A Generalized Probabilistic Gibbard-Satterthwaite Theorem

Jonathan Potter
jmp2909@rit.edu

April 15, 2014

Chair	Christopher Homan
Reader	Edith Hemaspaandra
Observer	Zack Butler

Abstract

Friedgut, Kalai, and Nisan have proved that social choice functions can be successfully manipulated by random preference reordering with non-negligible probability [FKN08]. However, their results require two restrictions: the social choice function must be neutral, and the election must have at most 3 alternatives. In this thesis we focus on removing the later restriction and generalizing the results to elections with any number of candidates. We also provide a survey of related work analyzing and comparing results from a number of authors.

Acknowledgments

First and foremost, I would like to thank my advisor, Christopher Homan, without whom this work and my academic endeavors would have been greatly diminished. Thank you for many hours of instruction and encouragement, and for challenging me to better myself. You have made this an enjoyable experience and I have learned and grown by leaps and bounds, both academically and otherwise.

Second, I would like to thank my family—which I am so lucky to be a part of—whose love and support undergird all of my endeavors.

Contents

Chapter 1

Introduction

In this thesis we endeavor to extend the results of Friedgut, Kalai, and Nisan [FKN08] who proved that social choice functions can be successfully manipulated by random preference reordering with non-negligible probability. However, there are two main restrictions on their results: the social choice function must be neutral and the election must have at most 3 alternatives. We attempt to remove the later restriction in order to generalize the results to elections with any number of candidates.

Our proof draws upon many aspects of Friedgut, Kalai, and Nisan's proof. Their proof is done in three steps, with the first two steps being already written in general terms, while the third is restricted to 3 alternatives. Therefore we need only generalize the third step. We rely heavily on lattice theory and combinatorics to prove this generalization.

1.1 Importance

It is obvious, and widely accepted that election systems are important to society. They are essential to democracy, which is the foundation of many nations' governments, and are also used in many non-political situations—anywhere a group of independent agents needs to come to a consensus. They are used in schools, electing board members for a business, and stock holders voting on issues affecting a company. Election systems are not even wholly restricted to humans. Elections can be used by artificial intelligence systems when a group of agents needs to make a decision [ER91, ER93, PHG00, DKNS01, FKS03], and they can be used in internet page ranking algorithms for search engines [CELM07]. Studying the stability of election systems under noise can even be used to determine how resistant certain

systems, e.g. network transfers, are to error [Sho08].

However, it is less clear that manipulation in elections—especially random manipulation—is important, so we will attempt to describe its importance by briefly explaining the history behind its investigation.

One obvious criteria for a good election system is fairness [CDE$^+$06], and it is generally accepted that the winning candidate should, on the whole, represent the will the constituents'. It is easy to recognize a fair election system if there are only two candidates: the one preferred by the majority of voters should win. But with a larger number of candidates, determining the fairness of an election system is more difficult.

Marquis de Condorcet was one of the first people to study the issue of fairness in election systems. He proposed that the winning candidate be the candidate who would win a head-to-head election against each of the other candidates, and such a winner is known as the *Condorcet winner.* Unfortunately, Condorcet also proved that a Condorcet winner does not always exist. Nevertheless, this criterion for fairness, called the *Condorcet criterion*, was one of the first formal fairness criteria, and is still widely used today.

In 1950, Kenneth Arrow, an American economist who was interested in the fairness of social welfare functions, made a large contribution to the field of social choice theory with his impossibility theorem [Arr50, Arr63]. This theorem demonstrates that no social welfare function can "fairly" convert the preferences of voters into a society-wide preference list, by showing that no social welfare function can satisfy the following criteria (which will be further described in the next chapter): unrestricted domain, independence of irrelevant alternatives, unanimity, and non-dictatorship.

One of the great enemies of fairness in election systems is *manipulation* (or strategic voting or tactical voting). Manipulation is when an individual purposefully misrepresents his preferences, hoping to achieve a more favorable outcome in the election. One way to avoid manipulation would be to devise a voting rule that is non-manipulable. Unfortunately, the Gibbard-Satterthwaite theorem states that every voting rule that is not a dictatorship, and under which any alternative can win, is subject to manipulation [Gib73, Sat75, DS00]. This means that we cannot make manipulation impossible via a cleverly devised voting rule.

In an attempt to circumvent the Gibbard-Satterthwaite theorem, Bartholdi, Tovey, and Trick studied the computational difficulty of finding a winner for various voting rules. For example, they showed that the Dodgson method mentioned above [Dod76] is actually infeasible to manipulate for the simple reason that figuring out the winner of the election is NP-hard. Therefore,

it is not sufficient for a desirable voting rule to be hard to manipulate: it must also be also be efficient to determine a winner.

Many others have followed in the vein of searching for a computational barrier to manipulation, but the majority of these results deal with the worst-case complexity of manipulation. In 2006, work by Conitzer and Sandholm [CS06] along with that of Procaccia and Rosenschein [PR06] showed that while manipulation can be hard in the worst case, it is often much easier in the average case. In the next few years more work was done to make this concern even more well-founded [PR07, EHRS07].

In 2008, Friedgut, Kalai, and Nisan [FKN08], instead of studying worst-case manipulation, performed a probabilistic analysis of random manipulation. That is, instead of a voter intelligently manipulating an election, which can be difficult in terms of worst-case complexity, he simply chooses his manipulation randomly (if his most preferred candidate is not already winning). They proved that even a random manipulation will succeed with non-negligible probability. This is significant because no matter how hard it is to find a profitable manipulation in the worst-case, it is trivial to find a random manipulation. If the probability of success of a random manipulation is high enough, it could completely bypass the computational barrier to manipulation. These are the results we hope to extend in the remainder of this thesis.

1.2 Difficulty

The difficulty of this problem can be seen by recent work that generalizes the results of Friedgut, Kalai, and Nisan. First, its difficulty can be seen by Friedgut, Kalai, and Nisan themselves failing to generalize it, both in the original paper [FKN08], and also later when they removed the neutrality constraint [FKKN11]. If it were an easy task, they would have done it from the outset.

In addition, other authors have done work along the same lines, but still without coming up with a general result. In 2008 Xia and Conitzer were able to prove a similar theorem for any number of candidates, but instead of neutrality they assumed 5 other conditions for the voting rule [XC08]:

- Homogeneity

- Anonymity

- Non-imposition

- Canceling out

- Stability

These conditions are formally defined and explained in Chapter 4: Related Work, and also by Xia and Conitzer themselves.

These conditions are stricter than the neutrality assumption of Friedgut, Kalai, and Nisan, in the sense that they do not capture all of the "common" voting rules, e.g. Bucklin.

Around the same time Dobzinski and Procaccia published complementary results for two voters and social choice functions satisfying unanimity (the Pareto principle) [DP08]. They proved the following:

Theorem 1.2.1 (Dobzinski and Procaccia)**.** *Let f be a Pareto-optimal SCF and let $n = 2$, $m \geq 3$, and $\delta < \frac{1}{32m^9}$. If f is δ-strategyproof then f is $16m^8\delta$-dictatorial.*

The fact that all of these authors worked on the same problem over multiple years and were unable to achieve a general result speaks to its difficulty.

1.3 Independent Work

Unfortunately for us, but fortunately for the field of social choice theory as a whole, Isaksson, Kindler, and Mossel *have*, independently and during the writing of this thesis, published a brilliant generalization of the original theorem of Friedgut, Kalai, and Nisan and even improved slightly upon the results [IKM10]. Translating their results into the terminology we have been using, they proved that for a neutral social choice function f with $m \geq 4$ alternatives and n voters that is ϵ-far from dictatorship, a uniformly chosen profile will be manipulable with probability at least $2^{-1}\epsilon^2 n^{-4} m^{-6}(m!)^{-3}$.

Later Friedgut et al. removed the neutrality constraint from their original theorem, and added an author [FKKN11].

Finally, Mossel and Rácz [MR11] took ideas from these two proofs and created a unified proof with the same results as Isaksson, Kindler, and Mossel, but without the neutrality constraint.

Though these results have independently achieved the goals we set out with, we believe that our work is still useful. At the very least ours simply stands as an alternate proof. However, our proof has the benefit that it uses very similar techniques to those of the original proof by Friedgut, Kalai, and Nisan, and additionally we believe that our proof is much simpler and more easily understood.

1.4 Proof Summary

Here we summarize our generalization and our main result, both for reference and to act as an outline of our method. Some of this notation will be defined in subsequent chapters, and might not be understood until then.

The proof we are generalizing is broken up into three steps. In the original paper they are called Step 1, Step 2, and Step 3, and in [FKKN11] they are called the following respectively:

Step 1: application of a quantitative version of Arrow's impossibility theorem,

Step 2: reduction from an SCF with low dependence on irrelevant alternatives to a GSWF with a low paradox probability,

Step 3: reduction from low manipulation power to low dependence on irrelevant alternatives,

In the original paper, Friedgut, Kalai, and Nisan were able to generalize Step 1 and Step 2 as follows:

Lemma 1.4.1 (Generalized Step 1). *For every fixed m and $\epsilon > 0$ there exists $\delta > 0$ such that if $F = f^{\otimes \binom{m}{2}}$ is a neutral IIA GSWF over m alternatives with $f : \{0,1\}^n \to \{0,1\}$, and $\Delta(f, DICT) > \epsilon$, then F has probability of at least $\delta \geq (C\epsilon)^{\lfloor m/3 \rfloor}$ of not having a Generalized Condorcet Winner, where $C > 0$ is an absolute constant.*

Lemma 1.4.2 (Generalized Step 2). *For every fixed m there exists $\delta > 0$ such that for all $\epsilon > 0$ the following holds. Let f be a neutral SCF among m alternatives such that $\Delta(f, DICT) > \epsilon$. Then for all (a, b) we have $M^{a,b}(f) \geq \delta$.*

Therefore, we focus on generalizing Step 3 so that together with the already generalized Steps 1 and 2 we will have a generalized main theorem. The original Step 3 was:

Lemma 1.4.3 (Non-General Step 3). *For every SCF f on 3 alternatives and every $a, b \in A$, $M^{a,b} \leq \sum_i M_i \cdot 6$*

And the generalization we attempt to prove is:

Lemma 1.4.4 (Generalized Step 3). *For every SCF f on m alternatives and every $a, b \in A$, $M^{a,b} \leq \sum_i M_i \cdot m!$*

When we put together all 3 generalized steps we get our main result:

Theorem 1.4.5 (Main Result)**.** *There exists a constant $C > 0$ such that for every $\epsilon > 0$ the following holds. If f is a neutral SCF for n voters over m alternatives and $\Delta(f, g) > \epsilon$ for any dictatorship g, then f has total manipulability: $\sum_{i=1}^{n} M_i(f) \geq \frac{(C\epsilon)^{\lfloor m/3 \rfloor}}{m!}$.*

1.5 Structure of the Remaining Chapters

Chapter 2: Preliminaries. In the next chapter we introduce the preliminaries, which include formal definitions and notation to serve as a reference for use in the rest of the thesis. The preliminaries are often elementary and provide a technical foundation for the following work.

Chapter 3: Background. Here we give some background information on the field of social choice theory and describe how it has evolved, leading to the problem we are addressing in this work.

Chapter 4: Related Work. In the related work chapter we describe, in a moderate amount of detail, the results and methods of various other authors relating both to this thesis, and to the work of Friedgut, Kalai, and Nisan on which our work is based.

Chapter 5: Results. This is the technical portion of the thesis in which we prove foundational lemmas and build up a proof of our main result.

Chapter 2

Preliminaries

In this chapter we present the formal definitions we will need for the rest of this thesis. These serve as a reference as well as an introduction to the technical work contained in the following chapters. Some definitions are very basic and many will already be known to the reader; however, they are stated explicitly here to provide maximum clarity and a solid foundation upon which to present the rest of our work.

For additional definitions, which are out of the scope of this thesis, the reader may refer to textbooks on set theory [Kun80] and lattice theory [Bir95].

2.1 Definitions

We will begin with basic definitions regarding set theory and lattice theory, and then towards the end of this section we will transition to definitions from social choice theory.

Definition 2.1.1. A *permutation* of a set X is a bijective function from X to X.

Definition 2.1.2. A *total ordering* over a set X is a binary relation on X which is antisymmetric, transitive, and total.

Although technically speaking permutations and total orderings are different constructs (bijective functions versus binary relations), they often have similar applications. For example, given a totally-ordered set X and a permutation σ on X, we can construct a total ordering $<_R = \{(x, y) \mid x, y \in X, \sigma^{-1}(x) < \sigma^{-1}(y)\}$ which is structurally analogous to σ. Likewise, for any

well-ordered set X and a total ordering $<_R$ over X, one could construct a permutation σ from $<_R$ where $\sigma : X \to X$ such that $\sigma(x) = y$ iff

$$|\{z \in X \mid z < x\}| = |\{z \in X \mid z <_R y\}|.$$

For countable sets we will sometimes view permutations and total orders as sequences, using a subscript notation, provided our meaning is clear from context.

Definition 2.1.3. We use $S(X)$ to denote the set of all permutations of X.

Definition 2.1.4. We use $L(X)$ to denote the set of all total orders over X.

Definition 2.1.5. We define a *poset*, or *partially ordered set*, to be $(X, \leq)$, where X is a set and $\leq$ is a binary relation on X that is antisymmetric, transitive, and reflexive. $\leq$ is called "partial" because not every pair of elements in X needs to be related by $\leq$, as opposed to a total ordering which must relate every pair.

