A Parameterized Perspective on Protecting Elections

Palash Dey\(^1\), Neeldhara Misra\(^2\), Swaprava Nath\(^3\) and Garima Shakya\(^3\)

\(^1\)Indian Institute of Technology, Kharagpur, India
\(^2\)Indian Institute of Technology, Gandhinagar, India
\(^3\)Indian Institute of Technology, Kanpur, India

palash.dey@cse.iitkgp.ac.in, neeldhara.m@iitgn.ac.in, \{swaprava, garima\}@cse.iitk.ac.in

Abstract

We study the parameterized complexity of the optimal defense and optimal attack problems in voting. In both the problems, the input is a set of voter groups (every voter group is a set of votes) and two integers \(k_a\) and \(k_d\) corresponding to respectively the number of voter groups the attacker can attack and the number of voter groups the defender can defend. A voter group gets removed from the election if it is attacked but not defended. In the optimal defense problem, we want to know if it is possible for the defender to commit to a strategy of defending at most \(k_d\) voter groups such that, no matter which \(k_d\) voter groups the attacker attacks, the outcome of the election does not change. In the optimal attack problem, we want to know if it is possible for the attacker to commit to a strategy of attacking \(k_a\) voter groups such that, no matter which \(k_a\) voter groups the defender defends, the outcome of the election is always different from the original (without any attack) one. We show that both the optimal defense problem and the optimal attack problem are computationally intractable for every scoring rule and the Condorcet voting rule even when we have only 3 candidates. We also show that the optimal defense problem for every scoring rule and the Condorcet voting rule is \(W[2]\)-hard for both the parameters \(k_a\) and \(k_d\), while it admits a fixed parameter tractable algorithm parameterized by the combined parameter \((k_a, k_d)\). The optimal attack problem for every scoring rule and the Condorcet voting rule turns out to be much harder – it is \(W[1]\)-hard even for the combined parameter \((k_a, k_d)\). We propose two greedy algorithms for the \textsc{Optimal Defense} problem and empirically show that they perform effectively on reasonable voting profiles.

1 Introduction

The problem of election control asks if it is possible for an external agent, usually with a fixed set of resources, to influence the outcome of the election by altering its structure in some limited way. There are several specific manifestations of this problem: for instance, one may ask if it is possible to change the winner by deleting \(k\) voter groups, presumably by destroying ballot boxes or rigging electronically submitted votes. Indeed, several cases of violence at the ballot boxes have been placed on record [Bhattacharjya, 2010; RT, 2013], and in 2010, Halderman and his students exposed serious vulnerabilities in the electronic voting systems that are in widespread use in several states [Hal, 2010]. A substantial amount of the debates around the recently concluded presidential elections in the United States revolved around issues of potential fraud, with people voting multiple times, stuffing ballot boxes, etc., all of which are well recognized forms of election control. For example, [Wolchok et al., 2012] studied security aspects on Internet voting systems.

The study of controlling elections is fundamental to computational social choice: it is widely studied from a theoretical perspective, and has deep practical impact. The pioneering work of [Bartholdi et al., 1992] initiated the study of these problems from a computational perspective, hoping that computational hardness of these problems may suggest a substantial barrier to the phenomena of control: if it is, say \(NP\)-hard to control an election, then the manipulative agent may not be able to compute an optimal control strategy in a reasonable amount of time. This basic approach has been intensely studied in various other scenarios [Faliszewski et al., 2011; Mattei et al., 2014; Dey, 2018; Dey et al., 2018; 2017; Dey and Misra, 2017; Dey et al., 2015; Dey, 2019].

Exploring parameterized complexity of various control problems has also gained a lot of interest. For example, [Betzler and Uhlmann, 2009] studied parameterized complexity of candidate control in elections and showed interesting connection with digraph problems. [Liu and Zhu, 2010; 2013] studied parameterized complexity of control problem by deleting voters for many common voting rules, and so on [Dey et al., 2016; 2019a]. Studying election control from a game theoretic approach using security games is also an active area of research. See, for example, the works of [An et al., 2013; Letchford et al., 2009].

The broad theme of using computational hardness as a barrier to control has two distinct limitations: one is, of course, that some voting rules simply remain computationally vulnerable to many forms of control, in the sense that optimal strategies can be found in polynomial time. The other is that even \(NP\)-hard control problems often admit reasonable heuristics, can be approximated well, or even admit efficient
exact algorithms in realistic scenarios. Therefore, relying on
NP-hardness alone is arguably not a robust strategy against
control. To address this issue, the work of [Yin et al., 2016]
explicitly defined the problem of protecting an election from
control, where in addition to the manipulative agent, we also
have a “defender”, who can also deploy some resources to
spoil a planned attack. In this setting, elections are defined
with respect to voter groups rather than voters, which is a
small difference from the traditional control setting. The
voter groups model allows us to consider attacks on sets of
voters, which is a more accurate model of realistic control
scenarios.

