A Parameterized Perspective on Attacking and Defending Elections

IWOCA, 2020

Kishen Gowda — Neeldhara Misra — Vraj Patel

June 9, 2020

Indian Institute of Technology, Gandhinagar

Background

Introduction

- Based on the paper **"Protecting Elections by Recounting Ballots"** (Elkind et. al., IJCAI '19)[2]
- Vote Manipulation Problem
- Has two stages:
  - Attacker: Tries to manipulate the election
  - Defender: Recounts the ballots to protect election

The Problem

- Set of k districts
- Set of m candidates (C)
- n voters spread across different districts
- v_{ij} representing number of votes of j^{th} candidate in the i^{th} district

The Problem

- PV: Plurality over Voters
- $SW(a) = \sum_{i \in [k]} v_{ia}$

The Problem

- PV: Plurality over Voters
- $SW(a) = \sum_{i \in [k]} v_{ia}$
- PD: Plurality over Districts
- i^{th} district is assigned a weight w_i
- Plurality winner in that district is given a "score" of w_i
- $SW(a) = \sum_{i \in [k]} w_i \cdot [a = \arg\max(v_i)]$

The Problem

- PV: Plurality over Voters
- $SW(a) = \sum_{i \in [k]} v_{ia}$
- PD: Plurality over Districts
- i^{th} district is assigned a weight w_i
- Plurality winner in that district is given a "score" of w_i
- $SW(a) = \sum_{i \in [k]} w_i \cdot [a = \arg\max(v_i)]$
- Order for tie-breaking: $\succ$ is a linear order over C.
- $a \succ b$ means a is favoured over b

The Attacker

- A preferred candidate w
- Budget of $B_{\mathcal{A}}$
- γ_i: how many votes can be manipulated in the i^{th} district

The Attacker

- A preferred candidate w
- Budget of $B_{\mathcal{A}}$
- γ_i: how many votes can be manipulated in the i^{th} district
- **Manipulation Problem (Man):** Is there a successful manipulation strategy $\mathbb{Z}$ where $\mathbb{Z}$ is a subset of the districts and $|\mathbb{Z}| \leqslant B_{\mathcal{A}}$, s.t. a preferred candidate a is the winner?
- Manipulated setting: v_{ij} to $\overline{v}_{ij}$

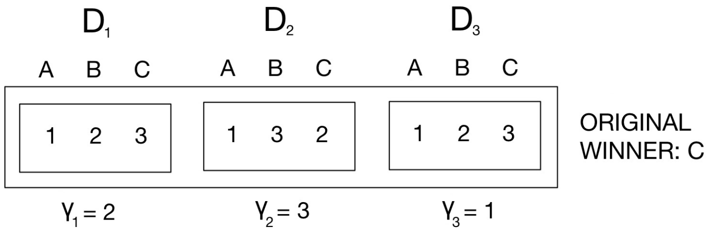
The Defender

- Orders recounts in some districts
- Budget of $B_{\mathcal{D}}$
- **Recounting Problem (Rec):** Is there a successful recounting strategy $\mathcal{R}$ where $\mathcal{R}$ is a subset of the districts and $|\mathcal{R}| \leqslant B_{\mathcal{D}}$, s.t. a preferred candidate b is the winner?

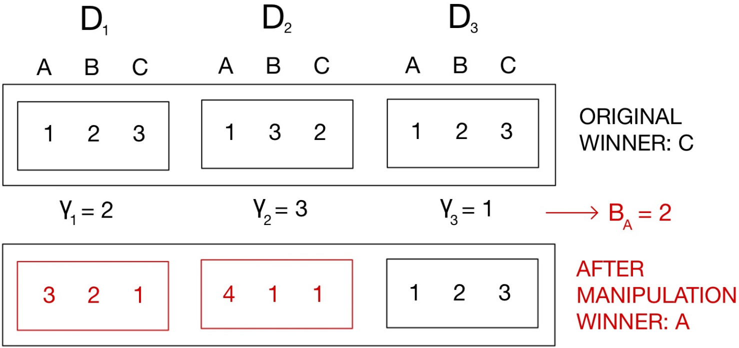
The Defender

- Orders recounts in some districts
- Budget of $B_{\mathcal{D}}$
- **Recounting Problem (Rec):** Is there a successful recounting strategy $\mathcal{R}$ where $\mathcal{R}$ is a subset of the districts and $|\mathcal{R}| \leqslant B_{\mathcal{D}}$, s.t. a preferred candidate b is the winner?
- Tries to make a better candidate win
- Better: had more social welfare
- Knows about both v_{ij} and $\overline{v}_{ij}$