Definition 2.1.6. For any partial order $\leq_x$ over a set X and $a, b \in X$, we define the following additional relations over X:

$$a \geq_x b \equiv b \leq_x a,$$
$$a =_x b \equiv a \leq_x b \text{ and } b \leq_x a,$$
$$a \neq_x b \equiv \text{not } a =_x b,$$
$$a <_x b \equiv a \leq_x b \text{ and } a \neq_x b,$$
$$a >_x b \equiv a \geq_x b \text{ and } a \neq_x b.$$

We will treat these additional relations as implicitly defined, and will not define them explicitly for each partial order individually.

Definition 2.1.7. For any poset $(P, \leq)$, a *lower bound* of a subset $X \subseteq P$ is an element $a \in P$ such that $a \leq x$ for every $x \in X$. A *greatest lower bound* is a *lower bound* that is greater than or equal to every other *lower bound*. We denote this *greatest lower bound* as $\inf_P X$, calling it the *infimum* [Bir67] and also as $\bigwedge_P X$, calling it the *meet*. When X contains only two elements, we can use the meet as a binary operator: $\bigwedge_P \{a, b\} = a \wedge_P b$. When P is obvious from context we will simply write $\inf X$ or $\bigwedge X$. If the infimum exists, it is unique because posets are antisymmetric.

Definition 2.1.8. For any poset $(P, \leq)$, an *upper bound* of a subset $X \subseteq P$ is an element $a \in P$ such that $a \geq x$ for every $x \in X$. A *least upper bound* is an *upper bound* that is less than or equal to every other *upper bound*. We denote this *least upper bound* as $\sup_P X$, calling it the *supremum* [Bir67] and also as $\bigvee_P X$, calling it the *join*. When X contains only two elements, we can use the join as a binary operator: $\bigvee_P \{a, b\} = a \vee_P b$. When P is obvious from context we will simply write $\sup X$ or $\bigvee X$. If the supremum exists, it is unique because posets are antisymmetric. The supremum is the same as the infimum in the inverse order, and vice versa.

Definition 2.1.9. A poset, $(P, \leq)$, is a *lattice* if for any $x, y \in P$ both the meet and join of $\{x, y\}$ exist. Note that the meet and join are unique by definition (if they exist).

Definition 2.1.10. The *transitive closure* of a binary relation R on a set X is the transitive relation R^t on X such that $R \subseteq R^t$ and R^t is minimal [LP98, p. 337].

Definition 2.1.11. For any poset $(P, \leq)$, let σ be a permutation of P. We define the *inversions* of σ to be a binary relation Inv_σ on P:

$$\text{Inv}_\sigma = \{(i, j) \mid i, j \in P, i < j, \sigma^{-1}(i) > \sigma^{-1}(j)\}.$$

We can read $i \,\text{Inv}_\sigma\, j$ as "i is inverted with j in σ".

Inv is a transitive relation because for $n \geq 1$ and $i, k, j \in P$ we have that if

$$(i, k), (k, j) \in \text{Inv}_\sigma$$

then both of the following hold:

$$i < k < j$$
$$\sigma^{-1}(i) > \sigma^{-1}(k) > \sigma^{-1}(j).$$

And therefore $(i, j) \in \text{Inv}_\sigma$.

Definition 2.1.12. For any poset $(P, \leq)$, let σ and π be permutations of P. We define the *Kendall tau distance*, K, between σ and π to be the number of adjacent swaps necessary to get from σ to π or vice versa. More formally:

$$K(\sigma, \pi) = \sum_{\{i,j\} \in P} \overline{K}_{i,j}(\sigma, \pi)$$

where

$$\overline{K}_{i,j}(\sigma, \pi) = \begin{cases} 0 & \text{if } i \text{ and } j \text{ are in the same order in } \sigma \text{ and } \pi \\ 1 & \text{if } i \text{ and } j \text{ are in the opposite order in } \sigma \text{ and } \pi \end{cases}$$

Alternatively we can define the Kendall tau distance in terms of inversions:

$$K(\sigma, \pi) = |\operatorname{Inv}_\sigma \triangle \operatorname{Inv}_\pi|,$$

with $\triangle$ denoting symmetric difference.

Definition 2.1.13. For any poset $(P, \leq)$, let $x, y \in P$. We say that x is a *predecessor* of y if $x < y$. We say that x is a *direct predecessor* of y if x is the greatest predecessor of y.

Definition 2.1.14. For any poset $(P, \leq)$, let $x, y \in P$. We say that x is a *successor* of y if $x > y$. We say that x is a *direct successor* of y if x is the least successor of y.

In the next couple of definitions and many of the lemmas in this section, we will be investigating lattices whose elements are permutations of a set. That is, given a set Y, we will study some of the properties of the lattice $(S(Y), \leq)$.

Definition 2.1.15 ($\leq_s$)**.** Let $(Y, \leq)$ be a poset and let $X = S(Y)$. We define the partial ordering $\leq_s$ on X such that for all $\sigma, \pi \in X$:

$$\sigma \leq_s \pi \iff \operatorname{Inv}_\sigma \supseteq \operatorname{Inv}_\pi.$$

In addition, if $(X, \leq_s)$ is a lattice, then for any $\sigma, \pi \in X$ we also have [Mar94]:

$$\operatorname{Inv}_{\sigma \wedge \pi} = (\operatorname{Inv}_\sigma \cup \operatorname{Inv}_\pi)^t.$$

Note that ^{t} indicates the transitive closure as defined in Definition 2.1.10.

Definition 2.1.16 ($X^{ij}, \leq^{ij}$)**.** Let Y be a set, let $X = S(Y)$, and let $(X, \leq)$ be a lattice. For any $i, j \in Y$ we define

$$X^{ij} = \{x \in X \mid x^{-1}(i) < x^{-1}(j)\}.$$

We then define the partial ordering, $\leq^{ij}$, over X^{ij} such that for all $x, y \in X^{ij}$:

$$x \leq^{ij} y \iff x \leq y$$

We will now introduce some definitions having to do with social choice theory. Throughout this paper we will use n to represent the number of voters in an election, and m to represent the number of alternatives (candidates).

Definition 2.1.17. Let $C = \{1, \ldots, m\}$ be the set of all *alternatives* (candidates).

Definition 2.1.18. We define a *preference list* to be a total order over C. Therefore the set of all preference lists is $L(C)$. Alternatively we can view a preference list as a permutation on C, and it will be obvious from context which approach we are using.

Definition 2.1.19. We define a *preference profile* to be $p \in L(C)^n$. And we define $P = L(C)^n$ to be the set of all preference profiles.

Definition 2.1.20. We define a *voting rule*, or *social choice function* (SCF), to be a function $f : P \to C$.

Definition 2.1.21. We define an *election* to be simply a voting rule paired with a profile: (f, p) where f is a voting rule and $p \in P$.

Definition 2.1.22. Let $v \in L(C)$ be a preference list, and let $x, y \in C$ be two alternatives. Since v is actually a total ordering, we denote $(x, y) \in v$ by

$$x <_v y$$

and if this is the case we view x as being ranked above y in v and we say that x beats y, and denote this as

$$x \succ_v y.$$

We view x as being ranked below y in v if

$$x >_v y$$

and we would say that x is beaten by y, we denote this as

$$x \prec_v y$$

Definition 2.1.23. For a set of candidates $D \subseteq C$, for a preference list $v \in L(C)$ and a preference profile $p \in P$ we denote v and p *restricted to* D by $v|_D$ and $p|_D$ respectively. $v|_D$ means v after all the candidates who are

not in D have been removed. $p|_D$ means that every preference list in p has been restricted to D.

We will sometimes wish to restrict to every alternative except those in D in which case we will write $v|_{\overline{D}}$ where the universe is understood to be C.

Since we will often use restriction when comparing two preference lists we will write $x|_D = y|_D$ simply as $x =_D y$.

Definition 2.1.24. For any sequence x, and $i \in \{1, \ldots, |x|\}$ we will denote by x_{-i}, x with x_i removed. Therefore (x_{-i}, x'_i) will mean a sequence equal to x except with x'_i replacing x_i.

Definition 2.1.25. A *successful manipulation* (or *profitable manipulation*) by voter i of a SCF f at profile p is a preference list p'_i such that

$$f((p_{-i}, p'_i)) \succ_i f((p_{-i}, p_i)).$$

Definition 2.1.26. The *distance* between two SCFs is defined to be the fraction of inputs on which they differ:

$$\mathbf{D}(f, g) = \mathbb{P}(f(\sigma) \neq g(\sigma)).$$

When dealing with a set of SCFs, G, we take the minimum distance over all SCFs in that set:

$$\mathbf{D}(f, G) = \min_{g \in G} \mathbf{D}(f, g).$$

For example, we will sometimes say that a SCF, f, is ϵ-*far from dictatorship*. This means that $\mathbf{D}(f, DICT) > \epsilon$, where $DICT$ is the set of SCFs that are dictatorships.

Definition 2.1.27. A SCF is *neutral* if its result does not change with the permutation of the alternatives. Formally, let f be a SCF, let σ be a permutation over the set of alternatives, and let π be a function which applies σ to each alternative in a preference list:

$$\pi(v) = (\sigma(v_1), \ldots, \sigma(v_m)).$$

Then f is neutral iff

$$f(\pi(p_1), \ldots, \pi(p_n)) = \sigma(f(p_1, \ldots, p_n)).$$

Chapter 3

Background

3.1 History of Social Choice Theory

Voting systems are not a recent invention—they have been around in one form or another for thousands of years. The earliest democracies resembling what we use today date back to around 508 BC in Athens, Greece, and the general idea of elections was used even before that in many other parts of the world [dem11]. In Athens, the assembly was the core of democracy, and any male citizen of at least eighteen years of age was allowed to attend and to vote [Hei52]. Athenians voted directly on public policy, instead of electing representatives, and voting was done by majority rule. Voting was also used outside of the assembly in a process known as ostracism which was used to exile individuals if necessary. This was done using the plurality voting rule, whereby each man wrote a name on a piece of pottery and the person with the most votes was exiled [OR02].

Both the majority rule and the plurality systems used in early Greek democracy were very simple. One drawback of these systems is that each voter can only cast a vote for a single candidate even if, for example, there are two candidates that he thinks are very good. In reality a voter usually does not like one candidate and hate all the others, but usually likes various candidates to different degrees. Therefore, a more accurate way to represent each voter's opinion is with a ranked list of all the candidates, which in social choice theory is called a preference list.

In more recent centuries, voting has taken great strides forward from the simpler methods used in ancient Greece. In 1770, Jean-Charles de Borda proposed a voting system, known now as the Borda count, as a way of electing members of the French Academy of Sciences [Bor81]. As a side

note, although the voting system is named after Borda, it has recently been discovered that Ramon Llull independently invented the same system even earlier—in the 13th century [HP01]. In the Borda count system, each candidate receives points based on his rank in each voter's preference list, i.e., a candidate will get the most points for each first place ranking, he will get slightly fewer points for each second place ranking, and so on. The winning candidate is the one who receives the greatest total number of points. It was around the time Borda proposed this system that voting systems began to be studied academically.

Majority rule, plurality, and the Borda count are a few examples of voting systems, but there are many others. Given the large number of voting systems, and that each system seems to have various strengths and weaknesses, it is useful to compare them to each other. The most obvious criterion for a good voting system is fairness [CDE$^+$06]. It seems natural that the best voting system is the one which best represents the constituents' preferences. Fairness of a voting system is easy to recognize if there are only two candidates: the candidate who is preferred by the majority of voters should win. But with a larger number of candidates, determining the fairness of a voting system is not so obvious.

Interest in the fairness of voting systems prompted Marquis de Condorcet, a contemporary of Borda, to propose that the winning candidate of an election be the candidate who would win a head-to-head election against each of the other candidates (he proposed this in the year 1785). Such a winner is known as the *Condorcet winner*. Unfortunately, Condorcet also proved that a Condorcet winner does not always exist because majority preferences are intransitive in elections with more than two alternatives [lmdCC85, BNM$^+$98]. In other words, it is possible to have alternative $a \succ$ (beats)b, $b \succ c$, $c \succ a$. A voting system that gives the Condorcet winner if one exists is said to satisfy the *Condorcet criterion*. The Condorcet criterion was one of the first formal fairness criteria, and is still widely used today.

In 1876, Charles Dodgson (also known as Lewis Carroll) proposed a voting system, satisfying the Condorcet criterion, known as Dodgson's method. Dodgson's method declares the winner to be whichever alternative can become a Condorcet winner with the fewest adjacent swaps in voters' preference lists [Dod76]. More precisely, given the original profile p, we select a profile p' such that p' has a Condorcet winner and the total Kendall tau distance (see Definition 2.1.12) between p and p' is minimum (compared to all possible profiles). Then the winner is the alternative that wins under p'. One major drawback of this method is that computing the winner is

NP-hard [BTT89a].

In 1950, an American economist named Kenneth Arrow made a large contribution to the field of Social Choice Theory with his impossibility theorem. Arrow was interested in the fairness of social welfare functions, which are similar to the social choice functions except that instead of a single winner, they yield a full ranking of all alternatives. Arrow's theorem [Arr50] (which he strengthened in 1963 [Arr63]) demonstrates that no social welfare function can "fairly" convert the preferences of voters into a society-wide preference list. While "fair" is clearly subjective, he gave a list of basic properties which seem intuitively required for fairness:

Unrestricted domain (universality) All individual preferences are allowed and yield a valid group preference.