In [Yin et al., 2016], the defense problem is modeled as a
Stackelberg game in which limited protection resources (say
$k_d$) are deployed to protect a collection of voter groups and
the adversary responds by attempting to subvert the election
(by attacking, say, at most $k_a$ groups). They consider the
plurality voting rule, and show that the problem of choosing
the minimal set of resources that guarantee that an election
cannot be controlled is NP-hard. They further suggest a
Mixed-Integer Program formulation that can usually be effi-
ciently tackled by solvers. Our main contribution is to study
this problem in a parameterized setting and provide a refined
complexity landscape for it. We also introduce the comple-
mentary attack problem, and extend the study to voting rules
beyond plurality. We now turn to a summary of our contribu-
tions.

1.1 Contribution

We refer the reader to Section 2 for the relevant formal defi-
ditions, while focusing here on a high-level overview of our results. Recall that the OPTIMAL DEFENSE problem asks for a
set of at most $k_d$ voter groups which, when protected, render
any attack on at most $k_a$ voter groups unsuccessful. In this
paper, we study the parameterized complexity of OPTIMAL
DEFENSE for all scoring rules and the Condorcet voting rule
(these are natural choices because they are computationally
vulnerable to control — the underlying “attack problem” can be
resolved in polynomial time). We show that the problem of
finding an optimal defense is tractable when both the at-
tacker and the defender have limited resources. Specifically,
we show that the problem is fixed-parameter tractable with
the combined parameter $(k_a, k_d)$ by a natural bounded-depth
search tree approach. We also show that the OPTIMAL DE-
FENSE problem is unlikely to admit a polynomial kernel un-
der plausible complexity theoretic assumption. We observe
that both these parameters are needed for fixed parameter
tractability, as we show $W[2]$-hardness when OPTIMAL DE-
FENSE is parameterized by either $k_a$ or $k_d$.

Another popular parameter considered for voting problems
is $m$, the number of candidates — as this is usually small
compared to the size of the election in traditional applica-
tion scenarios. Unfortunately, we show that OPTIMAL DE-
FENSE is NP-hard even when the election has only 3 can-
didates, eliminating the possibility of fixed-parameter algo-
rithms (and even XP algorithms). This strengthens a hardness
result shown in [Yin et al., 2016]. Our hardness results on a
constant number of candidates rely on a succinct encoding of
the information about the scores of the candidates from each
erector group. We also observe that the problem is polynomi-
solvable when only two candidates are involved.

We introduce the complementary problem of attacking an
election: here the attacker plays her strategy first, and the
defender is free to defend any of the attacked groups within
the budget. The attacker wins if she is successful in subvert-
ing the election no matter which defense is played out. This
problem turns out to be harder: it is already $W[1]$-hard when
parameterized by both $k_a$ and $k_d$, which is in sharp contrast to
the OPTIMAL DEFENSE problem. This problem is also hard
in the setting of a constant number of candidates — specif-
ically, it is coNP-hard for the plurality voting rule [Corol-
ary 1] and the Condorcet voting rule [Corollary 2] even when
we have only three candidates if every voter group is encoded
as the number of plurality votes every candidate receives from
that voter group. Our demonstration of the hardness of the at-
tack problem is another step in the program of using compu-
tational intractability as a barrier to undesirable phenomenon,
which, in this context, is the act of planning a systematic at-
tack on voter groups with limited resources.

We finally propose two simple greedy algorithms for the
OPTIMAL DEFENSE problem and empirically show that it
may be able to solve many instances of practical interest.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>OPTIMAL DEFENSE</th>
<th>OPTIMAL ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(k_a, k_d)$</td>
<td>$\Omega^*(k_d^m)$ [Theorem 7]</td>
<td>$W[1]$-hard [Theorem 6]</td>
</tr>
<tr>
<td>$m$</td>
<td>para-NP-hard [Corollary 3]</td>
<td>para-coNP-hard [Corollary 3]</td>
</tr>
</tbody>
</table>

Table 1: Summary of parameterized complexity results. $k_d$ : the maximum number of voter groups that the defender can defend. $k_a$ : the maximum number of voter groups that the attacker can attack. $m$ : the number of candidates.
be clear from the context. A voting rule (often called voting correspondence) is a function \( r : \mathbb{N}^n \rightarrow 2^C \setminus \{\emptyset\} \) which selects, from a preference profile, a nonempty set of candidates as the winners. We refer the reader to [Brandt et al., 2016] for a comprehensive introduction to computational social choice. In this paper we will be focusing on two voting rules – the scoring rules and the Condorcet voting rule which are defined as follows.

