoid locale would fix a function f of type $\alpha \to \alpha \to \alpha$ (a curried function taking two arguments of type α and returning a value of type α) and a neutral element e of type α and assume that f is associative and $f(x, e) = f(e, x) = x$.

Typically, it is convenient to also fix an explicit carrier set of type α *set*, since one would otherwise be restricted to viewing the entire universe of the type α as the carrier set, which means that something like 'The monoid of non-negative real numbers with addition' is not possible without introducing a new type for non-negative real numbers. It also makes it all but impossible to consider something like a sub-monoid.

This will be a common occurrence in this formalisation as well: We have a *type* of agents and a *type* of alternatives, but we do not consider all of these values to be 'an agent' or 'an alternative'. We therefore have an explicit set of type *agent set* and of type *alt set* and ignore all values of the type that are not in this carrier set.

Examples for locales in the formalisation are:

- Preorders: Fix a carrier set and a binary function *le* $:: \alpha \to \alpha \to$ bool with the assumptions that *le* is reflexive and transitive and returns false for all values not in the carrier
- Total preorders: Defined as a preorder with the additional assumption that *le* is total.
- Finite total preorders: Defined as a total preorder with a finite carrier set
- Preference profiles: Defined as a family of finite total preorders over the set of alternatives, indexed by the set of agents, i. e. a function that sends a value of type *agent* to a

relation on the type *alt* such that each agent is mapped to a finite complete preorder on the set of alternatives and every 'non-agent' is mapped to the empty relation.[4]

- Elections: Fixes a finite non-empty set of agents and a finite non-empty set of alternatives

- Social Decision Schemes: Defined as an election plus a function *sds* that sends preference profiles to discrete probability distributions on the type of alternatives (i. e. lotteries). Additionally, we require that any valid preference profile gets mapped to a lottery whose support is a subset of the set of alternatives. (i. e. every non-alternative has probability 0)

In a similar vein, I then define locales for Anonymity, Neutrality, *SD*-Strategy-Proofness, etc.

As a test of the practicality of the formalisation and to increase the confidence in the definitions of Strategy-Proofness and the other properties, I also defined Random Dictatorship and Random Serial Dictatorship and proved their properties.

The impossibility of an anonymous and neutral SDS that satisfies *SD*-Efficiency and *SD*-Strategy-Proofness is then stated by defining a locale that is a combination of the locales for anonymity, neutrality, *SD*-Efficiency, and *SD*-Strategy-Proofness and then proving *False* within that locale.

4.2 Gathering Facts

As a preparation to the Isabelle proof and the human-readable proof, let us first explore how the SMT proof by Brandl *et al.* works. All of this is also described in their paper [BBG16].

The four properties (Anonymity, Neutrality, *SD*-Strategy-Proofness, and *SD*-Efficiency) impose restrictions on the results that an SDS may produce for any given preference profile. If there is no SDS that fulfils all four properties, then the restrictions that arise from the four properties for all valid preference profiles are inconsistent.

Another insight is that, due to the symmetry conditions imposed by Anonymity and Neutrality, all preference profiles that are equivalent modulo permutation of the agents and / or the alternatives can be identified (e. g. by choosing a canonical representative). This reduces the number of preference profile that need to be considered from 31,640,625 to 471,956.

However, these are still to many profiles for an SMT proof, and certainly too many for a human-readable proof. The key insight is therefore that we may not have to consider *all* profiles to arrive at inconsistent conditions; a subset of them – ideally a small one – may already suffice.

[4] Note that the assumption that non-agents are mapped to the empty relation is important: otherwise, two preference profiles could differ only in what relations they assign to a non-agent, and a voting rule could examine this and return different results for the two profiles. With our additional assumption, we prevent this, since it implies that two preference profiles that have the same relations for all agents are logically equal.

This is, in fact, the case. Brandl *et al.* [BBG16] have found a set of 47 preference profiles (or rather anonymity–neutrality equivalence classes of profiles) for which the arising conditions are inconsistent. This set was found by starting from an initial profile and systematically introducing certain manipulations to obtain new profiles. Once a sizeable number of profiles has been gathered this way, one derives all conditions that arise from them and gives these conditions to an SMT solver. If the solver finds the conditions to be unsatisfiable, this proves the impossibility result.

The conditions that are given to the SMT solver are of the following form (where $p_{i,x}$ is the probability $f(R_i)(x)$):

Lottery conditions. $p_{i,x} \geq 0$ for any i, x and $\sum_{x \in A} p_{i,x} = 1$ for any i.

Orbit conditions. If $R^\sigma \circ \pi = R$, then $f(R)(\sigma(x)) = f(R)(x)$ for any $x \in A$. This essentially says that if there is a permutation σ of the alternatives such that renaming the alternatives in R with σ leads to a profile that is equivalent (w. r. t. anonymity) to R, then all alternatives on an orbit of σ must receive the same winning probability.

Example 3. *Consider the following profile:*

$$R: \quad \{b,d\},\{a,c\} \qquad \{c,d\},\{a,b\} \qquad a,b,\{c,d\} \qquad a,c,\{b,d\}$$

Renaming b to c and c to b, i.e. applying the permutation $\sigma = (a)(b\ c)(d)$, yields the following profile:

$$R^\sigma: \quad \{c,d\},\{a,b\} \qquad \{b,d\},\{a,c\} \qquad a,c,\{b,d\} \qquad a,b,\{c,d\}$$

This profile is obviously anonymity-equivalent to the original profile, and therefore, every anonymous and neutral SDS must assign the same probabilities to all elements of an orbit of σ. Since the only non-trivial orbit is $(b\ c)$, this means that the only orbit condition here is $f(R)(b) = f(R)(c)$.

Efficiency conditions. As we have seen in Observation 1, for a profile R_i, *SD*-Efficiency boils down to $\exists x \in A.\ p_{i,x}$ for each inclusion-minimal inefficient support A of R_i, and these inclusion-minimal inefficient supports can be found by solving linear programs. (see Example 2)

Strategy-Proofness conditions. If R_j, R_k are two profiles and $\sigma : A \to A, \pi : N \to N$ are permutations such that R_j and $R_k^\sigma \circ \pi$ agree except for voter i, then $f(R_k) \circ \sigma \not\succ_{SD(R_j(i))} f(R_j)$. This is equivalent to:

$$\exists x \in A.\ \sum_{y \succeq_{R_j(i)} x} p_{k,\sigma(y)} < \sum_{y \succeq_{R_j(i)} x} p_{j,y} \quad \vee \quad \forall x \in A.\ \sum_{y \succeq_{R_j(i)} x} p_{k,\sigma(y)} = \sum_{y \succeq_{R_j(i)} x} p_{j,y}$$

Example 4. *Consider the following two preference profiles:*

$$\begin{array}{rllll} R: & \{b,d\},\{a,c\} & \{c,d\},\{a,b\} & a,b,\{c,d\} & a,c,\{b,d\} \\ R': & \{a,b\},\{c,d\} & \{a,c\},\{b,d\} & d,\{a,b\},c & d,c,\{a,b\} \end{array}$$

If Agent 4 in R replaces her preferences with $a, \{c,d\}, b$, we obtain the following profile:

$$\{b,d\},\{a,c\} \qquad \{c,d\},\{a,b\} \qquad a,b,\{c,d\} \qquad a,\{c,d\},b$$

On the other hand, renaming the alternatives in R' with $\sigma = (a\ d)(b\ c)$ yields the following profile:

$$R'^{\sigma}: \quad \{d,c\},\{b,a\} \qquad \{d,b\},\{c,a\} \qquad a,\{d,c\},b \qquad a,b,\{d,c\}$$

It is now easy to see that these last two profiles are equivalent modulo anonymity. Strategy-Proofness therefore implies $f(R'^{\sigma}) = f(R') \circ \sigma \not\succ_{SD(R(4))} f(R)$, or, equivalently:

$$\begin{aligned} &f(R')(d) < f(R)(a) \vee f(R')(d) + f(R')(b) < f(R)(a) + f(R)(c) \vee \\ &\quad (f(R')(d) = f(R)(a) \wedge f(R')(d) + f(R')(b) = f(R)(a) + f(R)(c)) \end{aligned}$$

Since all quantification in these conditions is over finite sets, these conditions all fall into the realm of quantifier-free linear real arithmetic, which is a decidable theory, and virtually all SMT solvers have very efficient complete decision procedures for it.

4.3 Automation in Isabelle/HOL

Isabelle itself is written in Standard ML and contains a sophisticated ML system that allows compiling and adding new code at run-time. Users can add custom proof methods written in ML to automate proof steps and commands to automatically define constants, derive facts, etc. I developed a number of such Isabelle commands to automate the fact gathering described in the previous section:

preference_profiles defines one or more preference profiles from the corresponding weak rankings and automatically proves their well-definedness.

derive_orbit_equations computes the orbit conditions of preference profiles thus defined and proves them automatically. For each orbit, a canonical representative x is chosen and the orbit conditions have the form $f(R)(y) = f(R)(x)$, where $y \neq x$ is some other element on the orbit. This makes it possible to use the orbit conditions directly as rewrite rules for Isabelle's simplifier, since the equations are normalising.

find_inefficient_supports computes Pareto losers and SD-inefficient supports and automatically proves the corresponding conditions for *ex-post*- and SD-efficient SDSs. In order to find *SD*-inefficient supports and prove their inefficiency, the ML code invokes the external Linear Programming solver *QSOpt_ex* in the way described in Observation 1. Note again that *QSOpt_ex* uses exact arbitrary-precision rational arithmetic, which is important, because we need to import the solutions back into Isabelle and any rounding might lead Isabelle to reject the witnesses (e. g. if the probabilities do not sum to exactly 1 anymore).

prove_inefficient_supports takes a list of *ex-post*- and *SD*-inefficient supports where each *SD*-inefficient support is annotated with a witness lottery (i. e. a lottery that is strictly *SD*-preferred to the uniform distribution on the inefficient support). As explained in Observation 1, this witness lottery can be read directly from the solution of the corresponding linear program.

I introduced this command to make the final proof independent of the external linear programming solver: The witness lotteries can be computed once with *find_inefficient_supports* using the external solver; then, we can replace this invocation with a corresponding invocation of *prove_inefficient_supports*, annotated with the witnesses that were just computed. In fact, the *find_inefficient_supports* command outputs a hyperlink that allows the user to automatically replace it with a corresponding invocation of *prove_inefficient_supports* with all the witnesses filled in as needed.

derive_strategyproofness_conditions takes a list of preference profiles and computes all possible manipulations of all profiles in this list that yield another profile in the list and derives and proves all the conditions that arise from these manipulations for a (weakly) strategy-proof SDS. The user can specify an optional distance threshold to restrict the search to small manipulations.

Note that this ML code is *untrusted*: We did not verify it and there is, in fact, no need to verify it. Since all proofs go through the Isabelle kernel, a bug in our code would simply lead to one of our commands producing unprovable goals or failing to derive a fact that it should have derived – but it will never lead to an inconsistency unless Isabelle's kernel itself contains a bug.

All of this automation is also available in the *Archive of Formal Proofs* entry on Randomised Social Choice. [Ebe16a]

4.4 Proof

We are now ready to formulate the proof of our main theorem. The formal proof in Isabelle/HOL is available in its own entry in the *Archive of Formal Proofs* [Ebe16b]. The relevant parts should be fairly readable even for readers who are not too familiar with Isabelle. The following proof is a paraphrased version of this Isabelle proof.

Generally, we will attempt to 'solve' preference profiles, i. e. determine the exact value of $f(R_i)(x)$ (which we write as $p_{i,x}$) for a profile R_i and an alternative x. Where this is not possible, we try to express $p_{i,x}$ in terms of other $p_{j,y}$ or at least find simple inequalities that the $p_{i,x}$ satisfy. We do this until we have gained enough knowledge about the SDS to derive a contradiction.

A typical step in the proofs will be to pick a Strategy-Proofness condition (which usually consist of several disjunctions) and simplify it with all the knowledge that we have – substituting the $p_{i,x}$ whose values we already know, substituting $p_{i,d} = 1 - p_{i,a}$ if we know that $p_{i,b} = p_{i,c} = 0$ etc. We will use the fact that all $p_{i,x}$ are non-negative and that $\sum_{x \in A} p_{i,x} = 1$ without mentioning it explicitly.