Independence of irrelevant alternatives If all voters' preferences between alternatives x and y remain the same, the group preference between x and y is unchanged even if voters change their preferences regarding other alternatives.

Pareto principle (unanimity) Unanimity of individual preferences implies a group preference. E.g. if all individuals prefer alternative x to y, then the group will prefer x to y.

Non-dictatorship There is no voter whose preference always dictates the group's preference.

Arrow proved that these properties are inconsistent: no social welfare function can satisfy all of these properties, hence, no social welfare function can be completely fair.

The work done by Condorcet and Arrow is widely regarded as being foundational to the modern field of social choice theory, and marks a transition from viewing social choice as a purely practical problem to a more rigorous theoretical study.

3.2 History of Manipulation

One problem relating to the issue of fairness in social choice theory is that of manipulation (or strategic voting or tactical voting). Manipulation is when an individual purposefully misrepresents his preferences hoping to get a more favorable outcome in the election. For example, if a voter knows that his most preferred alternative has no chance of winning the election, he

may instead say that he prefers a different alternative, so that even though his favorite alternative cannot win, at least his second choice alternative has a better chance of winning. For a formal definition of manipulation, see Definition 2.1.25. Manipulation will benefit the voter but will not benefit the society in general, because by lying about his preferences the voter has skewed the results of the election in his favor. Therefore, it is beneficial to search for ways to avoid manipulation in social choice.

One way to avoid manipulation would be to devise a voting rule that is non-manipulable. Unfortunately, in 1973 the Gibbard-Satterthwaite theorem was published which states that every voting rule satisfying the following properties is subject to manipulation.

Non-dictatorship There is no voter whose preference always dictates the group preference.

Non-imposition Every alternative has the possibility of winning.

It would certainly seem that any reasonable voting rule would need to satisfy both of these criteria, hence, any reasonable voting rule is manipulable [Gib73, Sat75, DS00]. This means that we cannot make manipulation impossible via a cleverly devised voting rule—a rather disappointing conclusion.

Until this point in its history, social choice theory had been separate from computer science—and computer science was a very young discipline at this point. But around this time a new sub-field of social choice theory was spawned: computational social choice theory, which seeks to use computer science to solve problems in social choice theory. In 1989, Bartholdi, Tovey, and Trick proposed a computational barrier to manipulation in voting systems [BTT89b]: instead of trying to make manipulation impossible, they endeavored to make it computationally intractable [CELM07]. Even if a profitable manipulation exists, it is of no practical use if it is computationally infeasible to find. They were able to demonstrate that while many voting rules are easy to manipulate (a manipulation can be found in polynomial time), the problem of finding a manipulation for certain scoring rules is NP-complete. They called rules that can be manipulated in polynomial time *vulnerable*, and those for which manipulation is NP-hard *resistant*.

This research paved the way for approaching social choice problems from a computational footing. Bartholdi, Tovey, and Trick also studied the computational difficulty of finding a winner for various voting rules. For example, they showed that the Dodgson method mentioned above [Dod76] is actually infeasible to manipulate for the simple reason that figuring out the

winner of the election is NP-hard. Therefore, it is not sufficient for a desirable voting rule to be hard to manipulate; it must also be also be efficient to determine a winner.

In 1991, Bartholdi and Orlin [BO91] added to the above results by showing that the Single Transferable Vote (STV) rule was both resistant to manipulation, and quick to determine a winner. Although STV has problems of its own [Bra82, DK77, FB83, Hol89, Mou88], it is encouraging to see that it is possible for an efficient voting rule to resist manipulation.

In 2002, Conitzer and Sandholm took a slightly different approach [CS02] (which they later extended [CSL07]), studying coalition manipulation. Instead of a single voter manipulating an election, a group (coalition) of voters work together to manipulate an election. This vein of research has since been extended in various directions [CS03, EL05a, FHH06, HHR07, PRZ07, EL05b].

The work mentioned so far which attempts to erect a computational barrier to manipulation is encouraging, and may indeed provide ways to prevent manipulation in voting systems. However, it deals with the worst-case complexity of manipulation. In 2006, work by Conitzer and Sandholm [CS06] along with that of Procaccia and Rosenschein [PR06] showed that while manipulation can be hard in the worst case, it is much easier in the average case. In the next few years more work was done to make this concern even more well-founded [PR07, EHRS07]. Work along these lines by Friedgut, Kalai, and Nisan [FKN08] in 2008, is the main inspiration for this thesis, and has also spawned other work which will be discussed further in the Related Work chapter.

Chapter 4

Related Work

We will now take an in-depth look at some of the results leading up to and related to our own. For definitions of any unfamiliar notation, the reader should refer either to the Preliminaries chapter, or to the cited work that is being discussed. In general, an election will consist of a SCF f, a set of m alternatives C, n voters, and a profile $p \in L(C)^n$.

4.1 Elections Can be Manipulated Often

Complexity theorists have analyzed many voting systems using computational complexity as a means of inhibiting manipulation [BTT89b, HHR09]. Friedgut, Kalai, and Nisan, on the other hand, took a probabilistic approach to this problem [FKN08]. Instead of studying worst-case manipulation, they performed a probabilistic analysis of random manipulation. That is, instead of a voter intelligently manipulating an election, which can be difficult in terms of worst-case complexity, he simply chooses his manipulation randomly (if his most preferred candidate is not winning already). They proved that even a random manipulation will succeed with non-negligible probability. This is significant because no matter how hard it is in the worst-case to find a profitable manipulation, if it is trivial to find a random manipulation, that could be enough.

More formally, they defined a metric, *manipulation power* $M_i(f)$, of voter i on a social choice function f to be the probability that p'_i is a profitable manipulation by voter i, where p is a profile and p'_i is a preference list which are both chosen uniformly at random. Their main result is that there exists a constant C such that for 3 alternatives, n voters, and a neutral social choice function f that is ϵ-far from dictatorship ($\epsilon > 0$) then

$$\sum_{i=1}^{n} M_i(f) \geq C\epsilon^2.$$

This means that when ϵ is fixed—it is fixed once a voting rule is determined—then some voter has more than his share (a non-negligible amount) of manipulation power: $\max_i M_i(f) \geq \Omega(\frac{1}{n})$ [FKN08].

Besides the limitation to three alternatives, these results are incredibly general. They rest on two main assumptions which all common social choice functions satisfy. The first is the *impartial culture assumption* which states that voters are independent and equally likely to select any of the possible orderings of alternatives. In other words, votes are selected uniformly at random. The second assumption is the neutrality of the social choice function. The neutrality assumption was removed by Friedgut, Kalai, and Nisan in 2011 [FKKN11].

But the restriction to three alternatives renders these results useless for many practical applications, and it is also less satisfactory than a general solution from a theoretical standpoint. Therefore many people have worked to generalize these results.

4.2 A sufficient condition for voting rules to be frequently manipulable

In 2008 Xia and Conitzer were able to prove a similar theorem for any number of candidates, but instead of neutrality they assumed five other conditions for the voting rule [XC08]:

Homogeneity Let $k \in \mathbb{N}$, let p be a profile of length n, and let $j \in \mathbb{N}$ such that $k \leq j < (k + kn)$. A voting rule is homogeneous if $f(p) = f(p')$, where p' consists of k copies of every vote in p:

$$p'_j = p_{\lfloor j/k \rfloor}.$$

Anonymity The result of the election does not depend on the names of the voters. Formally, given a profile p and a permutation $\sigma(p)$ then: $f(p) = f(\sigma(p))$.

Non-imposition Every alternative has the possibility of winning.

Canceling out Adding the set of all linear orders to the votes does not change the result. More formally, for any profile p we have that: $f(p) = f(p \cup L(C))$.

Stability Given alternatives $C = \{c_1, c_2, \ldots, c_m\}$, there exists a profile p such that:

1. p and $D_m(p)$ are both stable, i.e. slight modifications don't change the winner. (See below for a definition of D_m.)

2. $f(p) = c_1$

3. $f(D_m(p)) = c_2$

Where D_m is defined such that if $D_m(p) = p'$, then $p|_{C\setminus\{c_m\}} = p'|_{C\setminus\{c_m\}}$ and the position of c_m is uniformly distributed in p'.

For a more formal definition of D_m we must first give a couple of preliminary definitions. First, we define a merging function $M \colon L(C)^n \times C^n \to L(C)^n$ such that

$$M((v_1, \ldots, v_n), (i_1, \ldots, i_n)) = (M(v_1, i_1), \ldots, M(v_n, i_n))$$

where $M(v_j, i_j)$ is the preference list that results from moving c_m to the $i_j{}^{\text{th}}$ position. Second, we note that any profile p can be written as $\sum_{i=1}^{m!} p_i l_i$ where $l_i \in L(C)$ and p_i indicates how many times the linear order l_i appears in p.

Then we can define D_m as follows. Given a profile $p = \sum_{i=1}^{m!} p_i l_i$, we define [XC08]:

$$D_m(p) = \sum_{i=1}^{m!} \sum_{j=1}^{m!} \frac{p_i}{m} M(l_i, j).$$

However, these conditions are stricter than the neutrality assumption of Friedgut, Kalai, and Nisan, in the sense that they do not capture all of the "common" voting rules, e.g. Bucklin.

4.3 Frequent manipulability of elections: The case of two voters

Around the same time Dobzinski and Procaccia published complementary results for two voters and social choice functions satisfying unanimity (the Pareto principle) [DP08]. They proved the following:

Theorem 4.3.1 (Dobzinski and Procaccia)**.** *Let f be a Pareto-optimal SCF and let $n = 2$, $m \geq 3$, and $\delta < \frac{1}{32m^9}$. If f is δ-strategyproof then f is $16m^8\delta$-dictatorial.*

We will translate these results into the same terms used by Friedgut, Kalai, and Nisan so that we can easily compare their results. According to Dobzinski and Procaccia, being δ-strategyproof means that f is manipulable with probability at most δ. This means that if

$$\sum_{i=1}^{n} M_i(f) \leq \delta$$

then f is $16m^8\delta$-near to dictatorship. If we let $\epsilon = 16m^8\delta$ then we get that

$$\sum_{i=1}^{n} M_i(f) \leq \frac{\epsilon}{16m^8}$$

implies f is ϵ-near to dictatorship. Or that

$$\sum_{i=1}^{n} M_i(f) \geq \frac{\epsilon}{16m^8}$$

implies f is ϵ-far from dictatorship. And since $\delta < \frac{1}{32m^9}$, we have $\epsilon < \frac{1}{2m}$. So we can reword their theorem as follows.

Theorem 4.3.2 (Dobzinski and Procaccia reworded)**.** *Let f be a Pareto-optimal SCF and let $n = 2$, $m \geq 3$, and $\epsilon < \frac{1}{2m}$. If $\sum_{i=1}^{n} M_i(f) \geq \frac{\epsilon}{16m^8}$ then f is ϵ-far from dictatorship.*

The limitation of these results to two voters makes them unsuitable for application to political elections because any political election with only two voters seems meaningless. However, Dobzinski and Procaccia point out that even without extending these results there are some social choice situations which have only two voters but many alternatives—and these results are more interesting as the number of alternatives becomes very large. One example of this would be a couple deciding where to eat dinner. There are only two "voters," but there can be a huge number of alternatives to choose from. This kind of situation can also occur among artificial intelligence agents deciding among a vast number of alternatives.

4.4 The geometry of manipulation: A quantitative proof of the Gibbard-Satterthwaite theorem

In 2010 Isaksson, Kindler, and Mossel published a brilliant generalization of the original theorem of Friedgut, Kalai, and Nisan and even improved slightly upon the results [IKM10]. Translating their results into the terminology we have been using, they proved that for a neutral social choice function f with $m \geq 4$ alternatives and n voters that is ϵ-far from dictatorship, a uniformly chosen profile will be manipulable with probability at least $2^{-1}\epsilon^2 n^{-4} m^{-6} (m!)^{-3}$. In other words

$$\sum_{i=1}^{n} M_i(f) \geq \frac{\epsilon^2}{2n^4 m^6 (m!)^3}.$$

This bound allows the manipulating voter to randomly permute his entire preference list, which is the case considered by Friedgut, Kalai, and Nisan. However if we restrict him to permuting only four adjacent alternatives, Isaksson, Kindler, and Mossel showed that the bound becomes polynomial in the number of alternatives:

$$\sum_{i=1}^{n} M_i(f) \geq \frac{\epsilon^2}{10^4 n^3 m^{30}}.$$

Isaksson, Kindler, and Mossel used purely geometric and combinatorial methods to achieve their results. One of the foundational techniques they employed was the canonical path method [JS93]. Given a graph G, the canonical path method attempts to give a lower bound on the 'surface area' of a subset of vertices, A. Surface area is defined as the number of vertices in A which have an edge to at least one vertex outside of A. Given two vertices x, y such that $x \in A$ and $y \notin A$, we call the path between them the canonical path, and clearly this path must contain at least one surface vertex. Then by proving that each surface vertex lies on at most r canonical paths, we bound the surface area of A below by $\frac{|A||\overline{A}|}{r}$ because the total number of total canonical paths is $|A||\overline{A}|$.