### 2.1 Scoring Rule
A collection of \( m \)-dimensional vectors \( \overrightarrow{s}_{\mathbb{N}} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{R}^m \) with \( \alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_m \) and \( \alpha_1 > \alpha_m \), for every \( m \in \mathbb{N} \) naturally defines a voting rule — a candidate gets score \( \alpha_i \) from a vote if it is placed at the \( i \)th position, and the score of the candidate is the sum of the scores it receives from all the votes. The winners are the candidates with the highest score. Given a set of candidates \( C \), a score vector \( \overrightarrow{\alpha} \) of length \( |C| \), a candidate \( x \in C \), and a profile \( P \), we denote the score of \( x \) in \( P \) by \( s^P(x) \). When the score vector \( \overrightarrow{\alpha} \) is clear from the context, we omit \( \overrightarrow{\alpha} \) from the superscript. A straightforward observation is that the scoring rules remain unchanged if we multiply every \( \alpha_i \) by any constant \( \lambda > 0 \) and/or add any constant \( \mu \). Hence, we assume without loss of generality that for any score vector \( \overrightarrow{s}_{\mathbb{N}} \), there exists a \( j \) such that \( \alpha_j - \alpha_{j+1} = 1 \) and \( \alpha_k = 0 \) for all \( k > j \). We call such a score vector a normalized score vector.

### 2.2 Weighted Majority Graph and Condorcet Voting Rule
Given an election \( E = (C, (\succ_1, \succ_2, \ldots, \succ_n)) \) and two candidates \( x, y \in C \), let us define \( N_E(x, y) \) to be the number of votes where the candidate \( x \) is preferred over \( y \). We say that a candidate \( x \) defeats another candidate \( y \) in pairwise election if \( N_E(x, y) > N_E(y, x) \). Using the election \( E \), we can construct a weighted directed graph \( G_E = (U = C, E) \) as follows. The vertex set \( U \) of the graph \( G_E \) is the set of candidates \( C \). For any two candidates \( x, y \in C \) with \( x \neq y \), let us define the margin \( D_E(x, y) \) of \( x \) from \( y \) to be \( N_E(x, y) - N_E(y, x) \). We have an edge from \( x \) to \( y \) in \( G_E \) if \( D_E(x, y) > 0 \). Moreover, in that case, the weight \( w(x, y) \) of the edge from \( x \) to \( y \) is \( D_E(x, y) \). A candidate \( c \) is called the Condorcet winner of an election \( E \) if there is an edge from \( c \) to every other vertices in the weighted majority graph \( G_E \). The Condorcet voting rule outputs the Condorcet winner if it exists and outputs the set \( C \) of all candidates otherwise.

Let \( r \) be a voting rule. We study the \( r \)-OPTIMAL DEFENSE problem which was defined by [Yin et al., 2016]. It is defined as follows. Intuitively, the \( r \)-OPTIMAL DEFENSE problem asks if there is a way to defend \( k_d \) voter groups such that, irrespective of which \( k_v \) voter groups the attacker attacks, the output of the election (that is the winning set of candidates) is always same as the original one. A voter group gets deleted if only if it is attacked but not defended.

**Definition 1 (r-OPTIMAL DEFENSE).** Given \( n \) voter groups \( G_i, i \in [n] \), two integers \( k_v \) and \( k_d \), does there exist an index set \( I \subseteq [n] \) with \( |I| \leq k_d \) such that, for every \( I' \subseteq [n] \setminus I \) with \( |I'| \leq k_v \), we have \( r(G_{I'}, i \in [n]) = r(G_{I}, i \in [n]) \)? The integers \( k_v \) and \( k_d \) are called respectively attacker’s resource and defender’s resource. We denote an arbitrary instance of the \( r \)-OPTIMAL DEFENSE problem by \( (C, \{G_i : i \in [n]\}, k_v, k_d) \).

We also study the \( r \)-OPTIMAL ATTACK problem which is defined as follows. Intuitively, in the \( r \)-OPTIMAL ATTACK problem the attacker is interested to know if it is possible to attack \( k_v \) voter groups such that, no matter which \( k_d \) voter groups the defender defends, the outcome of the election is never same as the original (that is the attack is successful).