Every step of the proof (i. e. 'Condition X simplifies to …' or 'Condition X implies …') is elementary in the sense that it can by solved automatically by Isabelle's automation – in fact, the proof printed here is often considerably more verbose and with more intermediate steps than would be necessary in Isabelle. Still, for a human, most of these steps will require a few steps of reasoning on paper. I chose not to go into more detail on the individual steps, since it would only have made the proof even longer and less readable.

The proof will reference orbit equations, support conditions, and Strategy-Proofness conditions on the set of 47 preference profiles mentioned before. These preference profiles and a list of the conditions with a justification for each of them can be found in the appendix. Furthermore, recall that the entire proof as printed here and all the conditions from the appendix have been machine-checked using Isabelle/HOL to minimise the chance of errors.

As an aid to the reader, the proof contains tables listing all the knowledge that we currently have about the probabilities of the lottery returned by the hypothetical SDS after every few steps.

Now, to begin with the proof, we shall first focus on those profiles that have rich symmetries (i. e. orbit conditions) and restrictive support conditions (e. g. that contain Pareto losers). We will start with the most obvious ones:

- The orbit conditions of R_{45} obviously imply $p_{45,a} = p_{45,b} = p_{45,c} = p_{45,d} = 1/4$.
- The support conditions for R_{10} state that at least one of $p_{10,b}$ and $p_{10,c}$ is 0, and since the orbit conditions state that $p_{10,b} = p_{10,c}$, we have $p_{10,b} = p_{10,c} = 0$.
- In the same fashion, we can show that $p_{i,x} = 0$ for $i \in \{26, 27, 28, 29\}$ and $x \in \{b, c\}$. For R_{29}, the orbit condition then additionally implies $p_{29,a} = p_{29,d} = 1/2$.

- The support conditions for R_{43} state $p_{43,b} = p_{43,c} = 0$, and with the orbit condition $p_{43,a} = p_{43,d}$ we have $p_{43,a} = p_{43,d} = 1/2$.

In summary, we have now derived the following information about the profiles:

	R_{10}	R_{26}	R_{27}	R_{28}	R_{29}	R_{43}	R_{45}
a	$1/2$	?	?	?	$1/2$	$1/2$	$1/4$
b	0	0	0	0	0	0	$1/4$
c	0	0	0	0	0	0	$1/4$
d	$1/2$	?	?	?	$1/2$	$1/2$	$1/4$

- Suppose $p_{39,c} = 0$. Then $(S_{29,39})$ implies $p_{39,d} \leq 1/2$ and $(S_{39,29})$ then implies $p_{39,b} = 0$. Since the support condition for R_{39} states that $p_{39,b} = 0 \vee p_{39,c} = 0$, we can conclude that, in any case, $p_{39,b} = 0$.
- Using this, $(S_{39,29})$ now simplifies to $p_{39,a} \leq 1/2$.
- $(S_{10,36})$ simplifies to $p_{36,a} + p_{36,b} \leq 1/2$. Using this, $(S_{36,10})$ simplifies to $p_{36,a} = 1/2 \wedge p_{36,b} = 0$.
- $(S_{36,39})$ simplifies to $p_{39,a} \geq 1/2$. Using this, $(S_{39,36})$ simplifies to $p_{39,a} = 1/2$.
- $(S_{12,10})$ simplifies to $p_{12,a} + p_{12,d} \geq 1$, which implies $p_{12,c} = 0$.
- $(S_{10,12})$ then simplifies to $p_{12,a} \geq 1/2$.
- $(S_{12,44})$ simplifies to $p_{44,a} \leq p_{12,a}$. Using this, $(S_{44,12})$ simplifies to $p_{44,a} = p_{12,a} \wedge p_{44,c} = 0$.
- $(S_{9,35})$ simplifies to $p_{35,a} \leq p_{9,a}$, and then $(S_{35,9})$ simplifies to $p_{9,a} = p_{35,a}$.
- $(S_{9,18})$ states that $p_{9,a} + p_{9,d} \leq p_{18,a} + p_{18,d}$, and then $(S_{9,18})$ simplifies to $p_{18,c} = p_{9,c}$.

To summarise:

	R_9	R_{10}	R_{12}	R_{18}	R_{26}	R_{27}	R_{28}	R_{29}	R_{36}	R_{39}	R_{43}	R_{44}	R_{45}
a	$p_{35,a}$	$1/2$	$\geq 1/2$	?	?	?	?	$1/2$	$1/2$	$1/2$	$1/2$	$p_{12,a}$	$1/4$
b	0	0	0	0	0	0	0	0	0	0	0	0	$1/4$
c	?	0	0	$p_{9,c}$	0	0	0	0	?	?	0	0	$1/4$
d	?	$1/2$	$\leq 1/2$	?	?	?	?	?	$1/2$	?	$1/2$	$1 - p_{12,a}$	$1/4$

- $(S_{5,10})$ implies $p_{5,d} \geq 1/2$.
- $(S_{5,17})$ implies $p_{5,d} \leq p_{17,d}$, and $(S_{17,7})$ simplifies to $p_{17,d} \leq p_{7,d}$. Combined with $p_{5,d} \geq 1/2$ from above, we have $p_{7,d} \geq 1/2$. Using this, $(S_{7,43})$ implies $p_{7,a} = 1/2$ and $p_{7,c} = 0$, and therefore $p_{7,d} = 1/2$.

- $(S_{5,7})$ now simplifies to $p_{5,d} \leq 1/2$, and $p_{5,d} \geq 1/2$ was already shown, so we have $p_{5,d} = 1/2$.
- $(S_{5,10})$ now simplifies to $p_{5,c} = 0$, and it is then clear that $p_{5,a} = 1/2$.
- Suppose $p_{15,b} = 0$. Then $(S_{10,15})$ simplifies to $p_{15,a} + p_{15,c} \leq 1/2$ and, using that, $(S_{15,10})$ implies $p_{15,c} = 0$. Since the support conditions for R_{15} tell us that $p_{15,b} = 0 \vee p_{15,c} = 0$, we can conclude $p_{15,c} = 0$.
- $(S_{15,5})$ then implies $p_{15,a} \geq 1/2$ and $(S_{15,7})$ implies $p_{15,a} \leq 1/2$. We can conclude that $p_{15,a} = 1/2$.
- $(S_{15,5})$ now simplifies to $p_{15,d} = 1/2 \wedge p_{15,b} = 0$.
- $(S_{27,13})$ simplifies to $p_{13,a} + p_{13,b} \leq p_{27,a}$. Using that, $(S_{13,27})$ simplifies to $p_{13,b} = p_{13,c} = 0$ and $p_{27,a} = p_{13,a}$.
- $(S_{15,13})$ now implies $p_{13,a} \geq 1/2$ and $(S_{13,15})$ simplifies to $p_{13,a} \leq 1/2$, so that we can conclude $p_{13,a} = p_{13,d} = p_{27,a} = p_{27,d} = 1/2$.

We summarise what we have learned so far:

	R_5	R_7	R_9	R_{10}	R_{12}	R_{13}	R_{15}	R_{18}	R_{26}	R_{27}	R_{28}	R_{29}
a	$1/2$	$1/2$	$p_{35,a}$	$1/2$	$\geq 1/2$	$1/2$	$1/2$	?	?	$1/2$	?	$1/2$
b	0	0	0	0	0	0	0	0	0	0	0	0
c	0	0	?	0	0	0	0	$p_{9,c}$	0	0	0	0
d	$1/2$	$1/2$	?	$1/2$	$\leq 1/2$	$1/2$	$1/2$	?	?	$1/2$	?	$1/2$

	R_{36}	R_{39}	R_{43}	R_{44}	R_{45}
a	$1/2$	$1/2$	$1/2$	$p_{12,a}$	$1/4$
b	0	0	0	0	$1/4$
c	?	?	0	0	$1/4$
d	?	?	$1/2$	$1 - p_{12,a}$	$1/4$

- We will now determine the probabilities for R_{19}. The support condition tells us that $p_{19,b} = 0 \vee p_{19,c} = 0$.
    - Suppose $p_{19,b} = 0$. Then $(S_{10,19})$ simplifies to $p_{19,a} + p_{19,c} \leq 1/2$ and $(S_{19,10})$ simplifies to $p_{19,a} + p_{19,c} = 1/2$. We can therefore conclude that $p_{19,d} = 1/2$. Using this, $(S_{27,19})$ then simplifies to $p_{19,a} = 1/2 \wedge p_{19,c} = 0$ and therefore $p_{19,d} = 1/2$.
    - Suppose $p_{19,c} = 0$. Then $(S_{19,10})$ simplifies to $p_{19,a} \geq 1/2$ and $(S_{19,27})$ simplifies to $p_{19,d} \geq 1/2$. This clearly implies $p_{19,a} = p_{19,d} = 1/2$ and $p_{19,b} = 0$.
- Using this, $(S_{19,1})$ simplifies to $p_{1,a} + p_{1,b} \leq 1/2$, and with that, $(S_{1,19})$ simplifies to $p_{1,a} = 1/2 \wedge p_{1,b} = 0$.

- $(S_{33,5})$ simplifies to $p_{33,a} \geq 1/2$. Moreover, $(S_{33,22})$ simplifies to $p_{22,c} + p_{22,d} \leq p_{33,c} + p_{33,d}$, i. e. $p_{33,a} \leq p_{22,a}$. We therefore have $p_{22,a} \geq 1/2$. Using this, $(S_{22,29})$ simplifies to $p_{22,a} = p_{22,d} = 1/2$ and therefore also $p_{22,c} = 0$.

- $(S_{32,28})$ implies $p_{28,a} \leq p_{32,d}$. Then $(S_{28,32})$ implies $p_{32,d} = p_{28,a}$. Moreover, $(S_{22,32})$ simplifies to $p_{32,a} \leq 1$. Using these two facts, $(S_{32,22})$ implies $p_{32,d} = 1/2$ and therefore also $p_{28,a} = p_{28,d} = 1/2$.

- $(S_{28,39})$ now simplifies to $p_{39,c} = 0$, and since we have already determined $p_{39,a} = 1/2$ and $p_{39,b} = 0$, we can conclude $p_{39,d} = 1/2$.

- $(S_{1,2})$ states that $p_{2,c} + p_{2,d} \leq p_{1,c} + p_{2,d}$. Using this, $(S_{2,1})$ simplifies to $p_{2,a} = p_{2,c} + p_{2,d} = 1/2$ and therefore also $p_{2,b} = 0$. Using this, $(S_{39,2})$ simplifies to $p_{2,c} = 0 \wedge p_{2,d} = 1/2$.

- We will now determine R_{42}:
  - $(S_{17,5})$ simplifies to $p_{17,a} + p_{17,c} \geq 1/2$ and $(S_{5,17})$ simplifies to $p_{17,a} + p_{17,c} \leq 1/2$, so we can conclude $p_{17,d} = 1/2$.
  - $(S_{6,42})$ states that $p_{42,a} + p_{42,c} \leq p_{6,a} + p_{6,c}$ and $(S_{6,19})$ implies $p_{6,a} + p_{6,c} \leq 1/2$. We can therefore conclude that $p_{42,a} + p_{42,c} \leq 1/2$.
  - $(S_{17,11})$ states that $p_{11,a} + p_{11,c} \leq p_{17,a} + p_{17,c}$. Since $p_{11,b} = p_{17,b} = 0$, this is equivalent to $p_{11,d} \geq p_{17,d} = 1/2 \geq p_{42,a} + p_{42,c}$. With this, $(S_{42,11})$ implies $p_{42,c} \geq p_{11,d} \geq 1/2$.
  - $(S_{17,3})$ simplifies to $p_{3,a} + p_{3,c} \leq p_{17,a} + p_{17,c}$; i. e. $p_{3,d} \geq p_{17,d} = 1/2$.
  - Finally, using $p_{42,c} \geq 1/2$ and $p_{3,d} \geq 1/2$, $(S_{42,3})$ simplifies to $p_{42,c} \geq 1/2 \wedge p_{42,d} \geq 1/2$ and therefore $p_{42,a} = p_{42,b} = 0$ and $p_{42,c} = p_{42,d} = 1/2$.

