

A Parameterized Perspective on Protecting Elections

Palash Dey¹, Neeldhara Misra², Swaprava Nath³ and Garima Shakya³

¹Indian Institute of Technology, Kharagpur, India

²Indian Institute of Technology, Gandhinagar, India

³Indian Institute of Technology, Kanpur, India

August 15, 2019



Setup of the Election

- A set of candidates and a set of voters.

Setup of the Election

- A set of candidates and a set of voters.
- The voters are partitioned into groups (or classes), e.g. polling booths or constituencies.

Setup of the Election

- A set of candidates and a set of voters.
- The voters are partitioned into groups (or classes), e.g. polling booths or constituencies.
- Each vote is a **strict preference order** over the set of candidates.

Setup of the Election

- A set of candidates and a set of voters.
- The voters are partitioned into groups (or classes), e.g. polling booths or constituencies.
- Each vote is a **strict preference order** over the set of candidates.
- **Computing Winner**: Using voting rules e.g. Plurality, Borda, Veto, Condorcet etc.

Setup of the Election

- A set of candidates and a set of voters.
- The voters are partitioned into groups (or classes), e.g. polling booths or constituencies.
- Each vote is a **strict preference order** over the set of candidates.
- **Computing Winner**: Using voting rules e.g. Plurality, Borda, Veto, Condorcet etc.
- All the valid votes are taken together and candidate with highest score is declared the winner.

Setup of the Election

- A set of candidates and a set of voters.
- The voters are partitioned into groups (or classes), e.g. polling booths or constituencies.
- Each vote is a **strict preference order** over the set of candidates.
- **Computing Winner**: Using voting rules e.g. Plurality, Borda, Veto, Condorcet etc.
- All the valid votes are taken together and candidate with highest score is declared the winner.
- **Attacker**'s objective is **to change the outcome of the election** and **Defender**'s job is to protect it.

Is it possible for an external agent to influence the outcome of the election?

Is it possible for an external agent to influence the outcome of the election?

Is it possible to change the winner by deleting k voter groups,

Is it possible for an external agent to influence the outcome of the election?

Is it possible to change the winner by deleting k voter groups,
(presumably by destroying ballot boxes or rigging electronically submitted
votes)?

- **Input**

- A set of voter groups (every voter group is a set of votes).

- **Input**

- A set of voter groups (every voter group is a set of votes).
- Two integers k_a and k_d .

- **Input**

- A set of voter groups (every voter group is a set of votes).
- Two integers k_a and k_d .
 - k_a : number of voter groups the **attackers** can attack

- **Input**

- A set of voter groups (every voter group is a set of votes).
- Two integers k_a and k_d .
 - k_a : number of voter groups the **attackers** can attack
 - k_d : number of voter groups the **defenders** can defend

- **Input**

- A set of voter groups (every voter group is a set of votes).
- Two integers k_a and k_d .
 - k_a : number of voter groups the **attackers** can attack
 - k_d : number of voter groups the **defenders** can defend
- A voter group gets removed if it is attacked but not defended.

Optimal Defense or Attack problems

Optimal Defense problem

Is it possible for the **defender** to find a strategy that, no matter which k_a voter groups the **attacker** attacks, the outcome of the election **does not change**.

Optimal Defense or Attack problems

Optimal Defense problem

Is it possible for the **defender** to find a strategy that, no matter which k_a voter groups the **attacker** attacks, the outcome of the election **does not change**.

Optimal Attack problem

Is it possible for the **attacker** to find a strategy that, no matter which k_d voter groups the **defender** defends, the outcome of the election is **always different** from the original (without any attack) one.

r-Optimal Defense and Attack Problem

- r is a voting rule.

r -Optimal Defense Problem $(\mathcal{C}, \{\mathcal{G}_i : i \in [n]\}, k_a, k_d)$

Given n voter groups $\mathcal{G}_i, i \in [n]$, two integers k_a and k_d , does there exist an index set $\mathcal{I} \subseteq [n]$ with $|\mathcal{I}| \leq k_d$ such that, for every $\mathcal{I}' \subset [n] \setminus \mathcal{I}$ with $|\mathcal{I}'| \leq k_a$, we have $r((\mathcal{G}_i)_{i \in [n] \setminus \mathcal{I}'}) = r((\mathcal{G}_i)_{i \in [n]})$?

r -Optimal Attack Problem $(\mathcal{C}, \{\mathcal{G}_i : i \in [n]\}, k_a, k_d)$

Given n voter groups $\mathcal{G}_i, i \in [n]$, two integers k_a and k_d , does there exist an index set $\mathcal{I} \subseteq [n]$ with $|\mathcal{I}| \leq k_a$ such that, for every $\mathcal{I}' \subset [n] \setminus \mathcal{I}$ with $|\mathcal{I}'| \leq k_d$, we have $r((\mathcal{G}_i)_{i \in [n] \setminus \mathcal{I}'}) \neq r((\mathcal{G}_i)_{i \in [n]})$?

Parameterized Complexity

- **Fixed Parameter Tractability (FPT):** 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 $|x|$.