**Definition 2 (r-OPTIMAL ATTACK).** Given \( n \) voter groups \( G_i, i \in [n] \), two integers \( k_v \) and \( k_d \), does there exist an index set \( \mathcal{I} \subseteq [n] \) with \( |\mathcal{I}| \leq k_v \) such that, for every \( \mathcal{I}' \subseteq [n] \setminus \mathcal{I} \) with \( |\mathcal{I}'| \leq k_d \), we have \( r(G_{\mathcal{I}'}, i \in [n]) \neq r(G_{\mathcal{I}}, i \in [n]) \)? We denote an arbitrary instance of the \( r \)-OPTIMAL ATTACK problem by \( (C, \{G_i : i \in [n]\}, k_v, k_d) \).

**Encoding of the Input Instance:** In both the \( r \)-OPTIMAL DEFENSE and \( r \)-OPTIMAL ATTACK problems, we assume that every input voter group \( G \) is encoded as follows. The encoding lists all the different votes \( \succ \) that appear in the voter group \( G \) along with the number of times the vote \( \succ \) appears in \( G \). Hence, if a voter group \( G \) contains only \( k \) different votes over \( m \) candidates and consists of \( n \) voters, then the encoding of \( G \) takes \( O(km \log \log n) \) bits of memory.

### 2.3 Parameterized complexity
A parameterized problem \( \Pi \) is a subset of \( \Gamma^* \times \mathbb{N} \), where \( \Gamma \) is a finite alphabet. A central notion is fixed parameter tractability (FPT) which means, for a given instance \( (x, k) \), solvability in time \((f(k) \cdot p(|x|))\), where \( f \) is an arbitrary function of \( k \) and \( p \) is a polynomial in the input size \(|x|\). There exists a hierarchy of complexity classes above FPT, and showing that a parameterized problem is hard for one of these classes is considered evidence that the problem is unlikely to be fixed-parameter tractable. The main classes in this hierarchy are: \( \text{FPT} \subseteq W[1] \subseteq W[2] \subseteq \cdots \subseteq W[P] \subseteq \text{XP} \). We now define the notion of parameterized reduction [Cygan et al., 2015].

**Definition 3.** Let \( A, B \) be parameterized problems. We say that \( A \) is \( fpt \)-reducible to \( B \) if there exist functions \( f, g : \mathbb{N} \rightarrow \mathbb{N} \), a constant \( \alpha \in \mathbb{N} \) and an algorithm \( \Phi \) which transforms an instance \((x, k)\) of \( A \) into an instance \((x', g(k))\) of \( B \) in time \( f(k) \cdot |x|^{\alpha} \) so that \((x, k) \in A\) if and only if \((x', g(k)) \in B\).

To show \( W \)-hardness, it is enough to give a parameterized reduction from a known hard problem.

### 3 Classical Complexity Results
[Yin et al., 2016] showed that the OPTIMAL DEFENSE problem is polynomial time solvable for the plurality voting rule when we have only 2 candidates. On the other hand, they also showed that the OPTIMAL DEFENSE problem is \( \text{NP} \)-complete when we have an unbounded number of candidates. We begin with improving their \( \text{NP} \)-completeness result by showing that the OPTIMAL DEFENSE problem becomes \( \text{NP} \)-complete even when we have only 3 candidates and the attacker can attack any number of voter groups. Towards that, we reduce the \( k \)-SUM problem to the OPTIMAL DEFENSE problem. The \( k \)-SUM problem is defined as follows.

**Definition 4 (k-SUM).** Given a set of \( n \) positive integers \( W = \{w_i, i \in [n]\}\), and two positive integers \( k \leq n \) and...
M, does there exist an index set $I \subset [n]$ with $|I| = k$ such that $\sum_{i \in I} w_i = M$?

The $k$-SUM problem can be easily proved to be NP-complete by modifying the NP-completeness proof of the Subset Sum problem in [Cormen et al., 2009]. We also need the following structural result for normalized scoring rules which has been used before [Baumeister et al., 2011; Dey et al., 2016].

**Lemma 1.** Let $C = \{c_1, \ldots, c_m\}$ be a set of candidates and $\vec{a}$ a normalized score vector of length $|C|$. Let $x, y \in C, x \neq y$, be any two arbitrary candidates. Then there exists a profile $P_x^n$ consisting of $m$ voters such that the following holds:

$s_{P_x^n}(x) + 1 = s_{P_x^n}(y) - 1 = s_{P_x^n}(a)$ for every $a \in C \setminus \{x, y\}$

For any two candidates $x, y \in C, x \neq y$, we use $P_x^n$ to denote the profile as defined in Lemma 1. We are now ready to present our NP-completeness result for the OPTIMAL DEFENSE problem for the scoring rules even in the presence of 3 candidates only. In the interest of space, we defer proof of some of our results to the full version of this paper [Dey et al., 2019b].