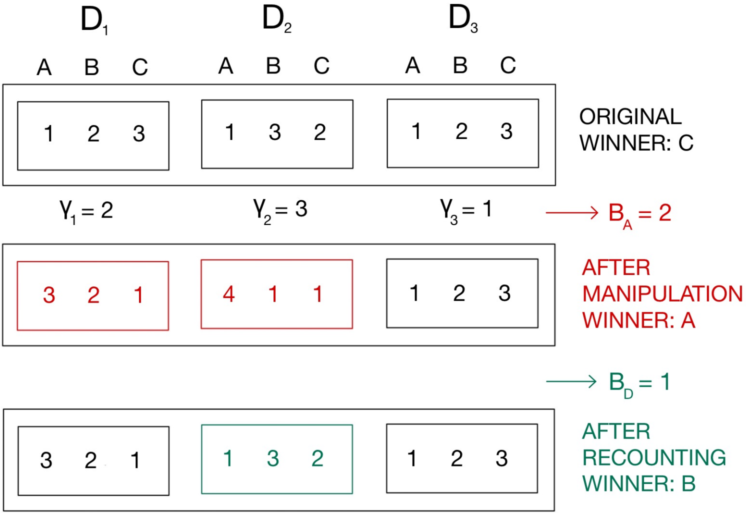
Example



Example


D1
D2
D3
A B C
A B C
A B C
1 2 3
1 3 2
1 2 3
ORIGINAL
WINNER: C
Y1 = 2
Y2 = 3
Y3 = 1
BA = 2
3 2 1
4 1 1
1 2 3
AFTER
MANIPULATION
WINNER: A

Example


D1
D2
D3
A B C
A B C
A B C
1 2 3
1 3 2
1 2 3
ORIGINAL
WINNER: C
Y1 = 2
Y2 = 3
Y3 = 1
BA = 2
3 2 1
4 1 1
1 2 3
AFTER
MANIPULATION
WINNER: A
BD = 1
3 2 1
1 3 2
1 2 3
AFTER
RECOUNTING
WINNER: B

Existing Hardness Results

	Plurality over Voters (PV)	**Plurality over Districts** (PD)	
		Unweighted	Weighted
REC	NP-c, Thm. 3.1 (i) ③ NP-c, Thm. 3.1 (ii) Ⓤ $O(n^{m+2})$, Thm. 3.2	P, Thm. 4.3	NP-c, Thm. 4.1 (i) ③ NP-c, Thm. 4.1 (ii) Ⓤ $O(n^{m+2})$, Thm. 4.2
MAN	NP-h, Thm. 3.3 (i) ③ ⓪ (∞) NP-h, Thm. 3.3 (ii) Ⓤ ⓪ (∞)	NP-c, Thm. 4.8 Ⓤ	Σ_2^P-c, Thm. 4.6 ③ NP-h, Thm. 4.7 Ⓤ ⓪

Figure 1: Summary of Existing Complexity Results [2]

Parameterized Complexity

Parameterized Terminology

Definition [1]

A parameterized problem is a language $L \subseteq \Sigma^* \times \mathbb{N}$, where Σ is a finite alphabet. The second component is called the parameter of the problem.

- FPT running time: $f(k) \cdot |x|^{O(1)}$
- FPT: Fixed-Parameter Tractable

W-Hardness

Definition

The W hierarchy is a collection of computational complexity classes defined for parameterized problems. $W[i] \subseteq W[j]$ for all $i \leqslant j$.