- Using these values for R_{42}, the two conditions $(S_{37,42}\,(1))$ and $(S_{37,42}\,(2))$ now simplify to $p_{37,a} = 1/2 \vee p_{37,a} + p_{37,b} > 1/2$ and $p_{37,c} = 1/2 \vee p_{37,c} + p_{37,d} > 1/2$. Together, these obviously imply $p_{37,a} = p_{37,c} = 1/2$ and $p_{37,b} = p_{37,d} = 0$.

- Similarly, R_{24} simplifies to $p_{24,a} + p_{24,b} \leq 0$ and therefore $p_{24,a} = p_{24,b} = 0$.

	R_1	R_2	R_5	R_7	R_9	R_{10}	R_{12}	R_{13}	R_{15}	R_{18}	R_{19}	R_{22}	R_{24}
a	$1/2$	$1/2$	$1/2$	$1/2$	$p_{35,a}$	$1/2$	$\geq 1/2$	$1/2$	$1/2$	?	$1/2$	$1/2$	0
b	0	0	0	0	0	0	0	0	0	0	0	0	0
c	?	0	0	0	?	0	0	0	0	$p_{9,c}$	0	0	?
d	?	$1/2$	$1/2$	$1/2$	?	$1/2$	$\leq 1/2$	$1/2$	$1/2$	?	$1/2$	$1/2$	?

	R_{26}	R_{27}	R_{28}	R_{29}	R_{36}	R_{37}	R_{39}	R_{42}	R_{43}	R_{44}	R_{45}
a	?	$1/2$	$1/2$	$1/2$	$1/2$	$1/2$	$1/2$	0	$1/2$	$p_{12,a}$	$1/4$
b	0	0	0	0	0	0	0	0	0	0	$1/4$
c	0	0	0	0	?	$1/2$	0	$1/2$	0	0	$1/4$
d	?	$1/2$	$1/2$	$1/2$	?	0	$1/2$	$1/2$	$1/2$	$1 - p_{12,a}$	$1/4$

- $(S_{24,34})$ implies $p_{34,b} \leq p_{24,c}$ and $(S_{34,24})$ implies $p_{24,c} \leq p_{34,b}$; we therefore have $p_{34,b} = p_{24,c}$. Using this, $(S_{34,24})$ simplifies to $p_{34,c} = 0$ and $(S_{24,34})$ simplifies to $p_{34,d} = 0$.
- $(S_{14,34})$ now simplifies to $p_{14,a} + p_{14,c} \geq 1$, so we have $p_{14,b} = p_{14,d} = 0$.
- $(S_{46,37})$ simplifies to $p_{46,a} = p_{46,c} = 0$.
- $(S_{46,20})$ now simplifies to $p_{20,a} + p_{20,c} \leq 0$, so we have $p_{20,a} = p_{20,c} = 0$.
- $(S_{20,21})$ now simplifies to $p_{21,b} = p_{21,c} = 0$.
- $(S_{12,16})$ simplifies to $p_{16,a} + p_{16,c} \leq p_{12,a}$.
- We now determine the probabilities for $p_{16,c}$:
  - $(S_{44,40})$ simplifies to $p_{12,a} \leq p_{40,a}$. Moreover, $(S_{9,40})$ simplifies to $p_{40,a} \leq p_{9,a}$. Combined with $p_{16,a} + p_{16,c} \leq p_{12,a}$, this implies $p_{16,a} + p_{16,c} \leq p_{9,a}$.
  - $(S_{14,16})$ implies $p_{16,a} \geq p_{14,a}$.
  - Combining the last two facts, we obtain $p_{16,c} \leq p_{9,a} - p_{14,a}$. Moreover, $(S_{14,9})$ implies $p_{9,a} - p_{14,a} \leq 0$. Combining this, we have $p_{16,c} = 0$.
- Therefore, the fact $p_{16,a} + p_{16,c} \leq p_{12,a}$, which we have shown before, now simplifies to $p_{16,a} \leq p_{12,a}$.
- Since $(S_{14,16})$ simplifies to $p_{14,a} \leq p_{16,a}$, we then have $p_{14,a} \leq p_{12,a}$.

	R_1	R_2	R_5	R_7	R_9	R_{10}	R_{12}	R_{13}	R_{14}	R_{15}	R_{16}	R_{18}	R_{19}
a	$1/2$	$1/2$	$1/2$	$1/2$	$p_{35,a}$	$1/2$	$\geq 1/2$	$1/2$	$\leq p_{12,a}$	$1/2$	?	?	$1/2$
b	0	0	0	0	0	0	0	0	0	0	0	0	0
c	?	0	0	0	?	0	0	0	?	0	0	$p_{9,c}$	0
d	?	$1/2$	$1/2$	$1/2$	?	$1/2$	$\leq 1/2$	$1/2$	0	$1/2$	?	?	$1/2$

	R_{20}	R_{21}	R_{22}	R_{24}	R_{26}	R_{27}	R_{28}	R_{29}	R_{34}	R_{36}	R_{37}	R_{39}
a	0	?	$1/2$	0	?	$1/2$	$1/2$	$1/2$	$1 - p_{24,c}$	$1/2$	$1/2$	$1/2$
b	?	0	0	0	0	0	0	0	$p_{24,c}$	0	0	0
c	0	0	0	?	0	0	0	0	0	?	$1/2$	0
d	?	?	$1/2$	?	?	$1/2$	$1/2$	$1/2$	0	?	0	$1/2$

	R_{42}	R_{43}	R_{44}	R_{45}	R_{46}
a	0	$1/2$	$p_{12,a}$	$1/4$	0
b	0	0	0	$1/4$	$?$
c	$1/2$	0	0	$1/4$	0
d	$1/2$	$1/2$	$1 - p_{12,a}$	$1/4$	$?$

- We now show that $p_{12,a} = p_{9,a} = p_{35,a}$:
  - $(S_{14,9})$ implies $p_{9,a} \leq p_{14,a}$. Since $p_{14,a} \leq p_{12,a}$, we have $p_{9,a} \leq p_{12,a}$.
  - $(S_{44,40})$ simplifies to $p_{12,a} \leq p_{40,a}$. Moreover, $(S_{9,40})$ simplifies to $p_{40,a} \leq p_{9,a}$; therefore, we have $p_{12,a} \leq p_{9,a}$.
  - Combining these two inequalities yields $p_{12,a} = p_{9,a}$.
- Recall that $p_{14,a} \leq p_{12,a} = p_{9,a}$. Then $(S_{14,9})$ simplifies to $p_{9,a} = p_{14,a} \wedge p_{9,d} = 0$.
- $(S_{23,19})$ simplifies to $p_{23,a} + p_{23,d} \geq 1$ and therefore $p_{23,b} = p_{23,c} = 0$.
- $(S_{35,21})$ simplifies to $p_{21,a} \leq p_{35,a} + p_{35,c}$. Then $(S_{21,35})$ simplifies to $p_{35,c} = 0 \wedge p_{35,a} = p_{21,a}$.
- Next, we derive the probabilities for R_{18}:
  - $(S_{23,12})$ simplifies to $p_{21,a} \leq p_{23,a}$.
  - $(S_{23,18})$ simplifies to $p_{18,c} + p_{18,d} \leq 1 - p_{23,a}$. Since $p_{18,c} = p_{9,c} = 1 - p_{9,a} = 1 - p_{35,a} = 1 - p_{21,a}$, this is equivalent to $p_{18,d} \leq p_{21,a} - p_{23,a}$. Recall that $p_{9,b} = p_{9,c} = 0$, i. e. $p_{18,c} = p_{9,c} = 1 - p_{9,a} = 1 - p_{35,a} = 1 - p_{21,a}$. Substituting this in the inequality we have just derived and rearranging yields $p_{18,d} \leq p_{21,a} - p_{23,a}$.
  - Since $p_{21,a} \leq p_{23,a}$, the right-hand side of the above inequality is 0 and therefore $p_{18,d} = 0$.

  Now we can derive the probabilities for R_4:
  - $(S_{47,30})$ simplifies to $p_{30,a} \leq p_{47,a}$.
  - $(S_{4,47})$ simplifies to $p_{47,a} + p_{47,d} \leq p_{4,a} + p_{4,d}$, i. e. $p_{4,c} \leq p_{47,c}$.
  - Adding these two inequalities, we obtain $p_{4,c} + p_{30,a} \leq 1 - p_{47,d}$.
  - $(S_{30,21})$ simplifies to $p_{21,a} \leq p_{30,a}$, and with the previous inequality, we obtain $p_{4,c} + p_{21,a} \leq 1 - p_{47,d} \leq 1$. Substituting $p_{21,a} = p_{14,a}$ yields $p_{4,c} + p_{14,a} \leq 1$.
  - $(S_{4,18})$ now simplifies to $p_{4,d} = 0 \wedge p_{4,c} = p_{21,d}$.
- $(S_{8,26})$ implies $p_{26,a} \leq p_{8,d}$. Using this, $(S_{26,8})$ simplifies to $p_{26,a} = p_{8,d}$. Using this, we look at $(S_{8,26})$ again and find that it now simplifies to $p_{8,a} + p_{8,d} = 1$, i. e. $p_{8,c} = p_{8,b} = 0$ and $p_{26,a} = 1 - p_{8,a}$.

	R_1	R_2	R_4	R_5	R_7	R_8	R_9	R_{10}	R_{12}	R_{13}	R_{14}
a	$1/2$	$1/2$	$p_{21,a}$	$1/2$	$1/2$	?	$p_{21,a}$	$1/2$	$p_{21,a}$	$1/2$	$p_{21,a}$
b	0	0	0	0	0	0	0	0	0	0	0
c	?	0	$1 - p_{21,a}$	0	0	0	$1 - p_{21,a}$	0	0	0	$1 - p_{21,a}$
d	?	$1/2$	0	$1/2$	$1/2$	?	0	$1/2$	$1 - p_{21,a}$	$1/2$	0

	R_{15}	R_{16}	R_{18}	R_{19}	R_{20}	R_{21}	R_{22}	R_{23}	R_{24}	R_{26}	R_{27}	R_{28}
a	$1/2$	?	$p_{21,a}$	$1/2$	0	?	$1/2$	?	0	$1 - p_{8,a}$	$1/2$	$1/2$
b	0	0	0	0	?	0	0	0	0	0	0	0
c	0	0	$1 - p_{21,a}$	0	0	0	0	0	?	0	0	0
d	$1/2$	?	0	$1/2$	?	?	$1/2$	?	?	$p_{8,a}$	$1/2$	$1/2$

	R_{29}	R_{34}	R_{35}	R_{36}	R_{37}	R_{39}	R_{42}	R_{43}	R_{44}	R_{45}	R_{46}
a	$1/2$	$1 - p_{24,c}$	$p_{21,a}$	$1/2$	$1/2$	$1/2$	0	$1/2$	$p_{12,a}$	$1/4$	0
b	0	$p_{24,c}$	0	0	0	0	0	0	0	$1/4$	?
c	0	0	0	?	$1/2$	0	$1/2$	0	0	$1/4$	0
d	$1/2$	0	$1 - p_{21,a}$	?	0	$1/2$	$1/2$	$1/2$	$1 - p_{12,a}$	$1/4$	?

- $(S_{4,47})$ simplifies to $p_{21,d} \leq p_{47,c}$.
- $(S_{47,30})$ simplifies to $p_{30,a} \leq p_{47,a}$. With this and the previous inequality, $(S_{30,21})$ simplifies to $p_{30,b} = p_{30,c} = 0$ and $p_{30,a} = p_{47,a}$.
- The last big and crucial step is to show that $p_{31,c} \geq 1/2$:
  - The support conditions for R_{25} tell us that $p_{25,b} = 0 \lor p_{25,c} = 0$. If $p_{25,c} = 0$, then $(S_{25,36})$ immediately implies $p_{25,a} \geq 1/2$. If, on the other hand, $p_{25,b} = 0$, then $(S_{36,25})$ implies $p_{25,a} + p_{25,c} \leq p_{36,c} + 1/2$, with which $(S_{25,36})$ then also implies $p_{25,a} \geq 1/2$.
  - Using $p_{25,a} \geq 1/2$, the condition $(S_{25,26})$ implies $p_{26,a} \geq 1/2$, and therefore also $1/2 \leq p_{26,a} + p_{47,d} = 1 - p_{8,a} + p_{47,d}$.
  - Now observe that $(S_{4,8})$ simplifies to $p_{21,a} \leq p_{8,a}$, which is equivalent to $1 - p_{8,a} \leq p_{21,d}$. Combined with $p_{21,d} \leq p_{47,c}$, which we have shown before, we now have $1/2 \leq p_{47,c} + p_{47,d}$.
  - $(S_{30,41})$ implies $p_{41,a} + p_{41,c} \leq p_{47,a}$, which is equivalent to $p_{47,c} + p_{47,d} \leq p_{41,d}$.
  - $(S_{41,31})$ simplifies to $p_{31,a} + p_{31,b} + p_{31,d} \leq p_{41,a} + p_{41,c}$, which is equivalent to $p_{41,d} \leq p_{31,c}$.
  - Combining this chain of inequalities, we finally have $p_{31,c} \geq 1/2$.