The graph used by Isaksson, Kindler, and Mossel is very similar to the one used by Friedgut, Kalai, and Nisan. It is also similar to the one used for the results in this thesis, except that ours is directed, and is missing certain edges.

Next we define the boundary of f with respect to alternatives a, b as

$$B_i^{a,b}(f) = \{(x, x') \mid f(x) = a, f(x') = b, \forall j \neq i : x_j = x'_j\}.$$

For any distinct alternatives a, b, c, d we construct canonical paths between $B_i^{a,b}$ and $B_j^{c,d}$ such that each path passes through a manipulation point. These paths are called manipulation paths.

We define manipulation paths between pairs of profiles in $B_i^{a,b}$ and $B_j^{c,d}$. In the first half of the path we will preserve the order or a, b, while in the second half of the path we will only modify the order of a, b and not any other alternatives. The length of the manipulation path will be $2n - 3$ because we are not modifying the last two indices. For any pair of profiles $(x, x') \in B_i^{a,b}$ and $(z, z') \in B_j^{c,d}$ we formally define the manipulation path as follows. The manipulation path is of the form:

$$(x^{(0)}, x'^{(0)}), \ldots, (x^{(n-2)}, x'^{(n-2)}), (z^{(n-2)}, z'^{(n-2)}), \ldots, (z^{(0)}, z'^{(0)})$$

such that $(x^{(0)}, x'^{(0)}) = (x, x')$ and $(z^{(0)}, z'^{(0)}) = (z, z')$. For all $k \in \{0, \ldots, n-2\}$, and all $s \in \{0, \ldots, n-2\}$ such that $s \neq k$ we restrict the path so that:

$$(x_s^{(k)}, x_s'^{(k)}) = (x_s^{(k-1)}, x_s'^{(k-1)}) \tag{4.1}$$

$$(z_s^{(k)}, z_s'^{(k)}) = (z_s^{(k-1)}, z_s'^{(k-1)}). \tag{4.2}$$

Now at the kth step we update the kth index to have the same ordering of a, b as $(x_k^{(0)}, x_k'^{(0)})$ and the same ordering of all other alternatives as $(z_k^{(0)}, z_k'^{(0)})$:

$$(x_k^{(0)}, x_k'^{(0)}) =_{\{a,b\}} (x_k^{(k)}, x_k'^{(k)}) =_{\overline{\{a,b\}}} (z_k^{(0)}, z_k'^{(0)}) \tag{4.3}$$

$$(x_k^{(0)}, x_k'^{(0)}) =_{\{a,b\}} (z_k^{(k)}, z_k'^{(k)}) =_{\overline{\{a,b\}}} (z_k^{(0)}, z_k'^{(0)}). \tag{4.4}$$

Note that by the pairwise notation for defining a path: $(x^{(0)}, x'^{(0)}), (x^{(1)}, x'^{(1)})$, we mean that we have two paths of equal length: $x^{(0)}, x^{(1)}$ and $x'^{(0)}, x'^{(1)}$. Additionally, by the notation $x_k =_D z_k$ we mean that the preference lists x_k and z_k have the same ordering for every alternative in the set D (see Definition 2.1.23).

We will perform a small example to illustrate how the above rules work together in forming the manipulation path. We use $n = 4$ voters which means we will have a manipulation path of length $2n - 3 = 5$. Here, for simplicity, we show only x and z but the example for x' and z' is exactly the same.

step	0	1	2	2	1	0
1st index	x_1	y_1	y_1	y_1	y_1	z_1
2nd index	x_2	x_2	y_2	y_2	z_2	z_2
3rd index	x_3	x_3	x_3	z_3	z_3	z_3
4th index	x_4	x_4	x_4	z_4	z_4	z_4

Here y_i for $i \in \{1, 2, 3, 4\}$ represents the result of Equation 4.3 (or 4.4 depending on whether it's on the x side or the z side). Therefore y_i can be defined as

$$x_i =_{\{a,b\}} y_i =_{\overline{\{a,b\}}} z_i$$

or in other words we get y_i by taking z_i and swapping a, b if necessary to ensure that their order is the same as in x_i. A visual representation of this example, with arbitrarily chosen preference lists, is illustrated in Figure 4.1.

We will now go through the example table step by step for the x side (left half); the z side is simply a mirror image of what happens in the x side. At step 0 we have $x^{(0)} = x$ because we specified above that our initial value was $(x^{(0)}, x'^{(0)}) = (x, x')$. At step 1 we first use Equation 4.1 to essentially copy over every index from step 0 except index 1 (because it is the kth index during this step). We then apply Equation 4.3 to index 1 to get y_1. At step 2 we again use Equation 4.1 to copy over every index from step 1 except for index 2 for which we use Equation 4.3 to get y_2. We don't modify the last two indices because these are the only ones on which x, x' and z, z' differ: recall that $(x, x') \in B_{n-1}^{a,b}$ and $(z, z') \in B_n^{c,d}$.

Lemma 4.4.1 (Lemma 5.1 of Isaksson, Kindler, and Mossel). *For any SCF f, distinct $i, j \in \{1, \ldots, n\}$ and distinct alternatives $a, b, c, d \in C$ there exists a mapping $h : B_i^{a,b}(f) \times B_j^{c,d}(f) \to M$ where*

$$M = \{x \in P \mid f \text{ is manipulable at } x\}$$

such that for any $x \in M$

$$|h^{-1}(x)| \leq 2n(m!)^{n+4}$$

Proof. Without loss of generality, let $i = n - 1$ and $j = n$. We construct a manipulation path between $(x, x') \in B_i^{a,b}(f)$ and $(z, z') \in B_j^{c,d}(f)$. Notice that (x, x') takes the values (a, b) while (z, z') takes the values (c, d) because $f(x) = a$, $f(x') = b$, $f(z) = c$, and $f(z') = d$. Our claim is that along this manipulation path is an edge $((u, u'), (v, v'))$ such that either

1. at least one of u, u', v, v' is a manipulation point

2. f takes on at least three values on the points u, u', v, v'.

In explanation, notice that there are at most three possible situations, and at least one of the above claims holds for each:

- On the first half of the path the value of the pair changes from (a, b) to something else. If the first value changes to b or the second value changes to a then we have a manipulation point because the ranking of a, b doesn't change on the first half of the path. Otherwise the values change to something other than a or b, so f takes at least three values at this point.

- On the second half of the path the value of the pair changes from (c, d) to something else — moving from the end towards the middle. If the first value changes to d or the second value changes to c then we have a manipulation point because the ranking of c, d doesn't change on the second half of the path. Otherwise the values change to something other than c or d, so f takes at least three values at this point.

- The middle edge $(x^{(n-2)}, x'^{(n-2)}), (z^{(n-2)}, z'^{(n-2)})$ connects a pair with values (a, b) and (c, d). Clearly f takes on at least three values at this point.

Notice that u, u', v, v' agree in all but two indices which will be either $\{n-1, k\}$, $\{n, k\}$, or $\{n-1, n\}$ depending on whether $(u, u'), (v, v')$ is on the first half, on the second half, or is the middle edge of the path respectively. For example, if $(u, u'), (v, v')$ is on the first half of the path u, u' and v, v' will both differ on the $n-1$ index because both pairs are in $B_{n-1}^{a,b}$. Additionally, u, v and u', v' will each differ on k^{th} index because of the definition of the manipulation path.

We claim that there exists a manipulation point $h((x, x'), (z, z')) = y$ which only differs from u, u', v, v' on two indices. If Case 1 above holds, then we can let y be whichever one of u, u', v, v' is a manipulation point.

If Case 2 holds then we apply the Gibbard-Satterthwaite theorem to a restricted version of f, which we will call f', which is f restricted to the two indices on which u, u', v, v' differ. We call these indices k, p. First we define a mapping $g : L(C)^2 \to L(C)^n$ which maps profiles from f' to f.

$$
\begin{aligned}
g(x)_q &= u_q \ \ \forall q \notin \{k, p\} \\
g(x)_k &= x_1 \\
g(x)_p &= x_2.
\end{aligned}
$$

We define the set of alternatives to be C where $|C| = m$ and we define $f' : L(C)^2 \to C$ such that

$$f'(x) = f(g(x)).$$

If we apply the Gibbard-Satterthwaite theorem [Gib73, Sat75] to f' we will see that f' is manipulable since it is not a dictator and it takes on at least 3 values (because Case 2 holds). Therefore some x is a manipulation point for f', so $g(x)$ is a manipulation point of f. And in fact $g(x)$ differs from u, u', v, v' on only two indices so $y = g(x)$.

The final step in the proof is to count the maximum number of pairs that could have lead to the manipulation point y and that will be simply the number of inverses of the mapping function: $|h^{-1}(f)|$. To begin with, we know that the length of the manipulation path between (x, x') and (z, z') is $2n - 3$. This gives us $2n - 3$ possibilities for $(u, u'), (v, v')$. In addition, given y there are at most $(q!)^2$ possibilities for u because it differs from y on at most two indices. We find that there are at most $(q!)^n$ possibilities for x and z as follows. For any $k \in \{1, \ldots, n\}$ we will have either:

- $u_k = x_k$ if u is on the first half of the path and k is an index that hasn't been updated—by update we mean that it has been made to conform to $x_k =_{\{a,b\}} u_k =_{\overline{\{a,b\}}} z_k$. In this case there are $q!$ possibilities for z_k because it can be any preference list.

- $u_k = z_k$ if u is on the second half of the path and k is an index that hasn't been updated. In this case there are $q!$ possibilities for x_k because it can be any preference list.

- $x_k =_{\{a,b\}} u_k =_{\overline{\{a,b\}}} z_k$ if k is an index that has been updated. In this case there are $\frac{q!}{2}$ possibilities for x_k because only the order of a, b needs to match u_k, and there are 2 possibilities for z_k because the order of every alternative besides a, b needs to match u_k.

No matter which of the previous cases hold for each k, the total number of possibilities for x and z is still bounded above by $(q!)^n$.

Lastly, given x and z there are at most $q!$ possibilitites for each of x' and z' respectively, since edges of the border set differ only in one index. Summing these we get:

$$|h^{-1}| \leq (2n - 3)(q!)^2 (q!)^n (q!)(q!)$$
$$|h^{-1}| \leq (2n - 3)(q!)^{n+4}.$$

$\square$

One of the open problems of Friedgut, Kalai, and Nisan was finding a way "to replace the neutrality condition with the weaker 'correct' condition: being far from having a range of size at most 2. [FKN08]" In 2011, Friedgut et al. successfully achieved this themselves with the help of one additional author [FKKN11]. Most of the work required to replace the neutrality condition focuses on the first step of the original theorem, and their results are as follows.

Theorem 4.4.2. *There exist universal constants $C, C' > 0$ such that for every $\epsilon > 0$ and any n the following holds:*

- *If F is an SCF on n voters and three alternatives, such that the distance of F from a dictatorship and from having only two alternatives in its range is at least ϵ, then*

$$\sum_{i=1}^{n} M_i(F) \geq C \cdot \epsilon^6.$$

- *If, in addition, F is neutral (that is, invariant under permutation of the alternatives), then:*

$$\sum_{i=1}^{n} M_i(F) \geq C' \cdot \epsilon^2.$$

Mossel and Rácz [MR11] took ideas from these two proofs and created a unified proof with the same results as Isaksson, Kindler, and Mossel, but without the neutrality constraint. This is a very useful result and is as follows.

Theorem 4.4.3. *Suppose we have $n \geq 1$ voters, $m \geq 3$ alternatives, and a SCF $f : L(C)^n \to C$ satisfying $\mathbf{D}(f, \text{NONMANIP}) \geq \epsilon$. Then*

$$\mathbb{P}(\sigma \in M(f)) \geq \mathbb{P}(\sigma \in M_4(f)) \geq p\left(\epsilon, \frac{1}{n}, \frac{1}{m}\right)$$

for some polynomial p, where $\sigma \in L(C)^n$ is selected uniformly. In particular, we show a lower bound of $\frac{\epsilon^{15}}{10^{39} n^{67} m^{166}}$.
    An immediate consequence is that

$$\mathbb{P}((\sigma, \sigma') \text{ is a manipulation pair for } f) \geq q\left(\epsilon, \frac{1}{n}, \frac{1}{m}\right)$$

for some polynomial q, where $\sigma \in L(C)^n$ is uniformly selected, and σ' is obtained from σ by uniformly selecting a coordinate $i \in \{1, \ldots, n\}$, uniformly selecting $j \in \{1, \ldots, n-3\}$, and then uniformly randomly permuting the following four adjacent alternatives in $\sigma_i : \sigma_i(j), \sigma_i(j+1), \sigma_i(j+2)$, and $\sigma_i(j+3)$. In particular, the specific lower bound for $\mathbb{P}(\sigma \in M_4(f))$ implies that we can take $q\left(\epsilon, \frac{1}{n}, \frac{1}{m}\right) = \frac{\epsilon^{15}}{10^{41} n^{68} m^{167}}$.