- $W[0]$, $W[1]$, ... correspond to increasing difficulty of problems.
- $W[0] = FPT$

Our Work

FPT Parameters

PV-Rec

- *FPT* when parameterized with parameters:
    - No. of districts (k)
    - No. of voters (n)
- Follows from a simple brute force algorithm

FPT Parameters

PV-MAN

- *FPT* when parameterized with no. of voters n.
- For each possible set of districts that can be chosen (2^k)
- For each district in the chosen set ($\leqslant B_{\mathcal{A}}$)
- Consider all possible ways votes can be manipulated (m^n)

FPT Parameters

PV-MAN

- *FPT* when parameterized with no. of voters n.
- For each possible set of districts that can be chosen (2^k)
- For each district in the chosen set ($\leqslant B_{\mathcal{A}}$)
- Consider all possible ways votes can be manipulated (m^n)
- Run FPT algorithm for PV-REC parameterized by n
- $k \leqslant n$, $B_{\mathcal{A}} \leqslant n$ and $m \leqslant 2n$

Why $m \leqslant 2n$?

- In practical scenarios, $m \leqslant n$
- A theoretical bound also exists

Why $m \leqslant 2n$?

- In practical scenarios, $m \leqslant n$
- A theoretical bound also exists
- At most n candidates can hold any votes
- After manipulation n others can
- $2n$ candidates are "interesting"

PV-Rec with parameter $B_{\mathfrak{D}}$

Lemma

PV-Rec is W[2]-hard parameterized by budget of the defender ($B_{\mathfrak{D}}$).

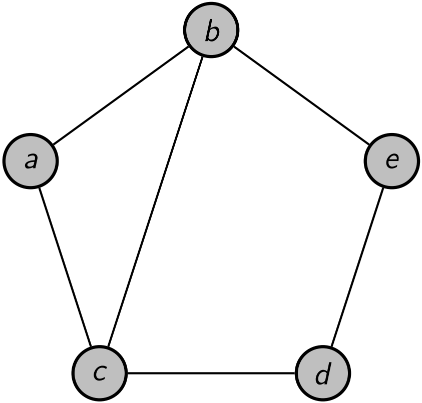
Proof: Follows from a reduction from the Dominating Set Problem.

Dominating Set Problem

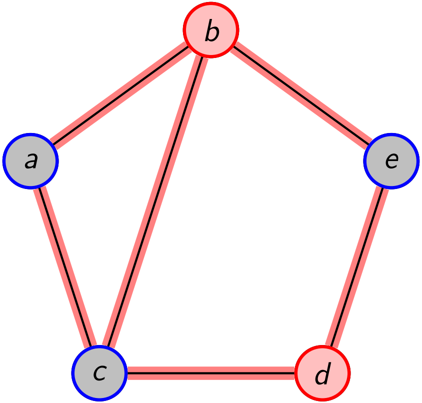
Dominating Set Problem

Given a graph $G = (V, E)$ and an integer $k \leqslant n$, is there a set $D \subseteq V$ such that D is a dominating set of G, i.e., $|D| \leqslant k$ and $V = N[D]$?

Dominating Set Example



Dominating Set Example



Reduction: Dominating Set to PV-Rec

Fact: Dominating Set Problem is W[2]-Hard [1].

Reduction: Dominating Set to PV-Rec

Fact: DOMINATING SET PROBLEM is W[2]-Hard [1].

Given an instance $(G = (V, E), k)$ of DOMINATING SET, construct an instance of PV-REC as follows:

Districts:

- A special district $\mathcal{D}_0$
- A district $\mathcal{D}_v$ corresponding to each vertex $v \in V$

Reduction: Dominating Set to PV-Rec

Candidates:

- A candidate $\mathcal{C}_v$ for each vertex $v \in V$
- A special candidate w
- *Dummy* candidates d_{vj} for all $v \in V$ where $j \in N_G[v]$.

Reduction: Dominating Set to PV-Rec

Candidates:

- A candidate $\mathcal{C}_v$ for each vertex $v \in V$
- A special candidate w
- *Dummy* candidates d_{vj} for all $v \in V$ where $j \in N_G[v]$.