- $(S_{2,38})$ simplifies to $p_{38,a} + p_{38,c} \leq 1/2$, i. e. $p_{38,b} + p_{38,d} \geq 1/2$. Using this and $p_{31,c} \geq 1/2$, the condition $(S_{31,38})$ simplifies to $p_{38,b} + p_{38,d} = p_{31,b} + p_{31,d}$. This means that $p_{31,b} + p_{31,d} \geq 1/2$, and since $p_{31,c} \geq 1/2$, we can conclude $p_{31,b} + p_{31,d} = p_{31,c} = 1/2$ and $p_{31,a} = 0$.

It is now easy to see that each of the three cases in $(S_{45,31})$ is a contradiction. We have thus shown that the conditions are inconsistent, and therefore, there is no anonymous and neutral SDS for four agents and alternatives that fulfils both SD-Strategy-Proofness and SD-Efficiency. □

About this proof. It may be of interest to the reader how I obtained this 'human-readable' proof. It was, in fact, manually extracted from the SMT proof in the following way: First of all, I defined the preference profiles in Isabelle and derived all the required conditions using the automation described before. Since Isabelle can invoke the SMT solver Z3 and automatically translate Z3 proof objects to Isabelle proofs, this was already enough to prove the impossibility result in Isabelle. However, this kind of proof has several drawbacks: while Isabelle does not trust the external SMT solver, there is still a dependency on this third-party software, which is heavily discouraged for Isabelle proofs. Also, this proof is somewhat unsatisfying since it cannot be examined or checked by a human in any reasonable way.

Therefore, I then attempted to fully determine the values of as many probabilities as possible using just one or two Strategy-Proofness conditions and then remove the corresponding conditions and used Isabelle's SMT proof method to see if the proof still worked. I was able to make progress this way for about the first third of the proof.

I then started to conjecture facts such as $p_{7,a} = 1/2$. Obviously, since the conditions are inconsistent, these conjectures are *all* true and provable, but a 'good' conjecture can be derived from a small subset of the conditions. I therefore attempted bisection of the conditions using the SMT solver to find a 'minimal set of preconditions', and when this set was sufficiently small, I attempted to prove the conjecture with heavy use of Isabelle's automation and related facts and then remove as many of the conditions that I used, replacing them with the facts I had just proven in the hope that I had identified the 'important core' of the conditions.

With this approach, I was able to remove more and more Strategy-Proofness conditions until I was able to prove False directly. This approach led to a very linear proof without any 'big' case distinctions, which is remarkable considering that there are over 60 disjunctions in the conditions altogether. I then proceeded by adding more detail to the individual proof steps, e. g. replacing a step using several Strategy-Proofness conditions with heavy use of automation by several steps, each using only one Strategy-Proofness condition and less automation. After that, the Isabelle proof was in its current form, from which I then derived the proof printed here.

5 Conclusion

Based on work by Brandl *et al.* [BBS16; BBG16], I have written a fully machine-checked proof of the incompatibility of SD-Strategy-Proofness and SD-Efficiency using the Isabelle/HOL theorem prover and, based on this, a 'human-readable' proof. In the process, I have also developed a high-level formalisation of basic concepts of Randomised Social Choice Theory and proof automation that automatically defines and derives facts from given preference profiles. Both of these can be used for similar future projects.

This work was also an interesting case study in how interactive theorem provers (like Isabelle) and powerful automated theorem provers (like Z3 and other SMT solvers) can be used not only to formally verify existing mathematical theorems, but also to find completely new and – more or less – human-readable proofs for conjectures. For human mathematicians, simplifying large terms and combining large numbers of complicated linear equations and inequalities is tedious and error-prone, but specialised computer programs (such as SMT solvers or Isabelle's decision procedures for linear arithmetic) excel at it. Using an interactive proof system such as Isabelle has the great advantage that one receives immediate feedback on everything, and it is easy to check whether an idea works out or not, and it is virtually impossible to make a mistake.

To stress this, I would like to mention the prior proof of a weaker version of the impossibility result due to Brandl *et al.* [BBS16] again: As explained in Section 1.1, the attempt to prove this result in Isabelle has brought forth a mistake in it. The proof for four voters and alternatives works in exactly the way that Brandl *et al.* say, and I formalised it in Isabelle/HOL in the initial phase of this project. However, the authors then use the lifting argument explained in section 3.6, but the RD-extension assumption does not 'survive' this lifting, since the lifting adds indifferent agents, which means that the resulting preference profile contains ties and the RD-extension assumption is no longer applicable.

While this proof has become obsolete through their subsequent proof of the same statement without the RD extension assumption [BBG16] and the original statement could have been salvaged by assuming additionally that the voting rule ignores fully indifferent agents (as the authors privately communicated to me), this shows once again that formalising mathematical proofs often brings problems to light that have been missed otherwise, which is particularly important in cases where the mistake cannot be repaired trivially, but requires an entirely different proof or a modified theorem statement.

A Appendix

A.1 Preference Profiles

Table 1 lists the 47 preference profiles used in the proof by giving the weak rankings of each agent.

Profile	Agent 1	Agent 2	Agent 3	Agent 4
R_1	$\{c,d\},\{a,b\}$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$\{a,c\},\{b,d\}$
R_2	$\{a,c\},\{b,d\}$	$\{c,d\},a,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$
R_3	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$d,\{a,b\},c$	$c,a,\{b,d\}$
R_4	$\{a,b\},\{c,d\}$	$\{a,d\},\{b,c\}$	$c,\{a,b\},d$	$d,c,\{a,b\}$
R_5	$\{c,d\},\{a,b\}$	$\{a,b\},\{c,d\}$	$\{a,c\},d,b$	$d,\{a,b\},c$
R_6	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{a,c\},\{b,d\}$	d,b,a,c
R_7	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	a,c,d,b	$d,\{a,b\},c$
R_8	$\{a,b\},\{c,d\}$	$\{a,c\},\{b,d\}$	$d,\{a,b\},c$	$d,c,\{a,b\}$
R_9	$\{a,b\},\{c,d\}$	$\{a,d\},c,b$	$d,c,\{a,b\}$	$\{a,b,c\},d$
R_{10}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{a,c\},d,b$	$\{b,d\},a,c$
R_{11}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$d,\{a,b\},c$	c,a,b,d
R_{12}	$\{c,d\},\{a,b\}$	$\{a,b\},\{c,d\}$	$\{a,c\},d,b$	$\{a,b,d\},c$
R_{13}	$\{a,c\},\{b,d\}$	$\{c,d\},a,b$	$\{b,d\},a,c$	a,b,d,c
R_{14}	$\{a,b\},\{c,d\}$	$d,c,\{a,b\}$	$\{a,b,c\},d$	a,d,c,b
R_{15}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{b,d\},a,c$	a,c,d,b
R_{16}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	a,c,d,b	$\{a,b,d\},c$
R_{17}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{a,c\},\{b,d\}$	$d,\{a,b\},c$
R_{18}	$\{a,b\},\{c,d\}$	$\{a,d\},\{b,c\}$	$\{a,b,c\},d$	$d,c,\{a,b\}$
R_{19}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{b,d\},a,c$	$\{a,c\},\{b,d\}$
R_{20}	$\{b,d\},a,c$	$b,a,\{c,d\}$	$a,c,\{b,d\}$	$d,c,\{a,b\}$
R_{21}	$\{a,d\},c,b$	$d,c,\{a,b\}$	$c,\{a,b\},d$	$a,b,\{c,d\}$
R_{22}	$\{a,c\},d,b$	$d,c,\{a,b\}$	$d,\{a,b\},c$	$a,b,\{c,d\}$
R_{23}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$\{a,c\},\{b,d\}$	$\{a,b,d\},c$
R_{24}	$\{c,d\},\{a,b\}$	d,b,a,c	$c,a,\{b,d\}$	$b,a,\{c,d\}$
R_{25}	$\{c,d\},\{a,b\}$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$a,c,\{b,d\}$
R_{26}	$\{b,d\},\{a,c\}$	$\{c,d\},\{a,b\}$	$a,b,\{c,d\}$	$a,c,\{b,d\}$
R_{27}	$\{a,b\},\{c,d\}$	$\{b,d\},a,c$	$\{a,c\},\{b,d\}$	$\{c,d\},a,b$
R_{28}	$\{c,d\},a,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$a,c,\{b,d\}$
R_{29}	$\{a,c\},d,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$d,c,\{a,b\}$
R_{30}	$\{a,d\},c,b$	$d,c,\{a,b\}$	$c,\{a,b\},d$	$\{a,b\},d,c$
R_{31}	$\{b,d\},a,c$	$\{a,c\},d,b$	$c,d,\{a,b\}$	$\{a,b\},c,d$
R_{32}	$\{a,c\},d,b$	$d,c,\{a,b\}$	$d,\{a,b\},c$	$\{a,b\},d,c$

R_{33}	$\{c,d\},\{a,b\}$	$\{a,c\},d,b$	$a,b,\{c,d\}$	$d,\{a,b\},c$
R_{34}	$\{a,b\},\{c,d\}$	a,c,d,b	$b,\{a,d\},c$	$c,d,\{a,b\}$
R_{35}	$\{a,d\},c,b$	$a,b,\{c,d\}$	$\{a,b,c\},d$	$d,c,\{a,b\}$
R_{36}	$\{c,d\},\{a,b\}$	$\{a,c\},d,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$
R_{37}	$\{a,c\},\{b,d\}$	$\{b,d\},\{a,c\}$	$a,b,\{c,d\}$	$c,d,\{a,b\}$
R_{38}	$\{c,d\},a,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$\{a,c\},b,d$
R_{39}	$\{a,c\},d,b$	$\{b,d\},a,c$	$a,b,\{c,d\}$	$\{c,d\},a,b$
R_{40}	$\{a,d\},c,b$	$\{a,b\},c,d$	$\{a,b,c\},d$	$d,c,\{a,b\}$
R_{41}	$\{a,d\},c,b$	$\{a,b\},d,c$	$\{a,b,c\},d$	$d,c,\{a,b\}$
R_{42}	$\{c,d\},\{a,b\}$	$\{a,b\},\{c,d\}$	d,b,a,c	$c,a,\{b,d\}$
R_{43}	$\{a,b\},\{c,d\}$	$\{c,d\},\{a,b\}$	$d,\{a,b\},c$	$a,\{c,d\},b$
R_{44}	$\{c,d\},\{a,b\}$	$\{a,c\},d,b$	$\{a,b\},d,c$	$\{a,b,d\},c$
R_{45}	$\{a,c\},d,b$	$\{b,d\},a,c$	$\{a,b\},c,d$	$\{c,d\},b,a$
R_{46}	$\{b,d\},a,c$	$d,c,\{a,b\}$	$\{a,c\},\{b,d\}$	$b,a,\{c,d\}$
R_{47}	$\{a,b\},\{c,d\}$	$\{a,d\},c,b$	$d,c,\{a,b\}$	$c,\{a,b\},d$

Table 1: The 47 preference profiles used in the proof.

A.2 Orbit Equations

Table 2 lists profile automorphisms, i. e. permutations of the alternatives such that applying the permutation to the profile yields a profile that is anonymity-equivalent to the original profile. Given such a profile, an anonymous and neutral SDS must return the same probability for each alternative on an orbit of the permutation.