**Theorem 1.** The OPTIMAL DEFENSE problem is NP-complete for every scoring rule even if the number of candidate voters is 3 and the attacker can attack any number of the voter groups.

**Proof.** For the interest of space, we only prove NP-hardness. Let $\vec{a}$ be any normalized score vector of length 3. The OPTIMAL DEFENSE problem for the scoring rule based on $\vec{a}$ belongs to NP. Let $(W = \{w_1, \ldots, w_n\}, k, M)$ be an arbitrary instance of the $k$-SUM problem. We can assume, without loss of generality, that 8 divides $M$ and $w_i$ for every $i \in [n]$; if this is not the case, we replace $M$ and $w_i$ by respectably $8M$ and $8w_i$ for every $i \in [n]$ which clearly is an equivalent instance of the original instance. Let us also assume, without loss of generality, that $2k < n$ (if not then add enough copies of $M + 1$ to $W$) and $M < \sum_{i=1}^n w_i$ (since otherwise, it is a trivial NO instance). We construct the following instance of the OPTIMAL DEFENSE problem for the scoring rule based on $\vec{a}$. Let $M'$ be an integer such that $M' > \sum_{i=1}^n w_i$ and 8 divides $M'$. We have 3 candidate voters, namely $a, b$, and $c$. We have the following voter groups.

- For every $i \in [n]$, we have a voter group $G_i$ consisting of $w_i$ copies of $P_a^c$ (as defined in Lemma 1) and $M' - w_i$ copies of $P_b^c$. Hence, we have the following:

$s_{G_i}(c) = s_{G_i}(a) + M' + w_i = s_{G_i}(a) + 2M' - w_i$

We have one voter group $\hat{G}$ consisting of $(kM' + M)/2 - 3$ copies of $P_a^c$, $(kM' - M)/2 - 1$ copies of $P_b^c$, and $1$ copy of $P_a^c$. We have the following:

$s_{\hat{G}}(c) = s_{\hat{G}}(a) - (kM' + M - 6) = s_{\hat{G}}(b) - (2kM' - M - 6)$

Let $Q$ be the resulting profile; that is $Q = \cup_{i=1}^n G_i \cup \hat{G}$. We have $s_Q(c) = s_Q(a) + (n - k)M' + \sum_{i=1}^n w_i - M + 6 = s_Q(b) + (n - 2k)M' + M - n \sum_{i=1}^n w_i + 6$. Since $n > 2k$ and $M' > \sum_{i=1}^n w_i$, we have $s_Q(c) > s_Q(a)$ and $s_Q(c) > s_Q(b)$. Thus the candidate $c$ wins the election uniquely. We define $k_2$, the maximum number of voter groups that the defender can defend, to be $k$. We define $k_n$, the maximum number of voter groups that the attacker can attack, to be $n + 1$.

This finishes the description of the OPTIMAL DEFENSE instance. We claim that the two instances are equivalent.

In the forward direction, let the $k$-SUM instance be a YES instance and $I \subset [n]$ with $|I| = k$ be an index set such that $\sum_{i \in I} w_i = M$. Let us consider the defense strategy where the defender protects the voter groups $G_i$ for every $i \in I$. Since $\sum_{i \in I} w_i = M$, we have $\sum_{i \in I} (M' - w_i) = kM' - M$. Let $H$ be the profile of voter groups corresponding to the index set $I$; that is, $H = \cup_{i \in I} G_i$. Let $H'$ be the profile remaining after the attacker attacks some voter groups. Without loss of generality, we can assume that the attacker does not attack the voter group $\hat{G}$ since otherwise the candidate $c$ continues to win uniquely. We thus obviously have $H \cup \hat{G} \subseteq H'$. We have $s_{\hat{G} \cup \hat{G}}(c) = s_{\hat{G} \cup \hat{G}}(a) + kM' + \sum_{i \in I} w_i - (kM' + M - 6) = s_{\hat{G} \cup \hat{G}}(a) + 6$ and $s_{\hat{G} \cup \hat{G}}(c) = s_{\hat{G} \cup \hat{G}}(b) + 2kM' - \sum_{i \in I} w_i - (2kM' - M - 6) = s_{\hat{G} \cup \hat{G}}(b) + 6$. Since the candidate $c$ receives as much score as any other candidate in the voter group $G_i$ for every $i \in [n]$, we have $s_{\hat{G} \cup \hat{G}}(c) = s_{\hat{G} \cup \hat{G}}(a) + 6$ and $s_{\hat{G} \cup \hat{G}}(c) = s_{\hat{G} \cup \hat{G}}(b) + 6$. Hence, the candidate $c$ wins uniquely in the resulting profile $H'$ after the attack and thus the defense is successful.