Budget $(B_{\mathcal{D}})$**:** k
Preferred Candidate: w
Tie Breaking Order: $\ldots \mathcal{C}_v \ldots \succ w \succ \ldots d_{vj} \ldots$

Reduction: Dominating Set to PV-Rec

Voting Profile: After Manipulation

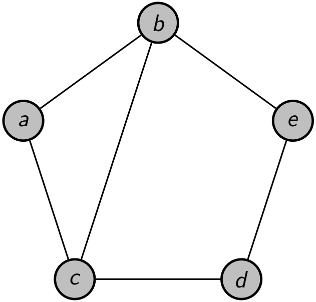
District	w	$\dots$	$\mathcal{C}_u$	$\dots$	d_{vj}
$\mathcal{D}_0$	$\|V\|$	$\dots$	$\|V\| - (\delta(u) + 1)$	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathcal{D}_v$	0	$\dots$	1 if $u \in N[v]$ else 0	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Reduction: Dominating Set to PV-Rec

Voting Profile: Before Manipulation

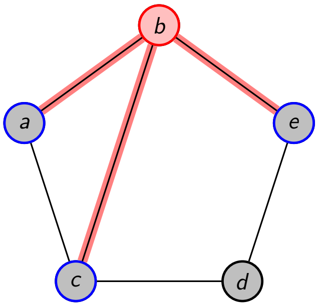
District	w	$\dots$	$\mathcal{C}_u$	$\dots$	d_{vj}
$\mathcal{D}_0$	$\lvert V \rvert$	$\dots$	$\lvert V \rvert - (\delta(u) + 1)$	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathcal{D}_v$	0	$\dots$	0	$\dots$	1 if $j \in N[v]$ else 0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Example: Dominating Set to PV-Rec



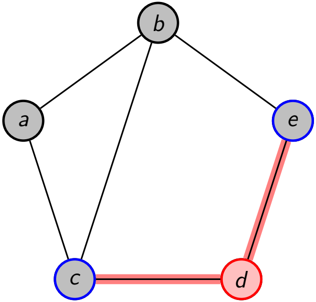
District	w	$\mathcal{C}_a$	$\mathcal{C}_b$	$\mathcal{C}_c$	$\mathcal{C}_d$	$\mathcal{C}_e$
$\mathcal{D}_0$	5	2	1	1	2	2
$\mathcal{D}_a$	0	1	1	1	0	0
$\mathcal{D}_b$	0	1	1	1	0	1
$\mathcal{D}_c$	0	1	1	1	1	0
$\mathcal{D}_d$	0	0	0	1	1	1
$\mathcal{D}_e$	0	0	1	0	1	1
Total	5	5	5	5	5	5

Example: Dominating Set to PV-Rec



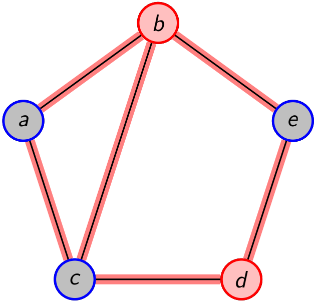
District	w	$\mathcal{C}_a$	$\mathcal{C}_b$	$\mathcal{C}_c$	$\mathcal{C}_d$	$\mathcal{C}_e$
$\mathcal{D}_0$	5	2	1	1	2	2
$\mathcal{D}_a$	0	1	1	1	0	0
$\mathcal{D}_b$	0	0	0	0	0	0
$\mathcal{D}_c$	0	1	1	1	1	0
$\mathcal{D}_d$	0	0	0	1	1	1
$\mathcal{D}_e$	0	0	1	0	1	1
Total	5	4	4	4	5	4

Example: Dominating Set to PV-Rec



District	w	$\mathcal{C}_a$	$\mathcal{C}_b$	$\mathcal{C}_c$	$\mathcal{C}_d$	$\mathcal{C}_e$
$\mathcal{D}_0$	5	2	1	1	2	2
$\mathcal{D}_a$	0	1	1	1	0	0
$\mathcal{D}_b$	0	1	1	1	0	1
$\mathcal{D}_c$	0	1	1	1	1	0
$\mathcal{D}_d$	0	0	0	0	0	0
$\mathcal{D}_e$	0	0	1	0	1	1
Total	5	5	5	4	4	4

Example: Dominating Set to PV-Rec



District	w	$\mathcal{C}_a$	$\mathcal{C}_b$	$\mathcal{C}_c$	$\mathcal{C}_d$	$\mathcal{C}_e$
$\mathcal{D}_0$	5	2	1	1	2	2
$\mathcal{D}_a$	0	1	1	1	0	0
$\mathcal{D}_b$	0	0	0	0	0	0
$\mathcal{D}_c$	0	1	1	1	1	0
$\mathcal{D}_d$	0	0	0	0	0	0
$\mathcal{D}_e$	0	0	1	0	1	1
Total	5	4	4	3	4	3