To increase readability, the permutations are already written as a product of their orbits; for instance, the first orbit condition states that $p_{10,a} = p_{10,d}$ and $p_{10,b} = p_{10,c}$.

Profile	Permutation
R_{10}	$(a\ d)(b\ c)$
R_{26}	$(a)(b\ c)(d)$
R_{27}	$(a)(b\ c)(d)$
R_{28}	$(a)(b\ c)(d)$
R_{29}	$(a\ d)(b\ c)$
R_{43}	$(a\ d)(b\ c)$
R_{45}	$(a\ b\ d\ c)$

Table 2: The relevant profile automorphisms, written as a product of their orbits.

A.3 Support Conditions

The alternative b is Pareto-dominated in the following profiles and must therefore be assigned probability 0 by any *ex-post*-efficient SDS (and thereby also by any SD-efficient SDS):

> R_3, R_4, R_5, R_7, R_8, R_9, R_{11}, R_{12}, R_{14}, R_{16}, R_{17}, R_{18}, R_{21}, R_{22}, R_{23}, R_{30}, R_{32}, R_{33}, R_{35}, R_{40}, R_{41}, R_{43}, R_{44}, R_{47}

Moreover, $\{b, c\}$ is an SD-inefficient support in the following profiles (i. e. any SD-efficient SDS must assign probability 0 to at least one of b and c):

> R_{10}, R_{15}, R_{19}, R_{25}, R_{26}, R_{27}, R_{28}, R_{29}, R_{39}

To see that this is true, note that the lottery $^1/_2\, a + {}^1/_2\, d$ strictly Pareto-SD-dominates the lottery $^1/_2\, b + {}^1/_2\, c$ for each of these profiles.

A.4 Strategy-Proofness Conditions

Table 3 lists the Strategy-Proofness conditions that were used in the impossibility proof. They are a subset of the conditions derived by the *derive_strategyproofness_conditions* command with a distance threshold of 2, i. e. the required manipulations all have a size ≤ 2.

The first number in the name of the condition indicates the original profile and the second one is the manipulated profile (possibly with a permutation applied to the alternatives).

$$p_{2,d} + p_{2,c} \leq p_{1,d} + p_{1,c} \tag{$S_{1,2}$}$$

$$p_{19,a} < p_{1,a} \lor p_{19,a} + p_{19,b} < p_{1,a} + p_{1,b} \lor (p_{19,a} = p_{1,a} \land p_{19,a} + p_{19,b} = p_{1,a} + p_{1,b}) \tag{$S_{1,19}$}$$

$$\begin{aligned} &p_{1,d} + p_{1,c} < p_{2,d} + p_{2,c} \lor p_{1,d} + p_{1,c} + p_{1,a} < p_{2,d} + p_{2,c} + p_{2,a} \\ &\qquad \lor (p_{1,d} + p_{1,c} = p_{2,d} + p_{2,c} \land p_{1,d} + p_{1,c} + p_{1,a} = p_{2,d} + p_{2,c} + p_{2,a}) \end{aligned} \tag{$S_{2,1}$}$$

$$p_{38,c} + p_{38,a} \leq p_{2,c} + p_{2,a} \tag{$S_{2,38}$}$$

$$p_{8,c} < p_{4,d} \lor p_{8,c} + p_{8,d} < p_{4,d} + p_{4,c} \lor (p_{8,c} = p_{4,d} \land p_{8,c} + p_{8,d} = p_{4,d} + p_{4,c}) \tag{$S_{4,8}$}$$

$$\begin{aligned} &p_{18,c} < p_{4,c} \lor p_{18,c} + p_{18,b} + p_{18,a} < p_{4,c} + p_{4,b} + p_{4,a} \\ &\qquad \lor (p_{18,c} = p_{4,c} \land p_{18,c} + p_{18,b} + p_{18,a} = p_{4,c} + p_{4,b} + p_{4,a}) \end{aligned} \tag{$S_{4,18}$}$$

$$p_{47,d} + p_{47,a} \leq p_{4,d} + p_{4,a} \tag{$S_{4,47}$}$$

$$\begin{aligned} &p_{7,c} + p_{7,a} < p_{5,c} + p_{5,a} \lor p_{7,c} + p_{7,a} + p_{7,d} < p_{5,c} + p_{5,a} + p_{5,d} \\ &\qquad \lor (p_{7,c} + p_{7,a} = p_{5,c} + p_{5,a} \land p_{7,c} + p_{7,a} + p_{7,d} = p_{5,c} + p_{5,a} + p_{5,d}) \end{aligned} \tag{$S_{5,7}$}$$

$$\begin{aligned} &p_{10,a} < p_{5,d} \lor p_{10,a} + p_{10,c} + p_{10,d} < p_{5,d} + p_{5,b} + p_{5,a} \\ &\qquad \lor (p_{10,a} = p_{5,d} \land p_{10,a} + p_{10,c} + p_{10,d} = p_{5,d} + p_{5,b} + p_{5,a}) \end{aligned} \tag{$S_{5,10}$}$$

$$\begin{aligned} &p_{17,c} + p_{17,a} < p_{5,c} + p_{5,a} \lor p_{17,c} + p_{17,a} + p_{17,d} < p_{5,c} + p_{5,a} + p_{5,d} \\ &\qquad \lor (p_{17,c} + p_{17,a} = p_{5,c} + p_{5,a} \land p_{17,c} + p_{17,a} + p_{17,d} = p_{5,c} + p_{5,a} + p_{5,d}) \end{aligned} \tag{$S_{5,17}$}$$

$$\begin{aligned}&p_{19,d} < p_{6,d} \lor p_{19,d} + p_{19,b} < p_{6,d} + p_{6,b} \lor p_{19,d} + p_{19,b} + p_{19,a} < p_{6,d} + p_{6,b} + p_{6,a}\\ &\quad \lor (p_{19,d} = p_{6,d} \land p_{19,d} + p_{19,b} = p_{6,d} + p_{6,b} \land p_{19,d} + p_{19,b} + p_{19,a} = p_{6,d} + p_{6,b} + p_{6,a})\end{aligned} \tag{$S_{6,19}$}$$

$$p_{42,c} + p_{42,a} \leq p_{6,c} + p_{6,a} \tag{$S_{6,42}$}$$

$$\begin{aligned}&p_{43,d} < p_{7,a} \lor p_{43,d} + p_{43,b} < p_{7,a} + p_{7,c} \lor p_{43,d} + p_{43,b} + p_{43,a} < p_{7,a} + p_{7,c} + p_{7,d}\\ &\quad \lor (p_{43,d} = p_{7,a} \land p_{43,d} + p_{43,b} = p_{7,a} + p_{7,c} \land p_{43,d} + p_{43,b} + p_{43,a} = p_{7,a} + p_{7,c} + p_{7,d})\end{aligned} \tag{$S_{7,43}$}$$

$$\begin{aligned}&p_{26,a} < p_{8,d} \lor p_{26,a} + p_{26,b} + p_{26,d} < p_{8,d} + p_{8,b} + p_{8,a}\\ &\quad \lor (p_{26,a} = p_{8,d} \land p_{26,a} + p_{26,b} + p_{26,d} = p_{8,d} + p_{8,b} + p_{8,a})\end{aligned} \tag{$S_{8,26}$}$$

$$\begin{aligned}&p_{18,d} + p_{18,a} < p_{9,d} + p_{9,a} \lor p_{18,d} + p_{18,a} + p_{18,c} < p_{9,d} + p_{9,a} + p_{9,c}\\ &\quad \lor (p_{18,d} + p_{18,a} = p_{9,d} + p_{9,a} \land p_{18,d} + p_{18,a} + p_{18,c} = p_{9,d} + p_{9,a} + p_{9,c})\end{aligned} \tag{$S_{9,18}$}$$

$$p_{35,b} + p_{35,a} \leq p_{9,b} + p_{9,a} \tag{$S_{9,35}$}$$

$$p_{40,b} + p_{40,a} \leq p_{9,b} + p_{9,a} \tag{$S_{9,40}$}$$

$$\begin{aligned}&p_{12,b} + p_{12,d} < p_{10,c} + p_{10,a} \lor p_{12,b} + p_{12,d} + p_{12,a} < p_{10,c} + p_{10,a} + p_{10,d}\\ &\quad \lor (p_{12,b} + p_{12,d} = p_{10,c} + p_{10,a} \land p_{12,b} + p_{12,d} + p_{12,a} = p_{10,c} + p_{10,a} + p_{10,d})\end{aligned} \tag{$S_{10,12}$}$$

$$\begin{aligned}&p_{15,a} + p_{15,c} < p_{10,d} + p_{10,b} \lor p_{15,a} + p_{15,c} + p_{15,d} < p_{10,d} + p_{10,b} + p_{10,a}\\ &\quad \lor (p_{15,a} + p_{15,c} = p_{10,d} + p_{10,b} \land p_{15,a} + p_{15,c} + p_{15,d} = p_{10,d} + p_{10,b} + p_{10,a})\end{aligned} \tag{$S_{10,15}$}$$

$$\begin{aligned}&p_{19,a} + p_{19,c} < p_{10,d} + p_{10,b} \lor p_{19,a} + p_{19,c} + p_{19,d} < p_{10,d} + p_{10,b} + p_{10,a}\\ &\quad \lor (p_{19,a} + p_{19,c} = p_{10,d} + p_{10,b} \land p_{19,a} + p_{19,c} + p_{19,d} = p_{10,d} + p_{10,b} + p_{10,a})\end{aligned} \tag{$S_{10,19}$}$$

$$p_{36,a} + p_{36,b} \leq p_{10,d} + p_{10,c} \tag{$S_{10,36}$}$$

$$p_{10,a} + p_{10,c} + p_{10,d} \leq p_{12,d} + p_{12,b} + p_{12,a} \tag{$S_{12,10}$}$$

$$\begin{aligned}&p_{16,c} + p_{16,a} < p_{12,c} + p_{12,a} \lor p_{16,c} + p_{16,a} + p_{16,d} < p_{12,c} + p_{12,a} + p_{12,d}\\ &\quad \lor (p_{16,c} + p_{16,a} = p_{12,c} + p_{12,a} \land p_{16,c} + p_{16,a} + p_{16,d} = p_{12,c} + p_{12,a} + p_{12,d})\end{aligned} \tag{$S_{12,16}$}$$

$$p_{44,b} + p_{44,a} \leq p_{12,b} + p_{12,a} \tag{$S_{12,44}$}$$

$$\begin{aligned}&p_{15,d} + p_{15,c} < p_{13,d} + p_{13,b} \lor p_{15,d} + p_{15,c} + p_{15,a} < p_{13,d} + p_{13,b} + p_{13,a}\\ &\quad \lor (p_{15,d} + p_{15,c} = p_{13,d} + p_{13,b} \land p_{15,d} + p_{15,c} + p_{15,a} = p_{13,d} + p_{13,b} + p_{13,a})\end{aligned} \tag{$S_{13,15}$}$$

$$\begin{aligned}&p_{27,a} < p_{13,a} \lor p_{27,a} + p_{27,c} < p_{13,a} + p_{13,b} \lor p_{27,a} + p_{27,c} + p_{27,d} < p_{13,a} + p_{13,b} + p_{13,d}\\ &\quad \lor (p_{27,a} = p_{13,a} \land p_{27,a} + p_{27,c} = p_{13,a} + p_{13,b} \land\\ &\qquad p_{27,a} + p_{27,c} + p_{27,d} = p_{13,a} + p_{13,b} + p_{13,d})\end{aligned} \tag{$S_{13,27}$}$$

$$\begin{aligned}&p_{9,a} < p_{14,a} \lor p_{9,a} + p_{9,d} < p_{14,a} + p_{14,d} \lor p_{9,a} + p_{9,d} + p_{9,c} < p_{14,a} + p_{14,d} + p_{14,c}\\ &\quad \lor (p_{9,a} = p_{14,a} \land p_{9,a} + p_{9,d} = p_{14,a} + p_{14,d} \land p_{9,a} + p_{9,d} + p_{9,c} = p_{14,a} + p_{14,d} + p_{14,c})\end{aligned} \tag{$S_{14,9}$}$$

$$\begin{aligned}&p_{16,c} < p_{14,d} \lor p_{16,c} + p_{16,d} < p_{14,d} + p_{14,c} \lor\\ &\quad (p_{16,c} = p_{14,d} \land p_{16,c} + p_{16,d} = p_{14,d} + p_{14,c})\end{aligned} \tag{$S_{14,16}$}$$