In the other direction, let the OPTIMAL DEFENSE instance be a YES instance. Without loss of generality, we can assume that the attacker does not attack the voter group $\hat{G}$ and thus the defender does not defend the voter group $\hat{G}$. We can also assume, without loss of generality, that the defender defends exactly $k$ voter groups since the candidate $c$ receives as much score as any other candidate in the voter group $G_i$ for every $i \in [n]$. Let $I \subset [n]$ with $|I| = k$ such that defending all the voter groups $G_i, i \in I$ is a successful defense strategy. We claim that $\sum_{i \in I} w_i \geq M$. Suppose not, then let us assume that $\sum_{i \in I} w_i < M$. Since, $w_i$ is divisible by 8 and positive for every $i \in [n]$ and $m$ is divisible by 8, we have $\sum_{i \in I} w_i < M - 8$. Let $H$ be the profile of voter groups corresponding to the index set $I$; that is, $H = \cup_{i \in I} G_i$. We have $s_{H \cup \hat{G}}(c) = s_{H \cup \hat{G}}(a) + kM' + \sum_{i \in I} w_i - (kM' + M - 6) \leq s_{H \cup \hat{G}}(a) + M - 8 + M + 6 = s_{H \cup \hat{G}}(a) - 2$. Hence attacking the voter groups $G_i, i \in [n] \setminus I$ makes the score of $c$ strictly less than the score of $a$. This contradicts our assumption that defending all the voter groups $G_i, i \in I$ is a successful defense strategy. Hence we have $\sum_{i \in I} w_i \geq M$. We now claim that $\sum_{i \in I} w_i \leq M$. Suppose not, then let us assume that $\sum_{i \in I} w_i > M$. Since, $w_i$ is divisible by 8 and positive for every $i \in [n]$ and $m$ is divisible by 8, we have $\sum_{i \in I} w_i > M + 8$. Let $H'$ be the profile of voter groups corresponding to the index set $I$; that is, $H' = \cup_{i \in I} G_i$. We have $s_{H' \cup \hat{G}}(c) = s_{H' \cup \hat{G}}(b) + 2kM' - \sum_{i \in I} w_i - (2kM' - M - 6) \leq s_{H' \cup \hat{G}}(b) + (M + 8) + M + 6 = s_{H' \cup \hat{G}}(b) - 2$. Hence attacking the voter groups $G_i, i \in [n] \setminus I$ makes the score of $c$ strictly less than the score of $b$. This contradicts our assumption that defending all the voter groups $G_i, i \in I$ is a successful defense strategy. Hence we have $\sum_{i \in I} w_i \leq M$. Therefore we have $\sum_{i \in I} w_i = M$ and thus the $k$-SUM instance is a YES instance.

In the proof of Theorem 1, we observe that the reduced instance of the OPTIMAL DEFENSE problem viewed as an
instance of the \textsc{Optimal Attack} problem is a \textsc{No} instance if and only if the $k$-\textsc{Sum} instance is a \textsc{Yes} instance. Hence, the same reduction as in the proof of Theorem 1 gives us the following result for the \textsc{Optimal Attack} problem.

\textbf{Corollary 1.} The \textsc{Optimal Attack} problem is co\textsc{NP}-hard for every scoring rule even if the number of candidates is 3 and the attacker can attack any number of voter groups.

We now prove a similar hardness result as of Theorem 1 for the Condorcet voting rule.

\textbf{Theorem 2.} The \textsc{Optimal Defense} problem is \textsc{NP}-complete for the Condorcet voting rule even if the number of candidates is 3 and the attacker can attack any number of voter groups.

In the proof of Theorem 2, we observe that the reduced instance of \textsc{Optimal Defense} viewed as an instance of the \textsc{Optimal Attack} problem is a \textsc{No} instance if and only if the $k$-\textsc{Sum} instance is a \textsc{Yes} instance. Hence, the same reduction as in the proof of Theorem 2 gives us the following result for the \textsc{Optimal Attack} problem.