Proof of Reduction

Forward Direction:

- Dominating set D of size at most k
- Select the districts $\mathcal{D}_v$ for all $v \in D$
- For each $v \in D$, votes of C_j for all $j \in N_G[v]$ drop by 1
- All vertex candidates lose at least one vote
- Dummy candidates cannot get more than one vote
- w has most votes and wins

Proof of Reduction

Reverse Direction:

- Defender has strategy $\mathcal{R}$ s.t $|\mathcal{R}| \leqslant B_{\mathcal{D}}$
- No use of recounting $\mathcal{D}_0$
- All $\mathcal{C}_v$ candidates must lose at least 1 vote.

Proof of Reduction

Reverse Direction:

- Defender has strategy $\mathcal{R}$ s.t $|\mathcal{R}| \leqslant B_{\mathcal{D}}$
- No use of recounting $\mathcal{D}_0$
- All $\mathcal{C}_v$ candidates must lose at least 1 vote.
- Suppose, if $\mathcal{R}$ is not a dominating set $\implies \exists$ at least one vertex u which is not covered by $\mathcal{R}$.
- None of the neighbours of $u \in \mathcal{R}$
- Vote count of $\mathcal{C}_u$ remains same. **Contradiction!**

PV-Man with parameter $B_{\mathcal{A}}$

Lemma

PV-MAN is W[1]-hard parameterized by budget of the attacker ($B_{\mathcal{A}}$).

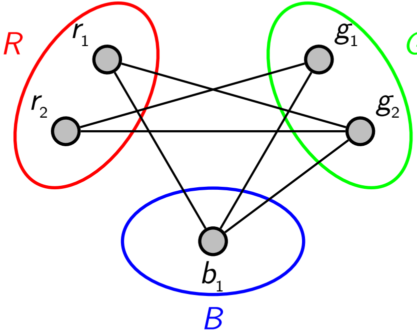
Proof: Follows from a reduction from the MULTICOLORED CLIQUE PROBLEM.

Multicolored Clique Problem

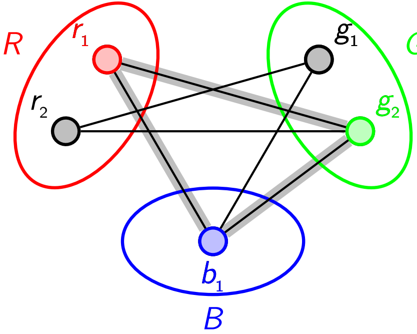
Multicolored Clique Problem

Given a graph G and a partition of the vertex set $V = V_1 \uplus V_2 \uplus \ldots \uplus V_k$ into k color classes, is there a set $S \subseteq V$ such that it is a multicolored clique of G, i.e., $|S| = k$ and $|S \cap V_i| = 1$ for each $i \in [k]$?

Multicolored Clique Example



Multicolored Clique Example



Reduction: Multicolored Clique to PV-Man

Fact: MULTICOLORED CLIQUE is W[1]-Hard [3, 4].

Reduction: Multicolored Clique to PV-Man

Fact: Multicolored Clique is W[1]-Hard [3, 4].

Given an instance $(G = (V = V_1 \uplus \ldots \uplus V_k, E), k)$ of Multicolored Clique, construct an instance of PV-Man as follows:

Districts:

- A baseline district $\mathcal{D}_0$
- A primary district $\mathcal{D}_v$ corresponding to each vertex $v \in V$
- Two secondary districts $\mathcal{D}_{uv}$ and $\mathcal{D}_{vu}$ corresponding to each edge $e = (u, v) \in E$.

Reduction: Multicolored Clique to PV-Man

Candidates:

- Main candidates: c_v for each vertex $v \in V$
- Challenger candidates: $\mathcal{R}_i$ for each color class $i \in [k]$
- Challenger candidates: $\mathcal{R}_{ij}$ and $\mathcal{R}_{ji}$ for each pair of color classes $1 \leqslant i < j \leqslant k$
- A special candidate w
- *Dummy* candidates: used to equalize number of votes across *primary* and *secondary* districts.