$$p_{34,d} + p_{34,b} + p_{34,a} \leq p_{14,c} + p_{14,b} + p_{14,a} \tag{$S_{14,34}$}$$

$$\begin{aligned}&p_{5,d} < p_{15,a} \lor p_{5,d} + p_{5,b} < p_{15,a} + p_{15,c} \lor p_{5,d} + p_{5,b} + p_{5,a} < p_{15,a} + p_{15,c} + p_{15,d}\\ &\quad \lor (p_{5,d} = p_{15,a} \land p_{5,d} + p_{5,b} = p_{15,a} + p_{15,c} \land p_{5,d} + p_{5,b} + p_{5,a} = p_{15,a} + p_{15,c} + p_{15,d})\end{aligned} \tag{$S_{15,5}$}$$

$$\begin{aligned} &p_{7,d} + p_{7,b} < p_{15,d} + p_{15,b} \lor p_{7,d} + p_{7,b} + p_{7,a} < p_{15,d} + p_{15,b} + p_{15,a} \\ &\quad \lor (p_{7,d} + p_{7,b} = p_{15,d} + p_{15,b} \land p_{7,d} + p_{7,b} + p_{7,a} = p_{15,d} + p_{15,b} + p_{15,a}) \end{aligned} \tag{$S_{15,7}$}$$

$$\begin{aligned} &p_{10,d} < p_{15,a} \lor p_{10,d} + p_{10,b} < p_{15,a} + p_{15,c} \lor p_{10,d} + p_{10,b} + p_{10,a} < p_{15,a} + p_{15,c} + p_{15,d} \\ &\quad \lor (p_{10,d} = p_{15,a} \land p_{10,d} + p_{10,b} = p_{15,a} + p_{15,c} \land \\ &\qquad p_{10,d} + p_{10,b} + p_{10,a} = p_{15,a} + p_{15,c} + p_{15,d}) \end{aligned} \tag{$S_{15,10}$}$$

$$p_{13,d} + p_{13,b} \leq p_{15,d} + p_{15,c} \tag{$S_{15,13}$}$$

$$p_{3,c} + p_{3,a} \leq p_{17,c} + p_{17,a} \tag{$S_{17,3}$}$$

$$p_{5,c} + p_{5,a} \leq p_{17,c} + p_{17,a} \tag{$S_{17,5}$}$$

$$p_{7,c} + p_{7,a} \leq p_{17,c} + p_{17,a} \tag{$S_{17,7}$}$$

$$p_{11,c} + p_{11,a} \leq p_{17,c} + p_{17,a} \tag{$S_{17,11}$}$$

$$p_{9,d} + p_{9,a} \leq p_{18,d} + p_{18,a} \tag{$S_{18,9}$}$$

$$p_{1,b} + p_{1,a} \leq p_{19,b} + p_{19,a} \tag{$S_{19,1}$}$$

$$p_{10,b} + p_{10,d} \leq p_{19,c} + p_{19,a} \tag{$S_{19,10}$}$$

$$p_{27,d} + p_{27,b} \leq p_{19,d} + p_{19,c} \tag{$S_{19,27}$}$$

$$\begin{aligned} &p_{21,c} < p_{20,a} \lor p_{21,c} + p_{21,b} < p_{20,a} + p_{20,c} \\ &\quad \lor (p_{21,c} = p_{20,a} \land p_{21,c} + p_{21,b} = p_{20,a} + p_{20,c}) \end{aligned} \tag{$S_{20,21}$}$$

$$\begin{aligned} &p_{35,c} < p_{21,c} \lor p_{35,c} + p_{35,b} + p_{35,a} < p_{21,c} + p_{21,b} + p_{21,a} \\ &\quad \lor (p_{35,c} = p_{21,c} \land p_{35,c} + p_{35,b} + p_{35,a} = p_{21,c} + p_{21,b} + p_{21,a}) \end{aligned} \tag{$S_{21,35}$}$$

$$\begin{aligned} &p_{29,a} < p_{22,d} \lor p_{29,a} + p_{29,c} + p_{29,d} < p_{22,d} + p_{22,b} + p_{22,a} \\ &\quad \lor (p_{29,a} = p_{22,d} \land p_{29,a} + p_{29,c} + p_{29,d} = p_{22,d} + p_{22,b} + p_{22,a}) \end{aligned} \tag{$S_{22,29}$}$$

$$\begin{aligned} &p_{32,a} < p_{22,a} \lor p_{32,a} + p_{32,b} < p_{22,a} + p_{22,b} \\ &\quad \lor (p_{32,a} = p_{22,a} \land p_{32,a} + p_{32,b} = p_{22,a} + p_{22,b}) \end{aligned} \tag{$S_{22,32}$}$$

$$p_{12,c} + p_{12,a} \leq p_{23,c} + p_{23,a} \tag{$S_{23,12}$}$$

$$p_{18,c} + p_{18,d} \leq p_{23,d} + p_{23,c} \tag{$S_{23,18}$}$$

$$p_{19,d} + p_{19,b} + p_{19,a} \leq p_{23,d} + p_{23,b} + p_{23,a} \tag{$S_{23,19}$}$$

$$\begin{aligned} &p_{34,b} < p_{24,c} \lor p_{34,b} + p_{34,d} < p_{24,c} + p_{24,a} \\ &\quad \lor (p_{34,b} = p_{24,c} \land p_{34,b} + p_{34,d} = p_{24,c} + p_{24,a}) \end{aligned} \tag{$S_{24,34}$}$$

$$\begin{aligned} &p_{26,d} + p_{26,c} < p_{25,d} + p_{25,b} \lor p_{26,d} + p_{26,c} + p_{26,a} < p_{25,d} + p_{25,b} + p_{25,a} \\ &\quad \lor (p_{26,d} + p_{26,c} = p_{25,d} + p_{25,b} \land p_{26,d} + p_{26,c} + p_{26,a} = p_{25,d} + p_{25,b} + p_{25,a}) \end{aligned} \tag{$S_{25,26}$}$$

$$\begin{aligned} &p_{36,a} < p_{25,a} \lor p_{36,a} + p_{36,c} < p_{25,a} + p_{25,c} \\ &\quad \lor (p_{36,a} = p_{25,a} \land p_{36,a} + p_{36,c} = p_{25,a} + p_{25,c}) \end{aligned} \tag{$S_{25,36}$}$$

$$\begin{aligned} &p_{8,d} < p_{26,a} \lor p_{8,d} + p_{8,b} < p_{26,a} + p_{26,c} \\ &\quad \lor (p_{8,d} = p_{26,a} \land p_{8,d} + p_{8,b} = p_{26,a} + p_{26,c}) \end{aligned} \tag{$S_{26,8}$}$$

$$p_{13,b} + p_{13,a} \leq p_{27,c} + p_{27,a} \tag{$S_{27,13}$}$$

$$\begin{aligned} &p_{19,d} + p_{19,c} < p_{27,d} + p_{27,b} \lor p_{19,d} + p_{19,c} + p_{19,a} < p_{27,d} + p_{27,b} + p_{27,a} \\ &\quad \lor (p_{19,d} + p_{19,c} = p_{27,d} + p_{27,b} \land p_{19,d} + p_{19,c} + p_{19,a} = p_{27,d} + p_{27,b} + p_{27,a}) \end{aligned} \tag{$S_{27,19}$}$$

$$\begin{aligned} &p_{32,d} < p_{28,a} \lor p_{32,d} + p_{32,b} < p_{28,a} + p_{28,c} \\ &\quad \lor (p_{32,d} = p_{28,a} \land p_{32,d} + p_{32,b} = p_{28,a} + p_{28,c}) \end{aligned} \tag{$S_{28,32}$}$$

$$\begin{aligned}&p_{39,a} < p_{28,a} \lor p_{39,a} + p_{39,c} < p_{28,a} + p_{28,b}\\ &\qquad \lor (p_{39,a} = p_{28,a} \land p_{39,a} + p_{39,c} = p_{28,a} + p_{28,b})\end{aligned} \tag{$S_{28,39}$}$$

$$\begin{aligned}&p_{39,d} < p_{29,a} \lor p_{39,d} + p_{39,c} < p_{29,a} + p_{29,b}\\ &\qquad \lor (p_{39,d} = p_{29,a} \land p_{39,d} + p_{39,c} = p_{29,a} + p_{29,b})\end{aligned} \tag{$S_{29,39}$}$$

$$\begin{aligned}&p_{21,b} + p_{21,a} < p_{30,b} + p_{30,a} \lor p_{21,b} + p_{21,a} + p_{21,d} < p_{30,b} + p_{30,a} + p_{30,d}\\ &\qquad \lor (p_{21,b} + p_{21,a} = p_{30,b} + p_{30,a} \land p_{21,b} + p_{21,a} + p_{21,d} = p_{30,b} + p_{30,a} + p_{30,d})\end{aligned} \tag{$S_{30,21}$}$$

$$\begin{aligned}&p_{41,c} < p_{30,c} \lor p_{41,c} + p_{41,b} + p_{41,a} < p_{30,c} + p_{30,b} + p_{30,a}\\ &\qquad \lor (p_{41,c} = p_{30,c} \land p_{41,c} + p_{41,b} + p_{41,a} = p_{30,c} + p_{30,b} + p_{30,a})\end{aligned} \tag{$S_{30,41}$}$$

$$\begin{aligned}&p_{38,b} + p_{38,d} < p_{31,d} + p_{31,b} \lor p_{38,b} + p_{38,d} + p_{38,c} < p_{31,d} + p_{31,b} + p_{31,a}\\ &\qquad \lor (p_{38,b} + p_{38,d} = p_{31,d} + p_{31,b} \land p_{38,b} + p_{38,d} + p_{38,c} = p_{31,d} + p_{31,b} + p_{31,a})\end{aligned} \tag{$S_{31,38}$}$$

$$\begin{aligned}&p_{22,b} + p_{22,a} < p_{32,b} + p_{32,a} \lor p_{22,b} + p_{22,a} + p_{22,d} < p_{32,b} + p_{32,a} + p_{32,d}\\ &\qquad \lor (p_{22,b} + p_{22,a} = p_{32,b} + p_{32,a} \land p_{22,b} + p_{22,a} + p_{22,d} = p_{32,b} + p_{32,a} + p_{32,d})\end{aligned} \tag{$S_{32,22}$}$$

$$\begin{aligned}&p_{28,a} < p_{32,d} \lor p_{28,a} + p_{28,c} + p_{28,d} < p_{32,d} + p_{32,b} + p_{32,a}\\ &\qquad \lor (p_{28,a} = p_{32,d} \land p_{28,a} + p_{28,c} + p_{28,d} = p_{32,d} + p_{32,b} + p_{32,a})\end{aligned} \tag{$S_{32,28}$}$$

$$\begin{aligned}&p_{5,a} < p_{33,a} \lor p_{5,a} + p_{5,b} < p_{33,a} + p_{33,b}\\ &\qquad \lor (p_{5,a} = p_{33,a} \land p_{5,a} + p_{5,b} = p_{33,a} + p_{33,b})\end{aligned} \tag{$S_{33,5}$}$$

$$p_{22,d} + p_{22,c} \leq p_{33,d} + p_{33,c} \tag{$S_{33,22}$}$$

$$\begin{aligned}&p_{24,c} < p_{34,b} \lor p_{24,c} + p_{24,a} + p_{24,d} < p_{34,b} + p_{34,d} + p_{34,a}\\ &\qquad \lor (p_{24,c} = p_{34,b} \land p_{24,c} + p_{24,a} + p_{24,d} = p_{34,b} + p_{34,d} + p_{34,a})\end{aligned} \tag{$S_{34,24}$}$$

$$\begin{aligned}&p_{9,a} < p_{35,a} \lor p_{9,a} + p_{9,b} < p_{35,a} + p_{35,b}\\ &\qquad \lor (p_{9,a} = p_{35,a} \land p_{9,a} + p_{9,b} = p_{35,a} + p_{35,b})\end{aligned} \tag{$S_{35,9}$}$$

$$p_{21,c} + p_{21,b} + p_{21,a} \leq p_{35,c} + p_{35,b} + p_{35,a} \tag{$S_{35,21}$}$$