\textbf{Corollary 2.} The \textsc{Optimal Attack} problem is co\textsc{NP}-hard for the Condorcet voting rule even if the number of candidates is 3 and the attacker can attack any number of voter groups.

\section{\textsc{W}-Hardness Results}

In this section, we present our hardness results for the \textsc{Optimal Defense} and the \textsc{Optimal Attack} problems in the parameterized complexity framework. We consider the following parameters for both the problems – number of candidate ($m$), defender’s resource ($k_a$), and attacker’s resource ($k_d$). From Theorems 1 and 2 and Corollaries 1 and 2 we immediately have the following result for the \textsc{Optimal Defense} and \textsc{Optimal Attack} problems parameterized by the number of candidates for both the scoring rules and the Condorcet voting rule.

\textbf{Corollary 3.} The \textsc{Optimal Defense} problem is para-\textsc{NP}-hard parameterized by the number of candidates for both the scoring rules and the Condorcet voting rule. The \textsc{Optimal Attack} problem is para-co\textsc{NP}-hard parameterized by the number of candidates for both the scoring rules and the Condorcet voting rule.

The \textsc{NP}-completeness proof for the \textsc{Optimal Defense} problem for the plurality voting rule by [Yin et al., 2016] is actually a parameter preserving reduction from the \textsc{Hitting Set} problem parameterized by the solution size.

Since the \textsc{Hitting Set} problem parameterized by the solution size $k$ is known to be \textsc{W}[2]-complete [Downey and Fellows, 1999], the following result immediately follows from Theorem 2 of [Yin et al., 2016].

\textbf{Observation 1} ([Yin et al., 2016]). The \textsc{Optimal Defense} problem for the plurality voting rule is \textsc{W}[2]-hard parameterized by $k_d$.

We now generalize Observation 1 to any scoring rule by exhibiting a polynomial parameter transform from the \textsc{Hitting Set} problem parameterized by the solution size.

\textbf{Theorem 3.} The \textsc{Optimal Defense} and \textsc{Optimal Attack} problems for every scoring rule is \textsc{W}[2]-hard parameterized by $k_d$.

Next, we show the \textsc{W}[2]-hardness of the \textsc{Optimal Defense} and \textsc{Optimal Attack} problems for the Condorcet voting rule parameterized by $k_d$. This is also a parameter-preserving reduction from the \textsc{Hitting Set} problem.

\textbf{Theorem 4.} The \textsc{Optimal Defense} and \textsc{Optimal Attack} problems for the Condorcet voting rule is \textsc{W}[2]-hard parameterized by $k_d$.

We now show that the \textsc{Optimal Defense} problem for scoring rules is \textsc{W}[2]-hard parameterized by $k_a$ also by exhibiting a parameter preserving reduction from a problem closely related to \textsc{Hitting Set}, which is \textsc{Set Cover} problem parameterized by the solution size. This is a \textsc{W}[2]-complete problem [Downey and Fellows, 1999]. We now state our \textsc{W}[2]-hardness proof for the \textsc{Optimal Defense} problem for scoring rules and the Condorcet voting rule, parameterized by $k_a$, by a reduction from \textsc{Set Cover}.

\textbf{Theorem 5.} The \textsc{Optimal Defense} problem for every scoring rule and Condorcet rule is \textsc{W}[2]-hard parameterized by $k_a$.

We now show that the \textsc{Optimal Attack} problem for the scoring rules is \textsc{W}[1]-hard even parameterized by the combined parameter $k_a$ and $k_d$. Towards that, we exhibit a polynomial parameter transform from the \textsc{Clique} problem parameterized by the size of the clique we are looking for which is known to be \textsc{W}[1]-complete.

\textbf{Theorem 6.} The \textsc{Optimal Attack} problem for every scoring rule and Condorcet rule is \textsc{W}[1]-hard parameterized by $(k_a, k_d)$.

Once we have a parameterized algorithm for the \textsc{Optimal Defense} problem for the parameter $(k_a, k_d)$, an immediate question is whether there exists a kernel for the \textsc{Optimal Defense} problem of size polynomial in $(k_a, k_d)$. We know that the \textsc{Hitting Set} problem does not admit polynomial kernel parameterized by the universe size [Downey and Fellows, 1999]. It turns out that the reductions from the \textsc{Hitting Set} problem to the \textsc{Optimal Defense} and \textsc{Optimal Attack} problems in Theorems 3, 4 and 6 are polynomial parameter transformations. Hence we immediately have the following corollary.