Parameterized Complexity

- **Fixed Parameter Tractability (FPT):** 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 $|x|$.
- Hierarchy of Parameterized complexity classes above FPT:
$$\text{FPT} \subseteq \text{W}[1] \subseteq \text{W}[2] \subseteq \dots \subseteq \text{W}[P] \subseteq \text{XP}.$$

Complexity Results

Parameters	Optimal Defense		Optimal Attack	
	<i>Scoring rules</i>	<i>Condorcet</i>	<i>Scoring rules</i>	<i>Condorcet</i>
k_d	W[2]-hard	W[2]-hard	W[2]-hard	W[2]-hard
k_a	W[2]-hard	W[2]-hard	W[1]-hard	W[1]-hard
(k_a, k_d)	$\mathcal{O}^*(k_a^{k_d})$ No poly kernel			
m	para-NP-hard		para-coNP-hard	

Parameterized Complexity Results

- OD problem for every scoring rule and the Condorcet voting rule is **W[2]-hard** for both the parameters k_a and k_d .

Parameterized Complexity Results

- OD problem for every scoring rule and the Condorcet voting rule is **W[2]-hard** for both the parameters k_a and k_d .
 - It admits a **fixed parameter tractable** algorithm parameterized by the combined parameter (k_a, k_d) .

Parameterized Complexity Results

- OD problem for every scoring rule and the Condorcet voting rule is **W[2]-hard** for both the parameters k_a and k_d .
 - It admits a **fixed parameter tractable** algorithm parameterized by the combined parameter (k_a, k_d) .
- OA problem for every scoring rule and the Condorcet voting rule turns out to be *much harder*.

Parameterized Complexity Results

- OD problem for every scoring rule and the Condorcet voting rule is **W[2]-hard** for both the parameters k_a and k_d .
 - It admits a **fixed parameter tractable** algorithm parameterized by the combined parameter (k_a, k_d) .
- OA problem for every scoring rule and the Condorcet voting rule turns out to be *much harder*.
 - **W[1]-hard** even for the combined parameter (k_a, k_d) .

Greedy DEFENSE strategy:

- Let the set of candidates $\{a, b, c, d, e\}$ and winner is 'a'.
- Voter groups are $\{S_1, S_2, S_3, S_4, \dots, S_{10}\}$, $k_d = k_a = 5$
- For each of the pair (a, b) , (a, c) , (a, d) and (a, e) , arrange the voter groups according to decreasing winning margin for 'a'.

For (a, b) :

$S_1, S_2, S_3, S_4, S_5, S_6, \dots$

For (a, d) :

$S_7, S_4, S_5, S_9, S_1, S_{10}, \dots$

For (a, c) :

$S_2, S_7, S_4, S_5, S_9, S_1, \dots$

For (a, e) :

$S_2, S_6, S_4, S_5, S_7, S_1, \dots$

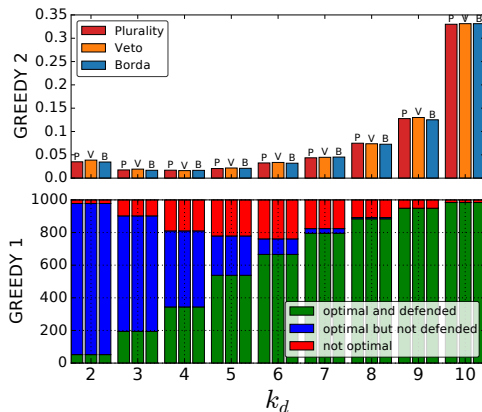
- Arrange the voter groups according to *decreasing frequencies* of them in the first k_d groups in each of these lists.

$S_4(4), S_5(4), S_2(3), S_7(3), S_1(2), S_9(2), S_3(1), S_6(1), S_8(0), S_{10}(0)$

- Choose the first $k_d (= 5)$ voter groups and defend them.

$\{S_4(4), S_5(4), S_2(3), S_7(3), S_1(2)\}$

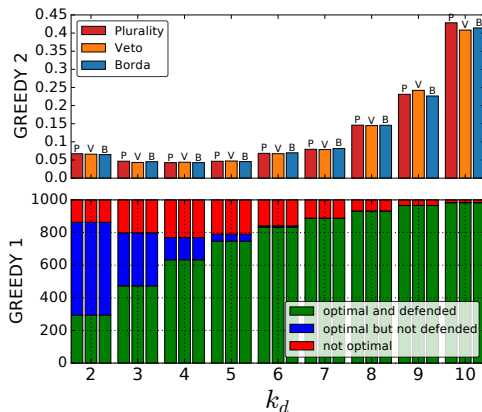
Empirical Results



Performances of Greedy Algorithm for uniform voting profile generation model

$$k_a = 12 - k_d$$

Empirical Results



Performances for two major contesting candidates voting profiles

$$k_a = 12 - k_d$$

Empirical Results

- Though optimal defense is a hard problem, a simple strategy like greedy achieves more than 70% optimality.

Empirical Results

- 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

Empirical Results

- 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

Empirical Results

- 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 $k_d = k_a = 6$.

Future Work

- To consider other objective of the attacker.

- To consider other objective of the attacker.
 - To find an attack strategy such that her desired candidate is the new winner.

- To consider other objective of the attacker.
 - To find an attack strategy such that her desired candidate is the new winner.
 - To not to destroy the votes but to manipulate them.

- To consider other objective of the attacker.
 - To find an attack strategy such that her desired candidate is the new winner.
 - To not to destroy the votes but to manipulate them.
- Experiment on real-world data.

- To consider other objective of the attacker.
 - To find an attack strategy such that her desired candidate is the new winner.
 - To not to destroy the votes but to manipulate them.
- Experiment on real-world data.

Thank you for your attention.