$$\begin{aligned}&p_{10,d} < p_{36,a} \lor p_{10,d} + p_{10,c} < p_{36,a} + p_{36,b}\\ &\qquad \lor (p_{10,d} = p_{36,a} \land p_{10,d} + p_{10,c} = p_{36,a} + p_{36,b})\end{aligned} \tag{$S_{36,10}$}$$

$$\begin{aligned}&p_{25,c} + p_{25,a} < p_{36,c} + p_{36,a} \lor p_{25,c} + p_{25,a} + p_{25,d} < p_{36,c} + p_{36,a} + p_{36,d}\\ &\qquad \lor (p_{25,c} + p_{25,a} = p_{36,c} + p_{36,a} \land p_{25,c} + p_{25,a} + p_{25,d} = p_{36,c} + p_{36,a} + p_{36,d})\end{aligned} \tag{$S_{36,25}$}$$

$$p_{39,d} + p_{39,c} \leq p_{36,d} + p_{36,c} \tag{$S_{36,39}$}$$

$$\begin{aligned}&p_{42,d} < p_{37,a} \lor p_{42,d} + p_{42,b} < p_{37,a} + p_{37,b}\\ &\qquad \lor (p_{42,d} = p_{37,a} \land p_{42,d} + p_{42,b} = p_{37,a} + p_{37,b})\end{aligned} \tag{$S_{37,42}\,(1)$}$$

$$\begin{aligned}&p_{42,d} < p_{37,c} \lor p_{42,d} + p_{42,b} < p_{37,c} + p_{37,d}\\ &\qquad \lor (p_{42,d} = p_{37,c} \land p_{42,d} + p_{42,b} = p_{37,c} + p_{37,d})\end{aligned} \tag{$S_{37,42}\,(2)$}$$

$$\begin{aligned}&p_{2,c} + p_{2,a} < p_{39,c} + p_{39,a} \lor p_{2,c} + p_{2,a} + p_{2,d} < p_{39,c} + p_{39,a} + p_{39,d}\\ &\qquad \lor (p_{2,c} + p_{2,a} = p_{39,c} + p_{39,a} \land p_{2,c} + p_{2,a} + p_{2,d} = p_{39,c} + p_{39,a} + p_{39,d})\end{aligned} \tag{$S_{39,2}$}$$

$$\begin{aligned}&p_{29,a} + p_{29,b} < p_{39,d} + p_{39,c} \lor p_{29,a} + p_{29,b} + p_{29,d} < p_{39,d} + p_{39,c} + p_{39,a}\\ &\qquad \lor (p_{29,a} + p_{29,b} = p_{39,d} + p_{39,c} \land p_{29,a} + p_{29,b} + p_{29,d} = p_{39,d} + p_{39,c} + p_{39,a})\end{aligned} \tag{$S_{39,29}$}$$

$$\begin{aligned}&p_{36,d} + p_{36,c} < p_{39,d} + p_{39,c} \lor p_{36,d} + p_{36,c} + p_{36,a} < p_{39,d} + p_{39,c} + p_{39,a}\\ &\qquad \lor (p_{36,d} + p_{36,c} = p_{39,d} + p_{39,c} \land p_{36,d} + p_{36,c} + p_{36,a} = p_{39,d} + p_{39,c} + p_{39,a})\end{aligned} \tag{$S_{39,36}$}$$

$$p_{31,d} + p_{31,b} + p_{31,a} \leq p_{41,c} + p_{41,b} + p_{41,a} \tag{$S_{41,31}$}$$

$$\begin{aligned} &p_{3,d} < p_{42,d} \lor p_{3,d} + p_{3,b} < p_{42,d} + p_{42,b} \lor p_{3,d} + p_{3,b} + p_{3,a} < p_{42,d} + p_{42,b} + p_{42,a} \\ &\quad \lor (p_{3,d} = p_{42,d} \land p_{3,d} + p_{3,b} = p_{42,d} + p_{42,b} \land p_{3,d} + p_{3,b} + p_{3,a} = p_{42,d} + p_{42,b} + p_{42,a}) \end{aligned} \tag{$S_{42,3}$}$$

$$\begin{aligned} &p_{11,d} < p_{42,c} \lor p_{11,d} + p_{11,b} < p_{42,c} + p_{42,a} \\ &\quad \lor (p_{11,d} = p_{42,c} \land p_{11,d} + p_{11,b} = p_{42,c} + p_{42,a}) \end{aligned} \tag{$S_{42,11}$}$$

$$p_{24,b} + p_{24,a} \leq p_{42,b} + p_{42,a} \tag{$S_{42,24}$}$$

$$\begin{aligned} &p_{12,b} + p_{12,a} < p_{44,b} + p_{44,a} \lor p_{12,b} + p_{12,a} + p_{12,d} < p_{44,b} + p_{44,a} + p_{44,d} \\ &\quad \lor (p_{12,b} + p_{12,a} = p_{44,b} + p_{44,a} \land p_{12,b} + p_{12,a} + p_{12,d} = p_{44,b} + p_{44,a} + p_{44,d}) \end{aligned} \tag{$S_{44,12}$}$$

$$p_{40,c} + p_{40,d} \leq p_{44,d} + p_{44,c} \tag{$S_{44,40}$}$$

$$\begin{aligned} &p_{31,c} + p_{31,d} < p_{45,b} + p_{45,a} \lor p_{31,c} + p_{31,d} + p_{31,b} < p_{45,b} + p_{45,a} + p_{45,c} \\ &\quad \lor (p_{31,c} + p_{31,d} = p_{45,b} + p_{45,a} \land p_{31,c} + p_{31,d} + p_{31,b} = p_{45,b} + p_{45,a} + p_{45,c}) \end{aligned} \tag{$S_{45,31}$}$$

$$p_{20,c} + p_{20,a} \leq p_{46,c} + p_{46,a} \tag{$S_{46,20}$}$$

$$\begin{aligned} &p_{37,a} + p_{37,c} < p_{46,d} + p_{46,b} \lor p_{37,a} + p_{37,c} + p_{37,d} < p_{46,d} + p_{46,b} + p_{46,a} \\ &\quad \lor (p_{37,a} + p_{37,c} = p_{46,d} + p_{46,b} \land p_{37,a} + p_{37,c} + p_{37,d} = p_{46,d} + p_{46,b} + p_{46,a}) \end{aligned} \tag{$S_{46,37}$}$$

$$p_{30,b} + p_{30,a} \leq p_{47,b} + p_{47,a} \tag{$S_{47,30}$}$$

Table 3: The Strategy-Proofness conditions used in the impossibility proof.

Table 4 lists the manipulations that were used to obtain these strategyproofness conditions: the first column gives the name of the manipulation condition in the form $(S_{i,j})$, which also contains the information which two profiles are involved in the manipulation (R_i and R_j) The next columns contain the manipulating agent, her truthful preferences, and the false preferences that she needs to submit. The last column gives the permutation of the alternatives that yields R_j when applied to the manipulated instance of R_i.

Condition	Agent	Old Preferences	New Preferences	Permutation
$(S_{1,2})$	1	$\{c,d\},\{a,b\}$	$\{c,d\},a,b$	$(a)(b)(c)(d)$
$(S_{1,19})$	3	$a,b,\{c,d\}$	$\{a,b\},\{c,d\}$	$(a)(b)(c)(d)$
$(S_{2,1})$	2	$\{c,d\},a,b$	$\{c,d\},\{a,b\}$	$(a)(b)(c)(d)$
$(S_{2,38})$	1	$\{a,c\},\{b,d\}$	$\{a,c\},b,d$	$(a)(b)(c)(d)$
$(S_{4,8})$	4	$d,c,\{a,b\}$	$c,d,\{a,b\}$	$(a)(b)(c\ d)$
$(S_{4,18})$	3	$c,\{a,b\},d$	$\{a,b,c\},d$	$(a)(b)(c)(d)$
$(S_{4,47})$	2	$\{a,d\},\{b,c\}$	$\{a,d\},c,b$	$(a)(b)(c)(d)$
$(S_{5,7})$	3	$\{a,c\},d,b$	a,c,d,b	$(a)(b)(c)(d)$
$(S_{5,10})$	4	$d,\{a,b\},c$	$\{b,d\},a,c$	$(a\ d)(b\ c)$
$(S_{5,17})$	3	$\{a,c\},d,b$	$\{a,c\},\{b,d\}$	$(a)(b)(c)(d)$
$(S_{6,19})$	4	d,b,a,c	$\{b,d\},a,c$	$(a)(b)(c)(d)$
$(S_{6,42})$	3	$\{a,c\},\{b,d\}$	$c,a,\{b,d\}$	$(a)(b)(c)(d)$

$(S_{7,43})$	3	a, c, d, b	$a, \{c, d\}, b$	$(a\ d)(b\ c)$
$(S_{8,26})$	3	$d, \{a, b\}, c$	$d, b, \{a, c\}$	$(a\ d)(b\ c)$
$(S_{9,18})$	2	$\{a, d\}, c, b$	$\{a, d\}, \{b, c\}$	$(a)(b)(c)(d)$
$(S_{9,35})$	1	$\{a, b\}, \{c, d\}$	$a, b, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{9,40})$	1	$\{a, b\}, \{c, d\}$	$\{a, b\}, c, d$	$(a)(b)(c)(d)$
$(S_{10,12})$	3	$\{a, c\}, d, b$	$\{a, c, d\}, b$	$(a\ d)(b\ c)$
$(S_{10,15})$	4	$\{b, d\}, a, c$	d, b, a, c	$(a\ d)(b\ c)$
$(S_{10,19})$	4	$\{b, d\}, a, c$	$\{b, d\}, \{a, c\}$	$(a\ d)(b\ c)$
$(S_{10,36})$	2	$\{c, d\}, \{a, b\}$	$d, c, \{a, b\}$	$(a\ d)(b\ c)$
$(S_{12,10})$	4	$\{a, b, d\}, c$	$\{b, d\}, a, c$	$(a\ d)(b\ c)$
$(S_{12,16})$	3	$\{a, c\}, d, b$	a, c, d, b	$(a)(b)(c)(d)$
$(S_{12,44})$	2	$\{a, b\}, \{c, d\}$	$\{a, b\}, d, c$	$(a)(b)(c)(d)$
$(S_{13,15})$	3	$\{b, d\}, a, c$	$\{b, d\}, \{a, c\}$	$(a)(b\ c)(d)$
$(S_{13,27})$	4	a, b, d, c	$\{a, b\}, \{c, d\}$	$(a)(b\ c)(d)$
$(S_{14,9})$	4	a, d, c, b	$\{a, d\}, c, b$	$(a)(b)(c)(d)$
$(S_{14,16})$	2	$d, c, \{a, b\}$	$\{c, d\}, \{a, b\}$	$(a)(b)(c\ d)$
$(S_{14,34})$	3	$\{a, b, c\}, d$	$b, \{a, c\}, d$	$(a)(b)(c\ d)$
$(S_{15,5})$	4	a, c, d, b	$a, \{c, d\}, b$	$(a\ d)(b\ c)$
$(S_{15,7})$	3	$\{b, d\}, a, c$	$d, \{a, b\}, c$	$(a)(b)(c)(d)$
$(S_{15,10})$	4	a, c, d, b	$\{a, c\}, d, b$	$(a\ d)(b\ c)$
$(S_{15,13})$	2	$\{c, d\}, \{a, b\}$	$\{c, d\}, a, b$	$(a)(b\ c)(d)$
$(S_{17,3})$	3	$\{a, c\}, \{b, d\}$	$c, a, \{b, d\}$	$(a)(b)(c)(d)$
$(S_{17,5})$	3	$\{a, c\}, \{b, d\}$	$\{a, c\}, d, b$	$(a)(b)(c)(d)$
$(S_{17,7})$	3	$\{a, c\}, \{b, d\}$	a, c, d, b	$(a)(b)(c)(d)$
$(S_{17,11})$	3	$\{a, c\}, \{b, d\}$	c, a, b, d	$(a)(b)(c)(d)$
$(S_{18,9})$	2	$\{a, d\}, \{b, c\}$	$\{a, d\}, c, b$	$(a)(b)(c)(d)$
$(S_{19,1})$	1	$\{a, b\}, \{c, d\}$	$a, b, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{19,10})$	4	$\{a, c\}, \{b, d\}$	$\{a, c\}, d, b$	$(a\ d)(b\ c)$
$(S_{19,27})$	2	$\{c, d\}, \{a, b\}$	$\{c, d\}, a, b$	$(a)(b\ c)(d)$
$(S_{20,21})$	3	$a, c, \{b, d\}$	$a, \{c, d\}, b$	$(a\ c\ b\ d)$
$(S_{21,35})$	3	$c, \{a, b\}, d$	$\{a, b, c\}, d$	$(a)(b)(c)(d)$
$(S_{22,29})$	3	$d, \{a, b\}, c$	$\{b, d\}, a, c$	$(a\ d)(b\ c)$
$(S_{22,32})$	4	$a, b, \{c, d\}$	$\{a, b\}, d, c$	$(a)(b)(c)(d)$
$(S_{23,12})$	3	$\{a, c\}, \{b, d\}$	$\{a, c\}, d, b$	$(a)(b)(c)(d)$
$(S_{23,18})$	2	$\{c, d\}, \{a, b\}$	$c, d, \{a, b\}$	$(a)(b)(c\ d)$
$(S_{23,19})$	4	$\{a, b, d\}, c$	$\{b, d\}, a, c$	$(a)(b)(c)(d)$
$(S_{24,34})$	3	$c, a, \{b, d\}$	$c, \{a, d\}, b$	$(a\ d)(b\ c)$
$(S_{25,26})$	2	$\{b, d\}, a, c$	$\{b, d\}, \{a, c\}$	$(a)(b\ c)(d)$
$(S_{25,36})$	4	$a, c, \{b, d\}$	$\{a, c\}, d, b$	$(a)(b)(c)(d)$