Above, the distance between SCFs is defined as in Definition 2.1.26. NONMANIP is defined to be the set of SCFs which are either dictators or take at most two values. Finally, $M(f)$ denotes the set of manipulation points of the SCF f, and for a given r, let $M_r(f)$ denote the set of r-manipulation points of f (we only allow permuting r adjacent alternatives instead of the entire preference list).
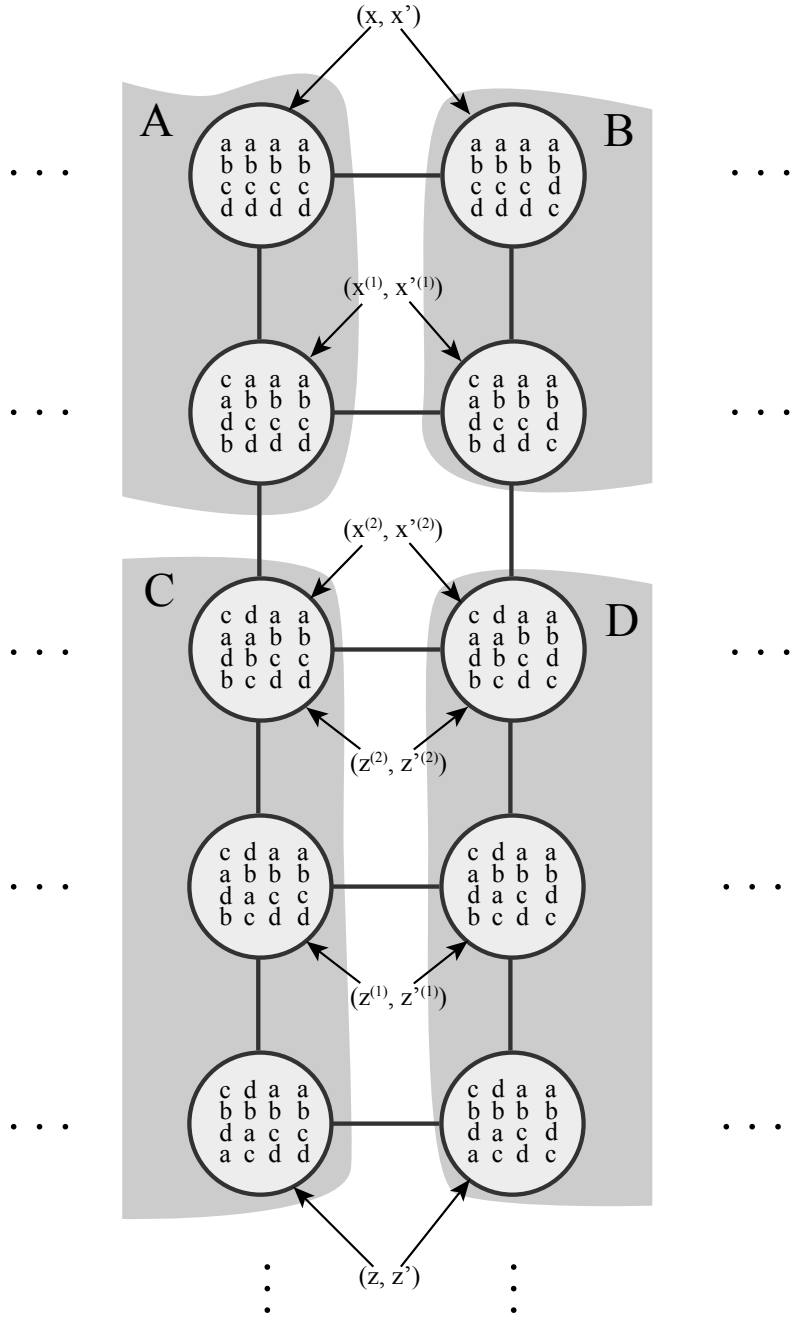
Figure 4.1: A visual example of a manipulation path.

Chapter 5

Results

In this chapter we will attempt to generalize step 3 of Friedgut by way of generalizing Friedgut's Lemma 6, Lemma 7, and Lemma 8. However, we will begin the chapter with some general lattice theory results that we will need later on in the chapter.

5.1 Lattice Theory

We are not aware of any existing proofs of these lemmas, but some of them are fairly elementary and seem to us to be broadly applicable.

First we will prove, in three steps, that our inversion lattice (ordered by $\leq_s$; Definition 2.1.15) remains a lattice when we identify two elements that are adjacent in the order $\leq$ (Definition 2.1.16). Recall from Definition 2.1.9 that in order to be a lattice the join and meet must exist for every pair of elements. Therefore Lemma 5.1.1 proves that the join exists, Lemma 5.1.2 proves that the meet exists (with similar reasoning), and Proposition 5.1.3 combines both lemmas to prove that our structure is indeed still a lattice.

Lemma 5.1.1. *Let $(Y, \leq)$ be a poset and let $X = S(Y)$. Let $(X, \leq_s)$ be as in Definition 2.1.15. Let* Inv *be the inversion binary relation (Definition 2.1.11) over Y, and let $\vee$ and $\vee^{ij}$ denote the join in $(X, \leq_s)$ and $(X^{ij}, \leq_s^{ij})$ (Definition 2.1.16) respectively. Then for any $i, j \in Y$, if i is either a direct successor or a direct predecessor of j according to $\leq$, it holds that for all $x, y \in X^{ij}$:*

$$x \vee y \text{ is defined} \implies x \vee^{ij} y \text{ is defined.}$$

Proof. Choose arbitrary $x, y \in X^{ij}$. Assume $x \vee y$ is defined. Let $z = x \vee y$.

Then z is an upper bound of $\{x, y\}$:

$$z \geq_s x \text{ and } z \geq_s y.$$

And z is the least upper bound of $\{x, y\}$. For every $a \in X$:

$$(a \geq_s x \text{ and } a \geq_s y) \implies z \leq_s a.$$

Since $x \in X^{ij}$, then $(i, j) \notin Inv_x$. Since $z \geq_s x$, then $(i, j) \notin Inv_z$, so $z \in X^{ij}$. By definition $z \geq_s x \implies z \geq_s^{ij} x$ and $z \geq_s y \implies z \geq_s^{ij} y$. Therefore z is an upper bound of $\{x, y\}$ in X^{ij}.

For any $a \in X^{ij}$ if a is an upper bound of $\{x, y\}$ in X^{ij} then clearly a is also an upper bound of $\{x, y\}$ in X. Therefore $z \leq_s a$, so $z \leq_s^{ij} a$, which means $z = x \vee^{ij} y$. So clearly $x \vee^{ij} y$ exists. □

Lemma 5.1.2. *Let Y be an ordered set and let $X = S(Y)$. Let $(X, \leq_s)$ be a lattice with $\leq_s$ defined as above (Definition 2.1.15). Let Inv be the inversion binary relation over Y as defined above (Definition 2.1.11). Let $\wedge$ and $\wedge^{ij}$ denote the meet in $(X, \leq_s)$ and $(X^{ij}, \leq_s^{ij})$ respectively. Then for any $i, j \in Y$, if i is either a direct successor or a direct predecessor of j according to $\leq$, it holds that for all $x, y \in X^{ij}$:*

$$x \wedge y \text{ is defined} \implies x \wedge^{ij} y \text{ is defined.}$$

Proof. Choose arbitrary $x, y \in X^{ij}$. Assume $x \wedge y$ is defined. Let $z = x \wedge y$. Then z is a lower bound of $\{x, y\}$:

$$z \leq_s x \text{ and } z \leq_s y.$$

And z is the greatest lower bound of $\{x, y\}$: for every $a \in X$:

$$(a \leq_s x \text{ and } a \leq_s y) \implies z \geq_s a.$$

We now show that $z \in X^{ij}$. Since $z = x \wedge y$, it holds that $\mathrm{Inv}_z = (\mathrm{Inv}_x \cup \mathrm{Inv}_y)^t$ (Definition 2.1.10, Definition 2.1.15) [Mar94]. Because $x, y \in X^{ij}$ we know that $(i, j) \notin (\mathrm{Inv}_x \cup \mathrm{Inv}_y)$. Therefore, in order to have $(i, j) \in (\mathrm{Inv}_x \cup \mathrm{Inv}_y)^t$ we would need to have

$$(i, k_1), (k_1, k_2), \ldots, (k_{n-1}, k_n), (k_n, j) \in \mathrm{Inv}_x \cup \mathrm{Inv}_y$$

for $n \geq 1$ and $k_1, \ldots, k_n \in Y$. But that is impossible because i is either a direct successor or a direct predecessor of j. Therefore $(i, j) \notin Inv_z$, so $z \in X^{ij}$.

By definition

$$z \leq_s x \text{ and } z \in X^{ij} \implies z \leq_s^{ij} x$$

and

$$z \leq_s y \text{ and } z \in X^{ij} \implies z \leq_s^{ij} y.$$

Therefore z is a lower bound of $\{x, y\}$ in X^{ij}.

For any $a \in X^{ij}$ if a is a lower bound of $\{x, y\}$ in X^{ij} then clearly a is also a lower bound of $\{x, y\}$ in X. Therefore $z \geq_s a$, so $z \geq_s^{ij} a$, which means $z = x \wedge^{ij} y$. So clearly $x \wedge^{ij} y$ is defined. $\square$

Theorem 5.1.3. *Let Y be a set and let $X = S(Y)$. Let $(X, \leq_s)$ be a lattice with $\leq_s$ as in Definition 2.1.15. Let* Inv *be the inversion binary relation over Y as in Definition 2.1.11. Then for any $i, j \in Y$, if i is either a direct successor or a direct predecessor of j according to $\leq_s$, it holds that $(X^{ij}, \leq_s^{ij})$ is a lattice.*

Proof. We know that $x \vee y$ is defined and $x \wedge y$ is defined because $(X, \leq_s)$ is a lattice. Therefore by Lemma 5.1.1 and Lemma 5.1.2 we have $x \vee^{ij} y$ is defined and $x \wedge^{ij} y$ is defined respectively. So $(X^{ij}, \leq_s^{ij})$ is a lattice, by definition of a lattice. $\square$

Now we will show that a cross-product of lattices is also a lattice. For example, suppose we have the lattice in Figure 5.1. The top element is the greatest, and the arrows show the "less than" relationship between elements. Each column of numbers represents a ranking of alternatives $1, 2, 3$ in which we don't care about the relationship between alternative 1 and 2 so we simply replace alternative 2 with 1 in the ranking. All this aside though, this proof is valid for any lattice.

If we were to make that lattice into a 2-dimensional "grid" it would look like Figure 5.2. This would be the case if we only had two voters ($n = 2$).

Proposition 5.1.4. *Let $(X, \leq)$ be a lattice. Let X^n be the set of all n-tuples of elements of X. Let $\leq^n$ be defined as: for all $x, y \in X$*

$$x \leq^n y \iff \forall i \in \{1, \ldots, n\}, x_i \leq y_i.$$

Then $(X^n, \leq^n)$ is a lattice.

Proof. By definition of a lattice, $(X^n, \leq^n)$ is a lattice if for any two elements $s, t \in S^n$, $s \vee t$ is defined and $s \wedge t$ is defined.
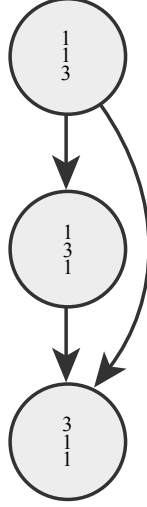
Figure 5.1: A single dimension of lattice.

First, we show that $s \vee t$ is defined. We define $u \in X^n$ such that $u_i = s_i \vee t_i$, $\forall i \in \{1, \ldots, n\}$, and we show that $u = s \vee t$. Because $u_i = s_i \vee t_i$, we have

$$u_i \geq s_i \text{ and } u_i \geq s_i$$

so

$$u \geq^n s \text{ and } u \geq^n t$$

meaning that u is an upper bound for s and t. Suppose there is some $v \in X^n$ which is also an upper bound for s and t. Then $\forall i \in \{1, \ldots, n\}$ we have

$$v_i \geq s_i \text{ and } v_i \geq t_i$$

so since $u_i = s_i \vee t_i$, then $u_i \leq v_i$. Therefore $u \leq^n v$, i.e. u is the least upper bound of $\{s, t\}$.

Second, it follows by analogy to the above proof for $s \vee t$, that $s \wedge t$ is defined. Therefore, $s \vee t$ is defined and $s \wedge t$ is defined, so $(X^n, \leq^n)$ is a lattice. □

5.2   Main Theorem

Hereafter, since we refer very often to [FKN08], instead of saying for example "Lemma 2 of Friedgut, Kalai, and Nisan" we will often shorten it to "Lemma
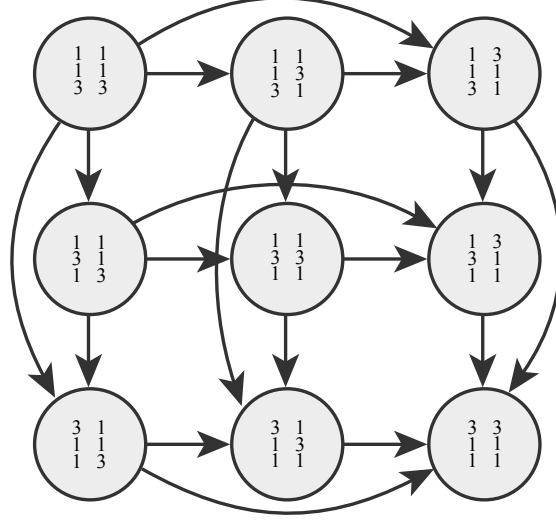
Figure 5.2: A 2-dimensional version of the lattice from Figure 5.1.