\textbf{Corollary 4.} The \textsc{Optimal Defense} and \textsc{Optimal Attack} problems for the scoring rules and the Condorcet rule do not admit a polynomial kernel parameterized by $(k_a, k_d)$.

\section{\textsc{FPT Algorithm}}

We complement the negative results of Observation 1 and Theorem 5 by presenting an \textsc{FPT} algorithm for the \textsc{Optimal Defense} problem parameterized by $(k_a, k_d)$. In the absence of a defender, that is when $k_d = 0$, [Yin et al., 2016] showed that the \textsc{Optimal Defense} problem is polynomial time solvable for the plurality voting rule. Their polynomial time algorithm for the \textsc{Optimal Defense} problem can easily be extended to any scoring rule. Using this polynomial time algorithm, we design the following $O^*(k_a^{k_a})$ time algorithm for the \textsc{Optimal Defense} problem for scoring rules.
Theorem 7. There is an algorithm for the Optimal Defense problem for every scoring rule and the Condorcet voting rule which runs in time $O^*(k_a^d)$. 

6 Experiments

Though the previous sections show that the optimal defending problem is computationally intractable, it is a worst-case result. In practice, elections have voting profiles that are generated from some (possibly known) distribution. In this section, we conduct an empirical study to understand how simple defending strategies perform for two such statistical voter generation models. The defending strategies we consider are variants of a simple greedy policy.

6.1 Defending Strategy

For a given voting profile and a voting rule, the defending strategy finds the winner. Suppose the winner is $a$. The strategy considers $a$ with every other candidate, and for each such pair it creates a sorted list of classes based on the winning margin of votes for $a$ in those classes, and picks the top $k_d$ classes to form a sub-list. Now, among all these $(m - 1)$ sorted sub-lists, the strategy picks the most frequent $k_d$ classes to protect. We call this version of the strategy GREEDY 1. For certain profiles an optimal attacker (a) may change the outcome by attacking some of the unprotected classes or (b) is unable to change the outcome. If (a) occurs, then there is a possibility that for the value of $k_d$ there does not exist any defense strategy which can guard the election from all possible strategies of the attacker. In that case, GREEDY 1 is optimal and is not optimal otherwise. It is always optimal for case (b). Note that, given a profile and $k_d$ protected classes, it is easy to find if there exists an optimal attack strategy, while it is not so easy to identify whether there does not exist any defending strategy if the GREEDY 1 fails to defend. We find the latter with a brute-force search for this experiment. A small variant of GREEDY 1 is the following: when GREEDY 1 is unable to defend (which is possible to find out in poly-time), the strategy chooses to protect $k_d$ classes uniformly at random. Call this strategy GREEDY 2.

6.2 Voting Profile Generation

Fix $m = 5$. We generate 1000 preference profiles over these alternatives for $n = 12000$, where each vote is picked uniformly at random from the set of all possible strict preference orders over $m$ alternatives. The voters are partitioned into 12 classes containing equal number of voters. We consider three voting rules: plurality, veto, and Borda. The lower plot in Figure 1 shows the number of profiles which belongs to the three categories: (i) GREEDY 1 defends (is optimal), (ii) GREEDY 1 cannot defend but no defending strategy exists (is optimal), (iii) GREEDY 1 cannot defend but defending strategy exists (not optimal). The x-axis shows different values of $k_d$ and we fix $k_a = 12 - k_d$.

The upper plot of Figure 1 shows the fraction of the profiles successfully defended by GREEDY 2 where GREEDY 1 is not optimal (i.e., cannot defend but defending strategy exists) when GREEDY 2 uniformly at random picks $k_d$ classes 100 times. These fractions therefore serve as an empirical probability of successful defense of GREEDY 2 given GREEDY 1 is not optimal.

In an election where the primary contest happens between two major candidates, even though there are more candidates present, the generation model may be a little different. We also consider another generation model that generates 40% profiles having a fixed alternative $a$ on top and the strict order of the $(m - 1)$ alternatives is picked uniformly at random, a similar 40% profiles with some other alternative $b$ on top, and the remaining 20% preferences are picked uniformly at random from the set of all possible strict preference orders. Similar experiments are run on this generation model and results are shown in Figure 2.

The results show that even though optimal defense is a hard problem, a simple strategy like greedy achieves more than 70% optimality. From the rest 30% non-optimal cases, the variant GREEDY 2 is capable of salvaging it into optimal with probability almost 5% for uniform generation model and above 5% for two-major contestant generation model for $k_d = k_a = 6$. This empirically hints at a possibility that defending real elections may not be too difficult.
References