$(S_{26,8})$	4	$a, c, \{b, d\}$	$a, \{c, d\}, b$	$(a\ d)(b\ c)$
$(S_{27,13})$	3	$\{a, c\}, \{b, d\}$	a, c, d, b	$(a)(b\ c)(d)$
$(S_{27,19})$	2	$\{b, d\}, a, c$	$\{b, d\}, \{a, c\}$	$(a)(b\ c)(d)$
$(S_{28,32})$	4	$a, c, \{b, d\}$	$a, \{c, d\}, b$	$(a\ d)(b\ c)$
$(S_{28,39})$	3	$a, b, \{c, d\}$	$\{a, b\}, d, c$	$(a)(b\ c)(d)$
$(S_{29,39})$	3	$a, b, \{c, d\}$	$\{a, b\}, d, c$	$(a\ d)(b\ c)$
$(S_{30,21})$	4	$\{a, b\}, d, c$	$a, b, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{30,41})$	3	$c, \{a, b\}, d$	$\{a, b, c\}, d$	$(a)(b)(c)(d)$
$(S_{31,38})$	1	$\{b, d\}, a, c$	$\{b, d\}, c, a$	$(a\ c)(b\ d)$
$(S_{32,22})$	4	$\{a, b\}, d, c$	$a, b, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{32,28})$	3	$d, \{a, b\}, c$	$d, b, \{a, c\}$	$(a\ d)(b\ c)$
$(S_{33,5})$	3	$a, b, \{c, d\}$	$\{a, b\}, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{33,22})$	1	$\{c, d\}, \{a, b\}$	$d, c, \{a, b\}$	$(a)(b)(c)(d)$
$(S_{34,24})$	3	$b, \{a, d\}, c$	$b, d, \{a, c\}$	$(a\ d)(b\ c)$
$(S_{35,9})$	2	$a, b, \{c, d\}$	$\{a, b\}, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{35,21})$	3	$\{a, b, c\}, d$	$c, \{a, b\}, d$	$(a)(b)(c)(d)$
$(S_{36,10})$	4	$a, b, \{c, d\}$	$\{a, b\}, \{c, d\}$	$(a\ d)(b\ c)$
$(S_{36,25})$	2	$\{a, c\}, d, b$	$a, c, \{b, d\}$	$(a)(b)(c)(d)$
$(S_{36,39})$	1	$\{c, d\}, \{a, b\}$	$\{c, d\}, a, b$	$(a)(b)(c)(d)$
$(S_{37,42}\,(1))$	3	$a, b, \{c, d\}$	a, b, d, c	$(a\ d)(b)(c)$
$(S_{37,42}\,(2))$	4	$c, d, \{a, b\}$	c, d, b, a	$(a\ c\ d\ b)$
$(S_{39,2})$	1	$\{a, c\}, d, b$	$\{a, c\}, \{b, d\}$	$(a)(b)(c)(d)$
$(S_{39,29})$	4	$\{c, d\}, a, b$	$d, c, \{a, b\}$	$(a\ d)(b\ c)$
$(S_{39,36})$	4	$\{c, d\}, a, b$	$\{c, d\}, \{a, b\}$	$(a)(b)(c)(d)$
$(S_{41,31})$	3	$\{a, b, c\}, d$	$\{b, c\}, a, d$	$(a)(b)(c\ d)$
$(S_{42,3})$	3	d, b, a, c	$d, \{a, b\}, c$	$(a)(b)(c)(d)$
$(S_{42,11})$	4	$c, a, \{b, d\}$	$c, \{a, b\}, d$	$(a\ b)(c\ d)$
$(S_{42,24})$	2	$\{a, b\}, \{c, d\}$	$b, a, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{44,12})$	3	$\{a, b\}, d, c$	$\{a, b\}, \{c, d\}$	$(a)(b)(c)(d)$
$(S_{44,40})$	1	$\{c, d\}, \{a, b\}$	$c, d, \{a, b\}$	$(a)(b)(c\ d)$
$(S_{45,31})$	3	$\{a, b\}, c, d$	$b, a, \{c, d\}$	$(a\ d)(b\ c)$
$(S_{46,20})$	3	$\{a, c\}, \{b, d\}$	$a, c, \{b, d\}$	$(a)(b)(c)(d)$
$(S_{46,37})$	1	$\{b, d\}, a, c$	$\{b, d\}, \{a, c\}$	$(a\ d)(b\ c)$
$(S_{47,30})$	1	$\{a, b\}, \{c, d\}$	$\{a, b\}, d, c$	$(a)(b)(c)(d)$

Table 4: The manipulations required to obtain the Strategy-Proofness conditions in Table 3

References

[ABB13] Haris Aziz, Felix Brandt, and Markus Brill. *On the Tradeoff between Economic Efficiency and Strategyproofness in Randomized Social Choice*. In: *Proceedings of the 12th International Conference on Autonomous Agents and Multi-Agent Systems*. AAMAS '13. IFAA-MAS, 2013, pp. 455–462. ISBN: 978-1-4503-1993-5. URL: `http://dl.acm.org/citation.cfm?id=2484920.2484993`.

[ABB14a] Haris Aziz, Florian Brandl, and Felix Brandt. *On the Incompatibility of Efficiency and Strategyproofness in Randomized Social Choice*. In: *Proceedings of the 28th AAAI Conference on Artificial Intelligence*. AAAI '14. AAAI Press, 2014, pp. 545–551. URL: `http://www.aaai.org/ocs/index.php/AAAI/AAAI14/paper/view/8534`.

[ABB14b] Haris Aziz, Florian Brandl, and Felix Brandt. *Universal Pareto Dominance and Welfare for Plausible Utility Functions*. In: *Proceedings of the Fifteenth ACM Conference on Economics and Computation*. EC '14. Palo Alto, California, USA: ACM, 2014, pp. 331–332. ISBN: 978-1-4503-2565-3. DOI: `10.1145/2600057.2602866`.

[App+07] David L. Applegate et al. *Exact Solutions to Linear Programming Problems*. In: *Operations Research Letters* 35.6 (2007), pp. 693–699. ISSN: 0167-6377. DOI: `http://dx.doi.org/10.1016/j.orl.2006.12.010`.

[Bal14] Clemens Ballarin. *Locales: A Module System for Mathematical Theories*. English. In: *Journal of Automated Reasoning* 52.2 (2014), pp. 123–153. ISSN: 0168-7433. DOI: `10.1007/s10817-013-9284-7`.

[BBG16] Florian Brandl, Felix Brandt, and Christian Geist. *Proving the incompatibility of Efficiency and Strategyproofness via SMT solving*. In: *Proceedings of the 25th International Joint Conference on Artificial Intelligence* (*IJCAI*) (2016). Forthcoming.

[BBS16] Florian Brandl, Felix Brandt, and Warut Suksompong. *The Impossibility of Extending Random Dictatorship to Weak Preferences*. In: *Economics Letters* 141 (2016), pp. 44–47. ISSN: 0165-1765. DOI: `http://dx.doi.org/10.1016/j.econlet.2016.01.028`.

[BM01] Anna Bogomolnaia and Hervé Moulin. *A New Solution to the Random Assignment Problem*. In: *Journal of Economic Theory* 100.2 (2001), pp. 295–328. ISSN: 0022-0531. DOI: `http://dx.doi.org/10.1006/jeth.2000.2710`.

[Böh09] Sascha Böhme. *Proof Reconstruction for Z3 in Isabelle/HOL*. In: *7th International Workshop on Satisfiability Modulo Theories* (*SMT '09*). 2009. URL: `http://www4.in.tum.de/~boehmes/proofrec.pdf`.

[Bra+16] Felix Brandt et al. *Handbook of Computational Social Choice*. 1st ed. Cambridge University Press, 2016. ISBN: 9781107060432.

[Ebe16a] Manuel Eberl. *Randomised Social Choice Theory*. In: *Archive of Formal Proofs* (May 2016). Formal proof development. ISSN: 2150-914x. URL: `http://isa-afp.org/entries/Randomised_Social_Choice.shtml`.

[Ebe16b] Manuel Eberl. *The Incompatibility of SD-Efficiency and SD-Strategy-Proofness*. In: *Archive of Formal Proofs* (May 2016). Formal proof development. ISSN: 2150-914x. URL: `http://isa-afp.org/entries/SDS_Impossibility.shtml`.

[Esp06] Daniel G. Espinoza. *On Linear Programming, Integer Programming and Cutting Planes*. PhD thesis. Georgia Institute of Technology, 2006. URL: `http://www.dii.uchile.cl/~daespino/files/espinoza_daniel_g_200605_phd.pdf`.

[Gib73] Allan Gibbard. *Manipulation of Voting Schemes: A General Result*. In: *Econometrica* 41.4 (1973), pp. 587–601. ISSN: 14680262. DOI: `10.2307/1914083`.

[Gib77] Allan Gibbard. *Manipulation of Schemes that Mix Voting with Chance*. In: *Econometrica* 45.3 (1977), pp. 665–681. ISSN: 14680262. DOI: `10.2307/1911681`.

[Hal+15] Thomas C. Hales et al. *A Formal Proof of the Kepler Conjecture*. In: *arXiv* 1501.02155 (2015). URL: `http://arxiv.org/abs/1501.02155`.

[KP15] Ondřej Kunčar and Andrei Popescu. *A Consistent Foundation for Isabelle/HOL*. In: *Interactive Theorem Proving: 6th International Conference, ITP 2015, Nanjing, China, August 24-27, 2015, Proceedings* (2015). Ed. by Christian Urban and Xingyuan Zhang, pp. 234–252. DOI: `10.1007/978-3-319-22102-1_16`.

[Kun15] Ondřej Kunčar. *Types, Abstraction and Parametric Polymorphism in Higher-Order Logic*. PhD thesis. TU München, 2015. URL: `http://www21.in.tum.de/~kuncar/documents/kuncar-phdthesis.pdf`.

[Nan98] Shasikanta Nandeibam. *An alternative proof of Gibbard's random dictatorship result*. In: *Social Choice and Welfare* 15.4 (1998), pp. 509–519. ISSN: 1432-217X. DOI: `10.1007/s003550050120`.

[Ste14] Jon Lund Steffensen. *QSopt_ex – An Exact Linear Programming Solver*. 2014. URL: `https://github.com/jonls/qsopt-ex`.

[Tuc99] Warwick Tucker. *The Lorenz Attractor Exists* (*revised March 10, 1999*). PhD thesis. Uppsala universitet, 1999. URL: `http://www2.math.uu.se/~warwick/main/thesis_2.1`.