2 of Friedgut".

Friedgut, Kalai, and Nisan's main theorem is proved in three steps; the first two are already general, and hold for any $n, m \in N^+$. Therefore, to generalize the main theorem we need only generalize the third step, and therefore this third step is our main theorem. This step is comprised of Lemma 6, Lemma 7, and Lemma 8 which we will generalize one at a time. The lemma we will generalize is:

Lemma 5.2.1 (Lemma 3 of Friedgut). *For every SCF f on 3 alternatives and every $a, b \in A$,*

$$M^{a,b} \leq \sum_i M_i \cdot 6$$

Which we will generalize as:

Theorem 5.2.2 (Main Theorem). *For every SCF f on m alternatives and every $a, b \in C$:*

$$M^{a,b}(f) \leq m! \cdot \sum_i M_i(f)$$

For the rest of the proof we will fix a SCF, f, and two alternatives $a, b \in C$.

5.3   Generalized Lemma 6 of Friedgut

For any preference profile $p \in P$ there are $(\frac{m!}{2})^n$ profiles x such that $x|_{\{a,b\}} = p|_{\{a,b\}}$. This is because there are $m!$ possible preference lists; half of them will have the preference between a and b that agrees with $p|_{\{a,b\}}$ and half will disagree. This gives $\frac{m!}{2}$ possible preference lists for each voter, so there are $(\frac{m!}{2})^n$ profiles comprised of these preference lists.

Definition 5.3.1. Let $a, b \in C$ be the first two alternatives, let $p \in L(C)^n$ be a preference profile, and let $X \subseteq L(C)^n$. We define

$$A(p, X) = \{x \in X \mid x|_{\{a,b\}} = p|_{\{a,b\}}, f(x) = a\}$$
$$B(p, X) = \{x \in X \mid x|_{\{a,b\}} = p|_{\{a,b\}}, f(x) = b\}.$$

When we do not explicitly specify X we assume $X = L(C)^n$:

$$A(p) = A(p, L(C)^n)$$
$$B(p) = B(p, L(C)^n).$$

Before we state Lemma 5.3.2, recall the definition of $M^{a,b}(f)$ from Friedgut [FKN08]:

$$M^{a,b}(f) = \mathrm{P}(f(p) = a, f(p') = b)$$

where p, p' are chosen at random in $L(C)^n$ with $p|_{\{a,b\}} = p'|_{\{a,b\}}$.

Therefore we can rewrite $M^{a,b}(f)$ as follows.

Lemma 5.3.2 (See Lemma 6 of Friedgut)**.**

$$M^{a,b}(f) = E_{q \in L(C)^n} \left[\frac{|A(q)|}{\left(\frac{m!}{2}\right)^n} \cdot \frac{|B(q)|}{\left(\frac{m!}{2}\right)^n} \right],$$

where q is chosen uniformly at random.

Proof. First we fix a profile q. Then

$$\frac{|A(q)|}{\left(\frac{m!}{2}\right)^n}$$

is the probability that a randomly chosen profile, p, satisfying $p|_{\{a,b\}} = q|_{\{a,b\}}$ also satisfies $f(p) = a$. This is because there are $(\frac{m!}{2})^n$ profiles that agree with $q|_{\{a,b\}}$, and $|A(q)|$ is the number of those for which the outcome is a.

Likewise,
$$\frac{|B(q)|}{\left(\frac{m!}{2}\right)^n}$$
is the probability that a randomly chosen profile, p', satisfying $p'|_{\{a,b\}} = q|_{\{a,b\}}$ also satisfies $f(p') = b$.

Since $p|_{\{a,b\}} = q|_{\{a,b\}}$ and $p'|_{\{a,b\}} = q|_{\{a,b\}}$, clearly we have that $p|_{\{a,b\}} = p'|_{\{a,b\}}$. Since $f(p) = a$ and $f(p') = b$ are independent events, the joint probability is
$$\frac{|A(q)|}{\left(\frac{m!}{2}\right)^n} \cdot \frac{|B(q)|}{\left(\frac{m!}{2}\right)^n}.$$

$\square$

5.4   Generalized Lemma 7 of Friedgut

We now attempt to relate $M_i(f)$ to A and B.

Recall the ordering, $\leq_s$, which was defined in Definition 2.1.15. We know that $(L(C), \leq_s)$ is a lattice by the following. First, $L(C)$ is the set of all total orderings of C, which is isomorphic to the set of all permutations of C. Second, $\leq_s$ is the weak Bruhat order (also known as the weak order of permutations). The weak Bruhat order applied to the set of all permutations is a lattice [Bjö84], so $(L(C), \leq_s)$ is a lattice. This is useful to note now, and will be invoked to help prove Lemma 5.5.4.

We have defined $(L(C), \leq_s)$ to be a lattice, but for the following definition, and for later in the chapter we will treat it as a graph with $L(C)$ being the set of vertices, and $\leq_s$ being the set of edges, oriented so that edges go from greater nodes to lesser nodes.

Definition 5.4.1. Let $p \in L(C)^n$. We define the *upper edge border* of $A(p)$, denoted $\partial A(p)$, to be the set of directed edges whose tail is in $A(p)$ and whose head is not in $A(p)$. We will use the notation (x_{-i}, x_i, x_i') as a shorthand to denote the edge $((x_{-i}, x_i), (x_{-i}, x_i'))$. Formally, for all $i \in \{1, \ldots, n\}$:

$$\partial_i A(p) = \{(x_{-i}, x_i, x_i') \mid (x_{-i}, x_i) \in A(p),$$
$$(x_{-i}, x_i') \notin A(p),$$
$$x_i|_{\{a,b\}} = x_i'|_{\{a,b\}},$$
$$x_i <_s x_i'\}$$

and

$$\partial A(p) = \bigcup_j \partial_j A(p)$$

We define the upper edge border of $B(p)$ analogously.

Before we continue we will prove a preliminary lemma that we will use later in our proof. This lemma will show that each edge in $(x_{-i}, x_i, x_i') \in \partial_i A(p) \cup \partial_i B(p)$ corresponds to a successful manipulation.

Lemma 5.4.2. *Let $p \in L(C)^n$, and let $i \in \{1, \ldots, n\}$. Then each $(x_{-i}, x_i, x_i') \in \partial_i A(p) \cup \partial_i B(p)$ corresponds to at least one successful manipulation.*

Proof. By definition of the upper edge border we have

$$x_i <_s x_i' \text{ and}$$
$$x_i|_{\{a,b\}} = x_i'|_{\{a,b\}}.$$

For $(x_{-i}, x_i, x_i') \in \partial_i A(p)$, we know that $f((x_{-i}, x_i)) = a$ and $f((x_{-i}, x_i')) = t$ for $t \in C \backslash \{a\}$. If $t \succ_{x_i} a$ then x_i' is a successful manipulation of (x_{-i}, x_i). Otherwise, $a \succ_{x_i} t$. If this is the case, then we know that $(a, t) \notin Inv_{x_i}$, and because $x_i <_s x_i'$ we have $(a, t) \notin Inv_{x_i'}$, which means $a \succ_{x_i'} t$. Therefore x_i is a successful manipulation of (x_{-i}, x_i').

And analogously for $(x_{-i}, x_i, x_i') \in \partial_i B(p)$, either x_i' is a successful manipulation of (x_{-i}, x_i) or x_i is a successful manipulation of (x_{-i}, x_i').   □

We now generalize Lemma 7 of Friedgut, Kalait, and Nisan. Their original lemma is:

Lemma 5.4.3 (See Lemma 7 of Friedgut)**.**

$$M_i(f) \geq \frac{1}{6} 3^{-n} E_x \left[|\partial_i A(p)| + |\partial_i B(p)| \right]$$

This lemma relates $M_i(f)$ to the upper edge border defined above, and we generalize it as follows.

Lemma 5.4.4.

$$M_i(f) \geq \frac{1}{m!} \left(\frac{m!}{2} \right)^{-n} E_x \left[|\partial_i A(p)| + |\partial_i B(p)| \right]$$

Proof. First, recall the definition of $M_i(f)$: given a profile $p \in P$ and a vote $p_i' \in L(C)$ chosen uniformly at random, $M_i(f)$ is the probability that p_i' is a successful manipulation of p by voter i. Therefore to lower bound $M_i(f)$ we start with p and p_i' chosen uniformly at random. We can think of these as two distinct profiles, p and p', where $p' = (p_{-i}, p_i')$.

Clearly $p_{-i}|_{\{a,b\}} = p'_{-i}|_{\{a,b\}}$, but we will have $p_i|_{\{a,b\}} = p'_i|_{\{a,b\}}$ only with probability $\frac{1}{2}$, and we condition the following on this being the case. So we assume that $p|_{\{a,b\}} = p'|_{\{a,b\}}$.

By Lemma 5.4.2, each $(x_{-i}, x_i, x'_i) \in (\partial_i A(p) \cup \partial_i B(p))$ corresponds to at least one successful manipulation. Note that if $(x_{-i}, x_i, x'_i) \in \partial_i A(p)$ then $(x_{-i}, x'_i, x_i) \notin \partial_i A(p)$.

Therefore we can lower bound the probability that p, p' is a manipulation, i.e. $M_i(f)$, by the probability that an edge is in $\partial_i A(p) \cup \partial_i B(p)$.

The total number of possible edges of the form (x_{-i}, x_i, x'_i) is

$$(m!)^{n-1} \cdot m! \cdot m!$$

but all edges in $\partial_i A(p) \cup \partial_i B(p)$ must agree with $p|_{\{a,b\}}$. The total number of possible edges agreeing with $p|_{\{a,b\}}$ is

$$\left(\frac{m!}{2}\right)^{n-1} \cdot \frac{m!}{2} \cdot \frac{m!}{2} = \frac{m!}{2}\left(\frac{m!}{2}\right)^n.$$

Since $\partial_i A(p)$ and $\partial_i B(p)$ are disjoint, no edge can be in both sets and so we have

$$|\partial_i A(p) \cup \partial_i B(p)| \leq \frac{m!}{2}\left(\frac{m!}{2}\right)^n.$$

Therefore, the probability that a randomly chosen edge is in either $\partial_i A(p)$ or $\partial_i B(p)$ is

$$\frac{2}{m!}\left(\frac{2}{m!}\right)^n \cdot E\left[|\partial_i A(p)| + |\partial_i B(p)|\right]$$

Note that we can sum the probabilities for $\partial_i A(p)$ and $\partial_i B(p)$ because they are disjoint by the definition of the upper edge border; an edge cannot satisfy both $(x_{-i}, x_i) \in A(p)$ and $(x_{-i}, x_i) \in B(p)$ simultaneously because if $f((x_{-i}, x_i)) = a$ then $f((x_{-i}, x_i)) \neq b$ and vice versa.

We conditioned our analysis on $p_{-i}|_{\{a,b\}} = p'_{-i}|_{\{a,b\}}$, so our lower bound becomes

$$M_i(f) \geq \frac{1}{2} \cdot \frac{2}{m!}\left(\frac{2}{m!}\right)^n \cdot E\left[|\partial_i A(p)| + |\partial_i B(p)|\right].$$

After simplifying, we have

$$M_i(f) \geq \frac{1}{m!}\left(\frac{2}{m!}\right)^n \cdot E\left[|\partial_i A(p)| + |\partial_i B(p)|\right].$$

$\square$

Summing over i we get the following corollary.

Corollary 5.4.5 (See Corollary 1 of Friedgut)**.**

$$\frac{1}{m!} \cdot \left(\frac{m!}{2}\right)^{-n} E_p[|\partial A(p)| + |\partial B(p)|] \leq \sum_i M_i(f)$$

5.5 Generalized Lemma 8 of Friedgut

In this section we will fix a profile p, and for the sake of readability we use the following shorthand notation:

$$\leq^n \equiv (\leq_s)^n$$
$$A \equiv A(p)$$
$$B \equiv B(p)$$
$$A(X) \equiv A(p, X)$$
$$B(X) \equiv B(p, X).$$

We also recall that $(L(C)^n, \leq^n)$ is our n-dimensional lattice as defined in Proposition 5.1.4, and that A and B reside in this space:

$$A \subseteq L(C)^n$$
$$B \subseteq L(C)^n$$

We now generalize Lemma 8 of Friedgut, Kalait, and Nisan. Their original lemma is:

Lemma 5.5.1 (See Lemma 8 of Freidgut)**.** *For every disjoint A, B we have that*

$$|\partial A| + |\partial B| \geq \left(\frac{1}{3}\right)^n |A| \cdot |B|$$

Our generalization of the above lemma is Lemma 5.5.4, but we must do a little bit of setup before we are ready to prove it. First we define an algorithm to consolidate A into A'. We define A' to be a consolidation of A in Algorithm 5.5.1.

Note that since we are dealing with a lattice, the max function in Algorithm 5.5.1 can yield multiple results. In this case we assume that one result is chosen at random.

Algorithm 5.5.1 Consolidate A'

$A' \leftarrow A$
for $i = 1 \rightarrow n$ **do**
    for $d \in L(C)^n$ **do**
        $D \leftarrow \{x \in L(C)^n \mid x_{-i} = d_{-i}\}$
        $F \leftarrow D \cap A'$
        for $a \in F$ **do**
            $a' \leftarrow \max_{\leq^n}(D \backslash A')$
            $A' \leftarrow (A' \backslash \{a\}) \cup \{a'\}$ $\triangleright$ replace a with a'
        end for
    end for
end for

Figure 5.3 gives visual example which may aid in understanding the above algorithm. It shows key steps in the process on a very small two-dimensional example lattice.

We do the same to consolidate B into B'.

One of the goals of this consolidation is to achieve $A' \subseteq B'$ or $B' \subseteq A'$. While the result of this algorithm comes close to satisfying those criteria, it does not hold in all cases; see Open Problem 5.5.2.

Open Problem 5.5.2. *When using the algorithm above, we do not necessarily have $A' \subseteq B'$ or $B' \subseteq A'$. We could modify the algorithm naively so that it satisfies those criteria, but then it would become difficult to prove our second condition:*

$$|A' \backslash A| \leq |\partial A| \ \text{and}$$
$$|B' \backslash B| \leq |\partial B|.$$

Therefore, we leave the modification of this algorithm to achieve $A' \subseteq B'$ or $B' \subseteq A'$ as our first open problem.

We will continue with the proof as if we do have $A' \subseteq B'$ or $B' \subseteq A'$, so that if this problem is resolved then the proof will be complete.

We will now prove the following lemma.

Lemma 5.5.3.

$$|A' \backslash A| \leq |\partial A| \ \text{and}$$
$$|B' \backslash B| \leq |\partial B|$$

Proof. First, we show that for every $a' \in A' \backslash A$, we have an edge in ∂A.

Let $a' \in A' \backslash A$. The above algorithm only adds elements to A' in the innermost for loop, and since that for loop iterates once for every $a \in A(D)$ we know that for every a' we have a corresponding a. Since $a' \in A' \backslash A$, we know that $a \neq a'$. Since $a' \leftarrow \max_{\leq^n}(A(D) \backslash A')$ and $a \neq a'$, we have that $a <^n a'$. According to the algorithm, $a, a' \in D$ which means $a_{-i} = a'_{-i}$. Therefore, $(a_{-i}, a_i, a'_i) \in \partial_i A$ by the definition of $\partial_i A$.

Therefore, every profile in $A' \backslash A$ corresponds to at least one profile in ∂A, so we know that

$$|A' \backslash A| \leq |\partial A|.$$

The same reasoning can be used to show that:

$$|B' \backslash B| \leq |\partial B|.$$

$\square$

And now we are ready to prove the final lemma in this section:

Lemma 5.5.4. *For every disjoint A, B we have that*

$$|\partial A| + |\partial B| \geq \left(\frac{2}{m!}\right)^n |A| \cdot |B|$$

Proof. Since for any two votes $v_1, v_2 \in A \cup B$ we have $v_1|_{\{a,b\}} = v_2|_{\{a,b\}}$ we can define a new set

$$P' = \{x \in P \mid x|_{\{a,b\}} = p|_{\{a,b\}}\}$$

and view A, B, A', and B' as residing in P' without losing any information. This is because, by definition, the elements of these sets agree with $p|_{\{a,b\}}$. Clearly $|P'| = (\frac{m!}{2})^n$.

For any vote $v \in P'$, let $E_{A'}$ be the event that v is in A', and let $E_{B'}$ be the event that v is in B'. Then

$$P(E_{A'} \cap E_{B'}) = P(E_{A'})P(E_{B'}|E_{A'})$$

Clearly

$$P(E_{A'} \cap E_{B'}) = \frac{|A' \cap B'|}{|P'|} \tag{5.1}$$

$$P(E_{A'}) = \frac{|A'|}{|P'|} \tag{5.2}$$

$$P(E_{B'}) = \frac{|B'|}{|P'|} \tag{5.3}$$

Since either $A' \subseteq B'$ or $B' \subseteq A'$, we have

$$P(E_{B'}|E_{A'}) \geq P(E_{B'})$$

Therefore

$$P(E_A \cap E_B) \geq P(E_A)P(E_B)$$

So by substitution from equations 5.1, 5.2, and 5.3 we get

$$\frac{|A' \cap B'|}{(\frac{m!}{2})^n} \geq \frac{|A'|}{(\frac{m!}{2})^n} \frac{|B'|}{(\frac{m!}{2})^n}$$
$$= \frac{|A|}{(\frac{m!}{2})^n} \frac{|B|}{(\frac{m!}{2})^n}$$

However A and B are disjoint so

$$A' \cap B' \subseteq (A'\backslash A) \cup (B'\backslash B)$$

which, along with Lemma 5.5.3, completes the proof as follows

$$|A' \cap B'| \leq |A'\backslash A| + |B'\backslash B|$$
$$|A' \cap B'| \leq |\partial A| + |\partial B|$$
$$\frac{|A||B|}{(\frac{m!}{2})^n} \leq |\partial A| + |\partial B|$$
$$\left(\frac{2}{m!}\right)^n |A| \cdot |B| \leq |\partial A| + |\partial B|$$
$$|\partial A| + |\partial B| \geq \left(\frac{2}{m!}\right)^n |A| \cdot |B|$$

$\square$

5.6 Finished Step 3 of Friedgut

Lemma 6, 7, and 8 fit together as follows. First we define the variables L_6, L_7, and L_8 to be variable values that multiply each of the lemmas respectively. The values of these variables will change depending on the value of m, so we evaluate the lemmas in terms of these variables to be

more general. We can define the lemmas in terms of these variables:

$$M^{a,b} = E[|A||B|] \cdot L_6 \qquad\qquad \text{lemma 6}$$

$$L_7 \cdot E[|\partial A| + |\partial B|] \leq \sum_i M_i \qquad\qquad \text{lemma 7}$$

$$\frac{1}{L_8} \cdot (|\partial A| + |\partial B|) \geq |A||B| \qquad\qquad \text{lemma 8}$$

Now we can solve for the result of step 3.

$$M^{a,b} = E[|A||B|] \cdot L_6 \qquad\qquad \text{by lemma 6}$$

$$M^{a,b} \leq E[|\partial A| + |\partial B|] \cdot \frac{L_6}{L_8} \qquad\qquad \text{by lemma 8}$$

$$M^{a,b} \leq \sum_i M_i \cdot \frac{L_6}{L_7 L_8} \qquad\qquad \text{by lemma 7}$$

If we can fully generalize this step and capture all of the v_i's our results will, possibly, look like this:

$$L_6 = \left(\frac{m!}{2}\right)^{-2n}$$

$$L_7 = \frac{1}{m!} \left(\frac{m!}{2}\right)^{-n}$$

$$L_8 = \left(\frac{m!}{2}\right)^{-n}$$

So we have that

$$\frac{L_6}{L_7 L_8} = \left(\frac{m!}{2}\right)^{-2n} \cdot m! \left(\frac{m!}{2}\right)^{n} \cdot \left(\frac{m!}{2}\right)^{n}$$

$$= \left(\frac{m!}{2}\right)^{-2n} \cdot m! \cdot \left(\frac{m!}{2}\right)^{2n}$$

$$= m!$$

And the final result for step 3 becomes

$$M^{a,b} \leq \sum_i M_i \cdot m!$$

5.7 Main Theorem of Friedgut

Now we can use the Friedgut's generalized steps 1 and 2 along with our generalized version of step 3 to prove a general version of Friedgut's main theorem. We will restate Friedgut's generalized lemmas from step 1 and 2.

Lemma 5.7.1 (Lemma 1 of Friedgut)**.** *For every fixed m and $\epsilon > 0$ there exists $\delta > 0$ such that if $F = f^{\otimes \binom{m}{2}}$ is a neutral IIA GSWF over m alternatives with $f : \{0, 1\}^n \to \{0, 1\}$, and $\Delta(f, DICT) > \epsilon$, then F has probability of at least $\delta \geq (C\epsilon)^{\lfloor m/3 \rfloor}$ of not having a Generalized Condorcet Winner, where $C > 0$ is an absolute constant.*

Lemma 5.7.2 (Lemma 2 of Friedgut)**.** *For every fixed m there exists $\delta > 0$ such that for all $\epsilon > 0$ the following holds. Let f be a neutral SCF among m alternatives such that $\Delta(f, DICT) > \epsilon$. Then for all (a, b) we have $M^{a,b}(f) \geq \delta$.*

And we restate our generalized version of Friedgut's Lemma 3.

Lemma 5.7.3 (Lemma 3 of Friedgut)**.** *For every SCF f on m alternatives and every $a, b \in A$, $M^{a,b} \leq \sum_i M_i \cdot m!$*

With these three lemmas we can now prove a generalized version of Friedgut's main theorem.

Theorem 5.7.4 (Theorem 1 of Friedgut)**.** *There exists a constant $C > 0$ such that for every $\epsilon > 0$ the following holds. If f is a neutral SCF for n voters over 3 alternatives and $\Delta(f, g) > \epsilon$ for any dictatorship g, then f has total manipulatiblity: $\sum_{i=1}^{n} M_i(f) \geq \frac{(C\epsilon)^{\lfloor m/3 \rfloor}}{m!}$.*

Proof. Lemma 5.7.2 gives us

$$M^{a,b}(f) \geq \delta$$

and by substituting the result from Lemma 5.7.1 for δ we get

$$M^{a,b}(f) \geq \delta \geq (C\epsilon)^{\lfloor m/3 \rfloor}$$
$$M^{a,b}(f) \geq (C\epsilon)^{\lfloor m/3 \rfloor}$$

We then relate $M^{a,b}$ to M_i by Lemma 5.7.3

$$\sum_{i=1}^{n} M_i(f) \cdot m! \geq M^{a,b}(f) \geq (C\epsilon)^{\lfloor m/3 \rfloor}$$

$$\sum_{i=1}^{n} M_i(f) \cdot m! \geq (C\epsilon)^{\lfloor m/3 \rfloor}$$

$$\sum_{i=1}^{n} M_i(f) \geq \frac{(C\epsilon)^{\lfloor m/3 \rfloor}}{m!}$$
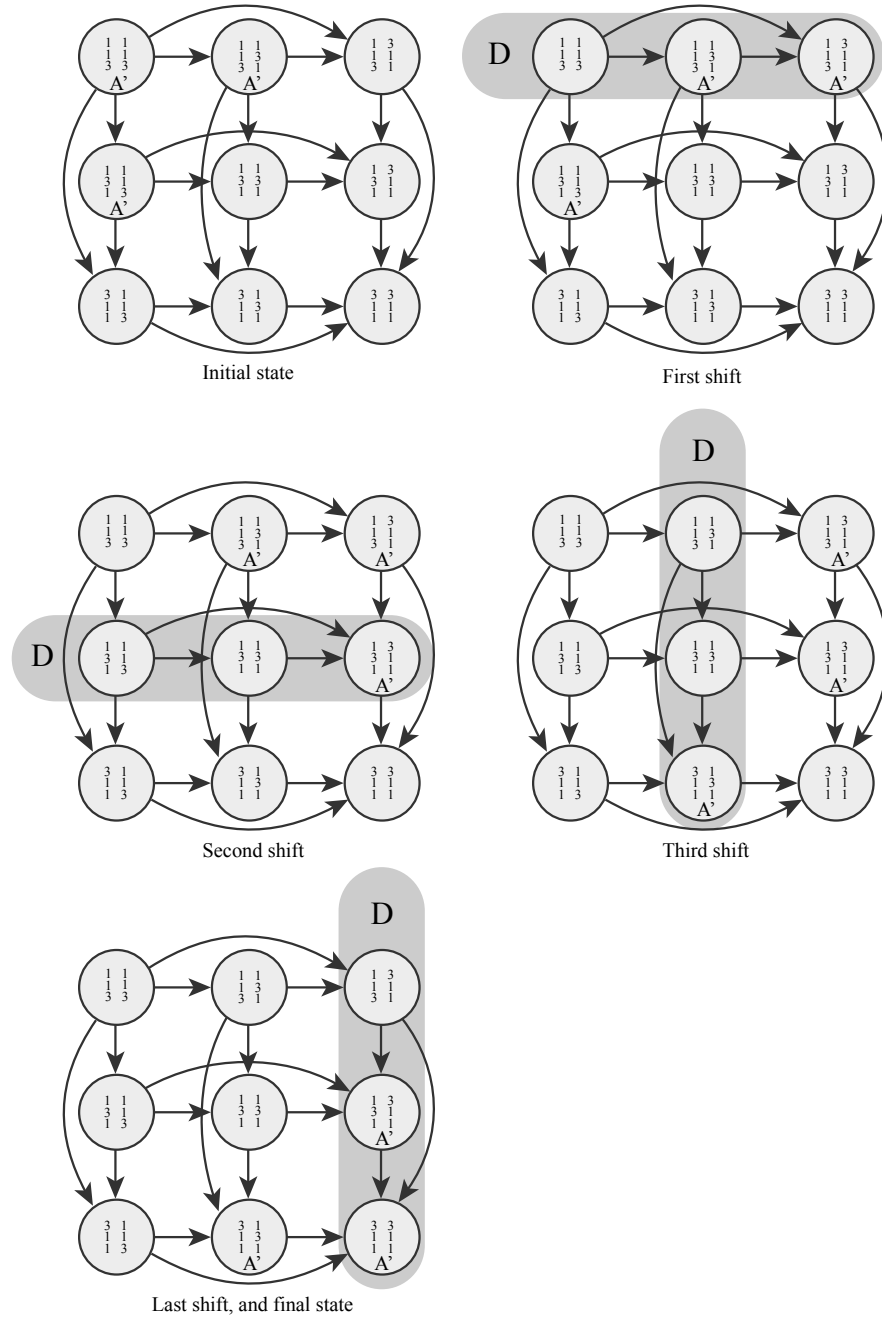
$\square$

Figure 5.3: Example of lattice shifting algorithm.

Chapter 6

Conclusion

We have attempted to prove the following main result in order to extend the results of Friedgut, Kalai, and Nisan in a straightforward manner, and along the same lines of reasoning as the original proof. Our main theorem is

Theorem 6.0.5 (Main Result). *There exists a constant $C > 0$ such that for every $\epsilon > 0$ the following holds. If f is a neutral SCF for n voters over 3 alternatives and $\Delta(f, g) > \epsilon$ for any dictatorship g, then f has total manipulatiblity: $\sum_{i=1}^{n} M_i(f) \geq \frac{(C\epsilon)^{\lfloor m/3 \rfloor}}{m!}$.*

Unfortunately, due to time constraints and unforseen difficulties, we were unable to prove (or disprove) Lemma 5.5.4 because of the problem noted in the attempted proof for that lemma. We conjecture that this can be proven without many changes to our attempted proof, and we leave this as an open problem.

Since our main result relies on Lemma 5.5.4, we have only been able to prove the following two lemmas.

Lemma 6.0.6. *Let C be a set of alternatives. Let $a, b \in C$ be any two alternatives. Let $m = |C|$ and let n be the number of voters. Let f be a SCF. We have*

$$M^{a,b}(f) = E_{p \in L(C)^n} \left[\frac{|A_a^{a,b}(p)|}{\left(\frac{m!}{2}\right)^n} \cdot \frac{|A_b^{a,b}(p)|}{\left(\frac{m!}{2}\right)^n} \right]$$

Lemma 6.0.7.

$$M_i(f) \geq \frac{1}{m!} \left(\frac{m!}{2}\right)^{-n} E_x \left[|\partial_i A_a^{a,b}(p)| + |\partial_i A_b^{a,b}(p)| \right]$$

Even though we were not able to complete the proof of Lemma 5.5.4, we made progress towards that end, and we were able to provide a detailed explanation of the difficulties we ran into. We have also shown that if Lemma 5.5.4 can be proven, then our main result will follow.

6.1 Open Problems

In closing we would like to point out a few potential areas of further research that may follow from this thesis. There are any number of directions that future research can take, but these are some of the most relevant questions that we have omitted, either intentionally or unintentionally, from this work. Therefore, we leave the following open problems.

1. As discussed above, we leave the completion of the proof of Lemma 5.5.4, by resolving Open Problem 5.5.2, open for further investigation.

2. Throughout this thesis we have been concerned only with average-case complexity based on a normal distribution of votes. This is common practice and it is a useful distribution, but in real-world elections the distribution is very rarely a normal distribution, so we leave the task of investigating the impact of a more realistic distribution open for further research.

3. Our bounds are certainly not tight, and neither are the bounds of Mossel and Rácz [MR11]. It would be very useful to find tight bounds, and we leave this as our third open problem.

4. This work deals with a lower bound on average case manipulability, but some subsets of SCFs may be close to this lower bound, while others may be significantly higher. It would be useful to investigate the average case manipulability of certain subsets of SCFs to see how close they are to this generic lower bound. This is one of the open problems stated by Mossel and Rácz [MR11]. We restate it here for emphasis, and leave this as our final open problem.

Bibliography

[Arr50]   K.J. Arrow. A difficulty in the concept of social welfare. *The Journal of Political Economy*, 58(4):328–346, 1950.

[Arr63]   K.J. Arrow. *Social choice and individual values*. Number 12. Yale Univ Pr, 1963.

[Bir67]   G. Birkhoff. Lattice theory. *American Mathematical Society*, 1967.

[Bir95]   G. Birkhoff. *Lattice theory*, volume 25. Amer Mathematical Society, 1995.

[Bjö84]   A. Björner. Orderings of coxeter groups. *Combinatorics and algebra*, 34:175–195, 1984.

[BNM⁺98] D. Black, R.A. Newing, I. McLean, A. McMillan, and B.L. Monroe. *The theory of committees and elections*. Kluwer Academic Pub, 1998.

[BO91]   J.J. Bartholdi and J.B. Orlin. Single transferable vote resists strategic voting. *Social Choice and Welfare*, 8(4):341–354, 1991.

[Bor81]   J.C. Borda. Mémoire sur les élections au scrutin. *Histoire de lacadémie royale des sciences*, 2:85, 1781.

[Bra82]   S.J. Brams. The ams nomination procedure is vulnerable to truncation of preferences. *Notices of the American Mathematical Society*, 29(2):136–138, 1982.

[BTT89a] J. Bartholdi, C.A. Tovey, and M.A. Trick. Voting schemes for which it can be difficult to tell who won the election. *Social Choice and welfare*, 6(2):157–165, 1989.

[BTT89b] J.J. Bartholdi, C.A. Tovey, and M.A. Trick. The computational difficulty of manipulating an election. *Social Choice and Welfare*, 6(3):227–241, 1989.

[CDE⁺06] Y. Chevaleyre, P.E. Dunne, U. Endriss, J. Lang, M. Lemaıtre, N. Maudet, J. Padget, S. Phelps, J.A. Rodrıguez-Aguilar, and P. Sousa. Issues in multiagent resource allocation. *Special Issue: Hot Topics in European Agent Research II Guest Editors: Andrea Omicini*, 30:3–31, 2006.

[CELM07] Y. Chevaleyre, U. Endriss, J. Lang, and N. Maudet. A short introduction to computational social choice. *SOFSEM 2007: Theory and Practice of Computer Science*, pages 51–69, 2007.

[CS02] V. Conitzer and T. Sandholm. Vote elicitation: Complexity and strategy-proofness. In *PROCEEDINGS OF THE NATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE*, pages 392–397. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999, 2002.

[CS03] V. Conitzer and T. Sandholm. Universal voting protocol tweaks to make manipulation hard. *Arxiv preprint cs/0307018*, 2003.

[CS06] V. Conitzer and T. Sandholm. Nonexistence of voting rules that are usually hard to manipulate. In *Proceedings of the National Conference on Artificial Intelligence*, volume 21, page 627. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999, 2006.

[CSL07] V. Conitzer, T. Sandholm, and J. Lang. When are elections with few candidates hard to manipulate? *Journal of the ACM (JACM)*, 54(3):14, 2007.

[dem11] Democracy. *Encyclopedia Britannica*, 2011. Retrived from `http://www.britannica.com/EBchecked/topic/157129/democracy`.

[DK77] G. Doron and R. Kronick. Single transferrable vote: an example of a perverse social choice function. *American Journal of Political Science*, pages 303–311, 1977.

[DKNS01] C. Dwork, R. Kumar, M. Naor, and D. Sivakumar. Rank aggregation methods for the web. In *Proceedings of the 10th inter-*

national conference on World Wide Web, pages 613–622. ACM, 2001.

[Dod76]   C.L. Dodgson. A method of taking votes on more than two issues. *The theory of committees and elections*, pages 222–234, 1876.

[DP08]   S. Dobzinski and A. Procaccia. Frequent manipulability of elections: The case of two voters. *Internet and Network Economics*, pages 653–664, 2008.

[DS00]   J. Duggan and T. Schwartz. Strategic manipulability without resoluteness or shared beliefs: Gibbard-Satterthwaite generalized. *Social Choice and Welfare*, 17(1):85–93, 2000.

[EHRS07]   G. Erdélyi, L. Hemaspaandra, J. Rothe, and H. Spakowski. On approximating optimal weighted lobbying, and frequency of correctness versus average-case polynomial time. In *Fundamentals of Computation Theory*, pages 300–311. Springer, 2007.

[EL05a]   E. Elkind and H. Lipmaa. Hybrid voting protocols and hardness of manipulation. *Algorithms and Computation*, pages 206–215, 2005.

[EL05b]   E. Elkind and H. Lipmaa. Small coalitions cannot manipulate voting. *Financial Cryptography and Data Security*, pages 578–578, 2005.

[ER91]   E. Ephrati and J.S. Rosenschein. The clarke tax as a consensus mechanism among automated agents. In *Proceedings of the Ninth National Conference on Artificial Intelligence*, pages 173–178, 1991.

[ER93]   E. Ephrati and J.S. Rosenschein. Multi-agent planning as a dynamic search for social consensus. In *International Joint Conference on Artificial Intelligence*, volume 13, pages 423–423. Citeseer, 1993.

[FB83]   P.C. Fishburn and S.J. Brams. Paradoxes of preferential voting. *Mathematics Magazine*, 56(4):207–214, 1983.

[FHH06]   P. Faliszewski, E. Hemaspaandra, and L.A. Hemaspaandra. The complexity of bribery in elections. In *PROCEEDINGS OF*

THE NATIONAL CONFERENCE ON ARTIFICIAL INTEL-LIGENCE, volume 21, page 641. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999, 2006.

[FKKN11] E. Friedgut, G. Kalai, N. Keller, and N. Nisan. A quantitative version of the gibbard-satterthwaite theorem for three alternatives. *Arxiv preprint arXiv:1105.5129*, 2011.

[FKN08] E. Friedgut, G. Kalai, and N. Nisan. Elections can be manipulated often. In *IEEE 49th Annual IEEE Symposium on Foundations of Computer Science, 2008. FOCS'08*, pages 243–249, 2008.

[FKS03] R. Fagin, R. Kumar, and D. Sivakumar. Efficient similarity search and classification via rank aggregation. In *Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, pages 301–312. ACM, 2003.

[Gib73] A. Gibbard. Manipulation of voting schemes: a general result. *Econometrica: journal of the Econometric Society*, 41(4):587–601, 1973.

[Hei52] William Heinemann. *Aristotle in 23 Volumes*, volume 20. Harvard University Press, 1952. Translated by H. Rackham.

[HHR07] E. Hemaspaandra, L.A. Hemaspaandra, and J. Rothe. Anyone but him: The complexity of precluding an alternative. *Artificial Intelligence*, 171(5):255–285, 2007.

[HHR09] E. Hemaspaandra, L.A. Hemaspaandra, and J. Rothe. Hybrid elections broaden complexity-theoretic resistance to control. *Mathematical Logic Quarterly*, 55(4):397–424, 2009.

[Hol89] R. Holzman. To vote or not to vote: what is the quota? *Discrete Applied Mathematics*, 22(2):133–141, 1989.

[HP01] G. Hägele and F. Pukelsheim. Llull's writings on electoral systems. *Studia Lulliana*, 41(97):3–38, 2001.

[IKM10] M. Isaksson, G. Kindler, and E. Mossel. The geometry of manipulation: A quantitative proof of the gibbard-satterthwaite theorem. In *Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on*, pages 319–328. IEEE, 2010.

[JS93]   M. Jerrum and A. Sinclair. Polynomial-time approximation algorithms for the ising model. *SIAM Journal on computing*, 22(5):1087–1116, 1993.

[Kun80]   K. Kunen. *Set theory: An introduction to independence proofs*, volume 102. Elsevier Science, 1980.

[lmdCC85]   M. le marquis de Condorcet and A.N. Caritat. Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix. 1785.

[LP98]   R. Lidl and G. Pilz. *Applied abstract algebra*. Springer Verlag, 1998.

[Mar94]   G. Markowsky. Permutation lattices revised. *Mathematical Social Sciences*, 27(1):59–72, 1994.

[Mou88]   H. Moulin. Condorcet's principle implies the no show paradox. *Journal of Economic Theory*, 45(1):53–64, 1988.

[MR11]   E. Mossel and M.Z. Rácz. A quantitative gibbard-satterthwaite theorem without neutrality. *Arxiv preprint arXiv:1110.5888*, 2011.

[OR02]   JJ OConnor and EF Robertson. The history of voting. *Retrived from `http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Voting.html`*, 2002.

[PHG00]   D.M. Pennock, E. Horvitz, and C.L. Giles. Social choice theory and recommender systems: Analysis of the axiomatic foundations of collaborative filtering. In *PROCEEDINGS OF THE NATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE*, pages 729–734. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999, 2000.

[PR06]   A.D. Procaccia and J.S. Rosenschein. Junta distributions and the average-case complexity of manipulating elections. In *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*, pages 497–504. ACM, 2006.

[PR07]   A.D. Procaccia and J.S. Rosenschein. Average-case tractability of manipulation in voting via the fraction of manipulators. In *Proc. AAMAS*, volume 7, 2007.

[PRZ07]   A.D. Procaccia, J.S. Rosenschein, and A. Zohar. Multi-winner elections: Complexity of manipulation, control and winner-determination. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI)*, pages 1476–1481, 2007.

[Sat75]   M.A. Satterthwaite. Strategy-proofness and Arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions* 1. *Journal of Economic Theory*, 10(2):187–217, 1975.

[Sho08]   D.M. Shockey. A comparative study of the robustness of voting systems under various models of noise. Master's thesis, ROCHESTER INSTITUTE OF TECHNOLOGY, 2008.

[XC08]   L. Xia and V. Conitzer. A sufficient condition for voting rules to be frequently manipulable. In *Proceedings of the 9th ACM Conference on Electronic Commerce*, pages 99–108. ACM, 2008.