Reduction: Multicolored Clique to PV-Man

Candidates:

- Main candidates: c_v for each vertex $v \in V$
- Challenger candidates: $\mathcal{R}_i$ for each color class $i \in [k]$
- Challenger candidates: $\mathcal{R}_{ij}$ and $\mathcal{R}_{ji}$ for each pair of color classes $1 \leqslant i < j \leqslant k$
- A special candidate w
- *Dummy* candidates: used to equalize number of votes across *primary* and *secondary* districts.

Budgets: $B_{\mathcal{A}} = k^2$, $B_{\mathcal{D}} = 0$

Preferred Candidate: w

Tie Breaking Order:

$\ldots \mathcal{R}_i \ldots \succ \ldots \mathcal{R}_{ij} \ldots \succ \ldots c_v \ldots \succ w \succ \ldots \text{dummies} \ldots$

Reduction: Multicolored Clique to PV-Man

Voting Profile:

District	w	$\mathcal{R}_i$	$\mathcal{R}_{ij}$	c_x
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathcal{D}_v$	0	1 if $v \in V_i$ else 0	0	$k-1$ if $v = x$ else 0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathcal{D}_{uv}$	0	0	1 if $u \in V_i$ & $v \in V_j$, else 0	1 if $u, x \in V_{i'}$ & $u \neq x$, else 0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Reduction: Multicolored Clique to PV-Man

Voting Profile:

- Let ℓ be a large constant.
- For district D with ν voters, add $\ell - \nu$ dummy candidates, and a distinct dummy voter to each.
- Let $F = \ell k^2$.

Reduction: Multicolored Clique to PV-Man

Voting Profile:

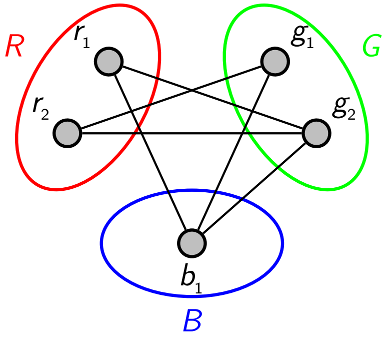
- Let ℓ be a large constant.
- For district D with ν voters, add $\ell - \nu$ dummy candidates, and a distinct dummy voter to each.
- Let $F = \ell k^2$.
- **District $\mathcal{D}_0$:** Designed such that all main candidates (c_v) get overall $F + k - 2$ votes and the challenger candidates $(\mathcal{R}_i' s$ and $\mathcal{R}_{ij}' s)$ get overall F votes.
- w gets 0 votes overall.
- $\gamma_{\mathcal{D}_0} = 0$, $\gamma_D = \ell$ for all other districts D.

Reduction: Multicolored Clique to PV-Man

Attack Plan:

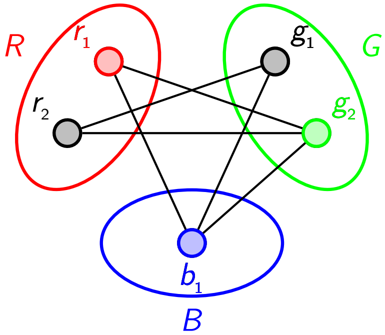
- Our strategy will be to transfer all (i.e. ℓ) votes in selected districts to w.
- Final score of w will be $\ell k^2 = F$.
- All the candidates $\mathcal{R}_i$'s, $\mathcal{R}_{ij}$'s and c_v's are above w
- Need them to lose at least 1, 1 and $k-1$ votes respectively.

Example: Multicolored Clique to PV-Man



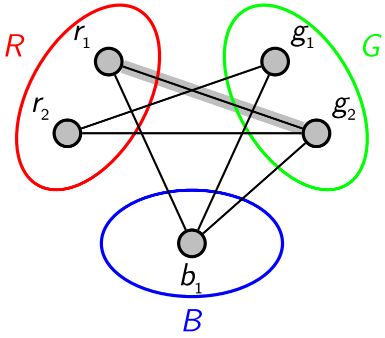
- $k = 3, \ell = 3, F = 27$
- $\mathcal{R}_i = 27, \mathcal{R}_{ij} = 27, c_v = 28$

Example: Multicolored Clique to PV-Man



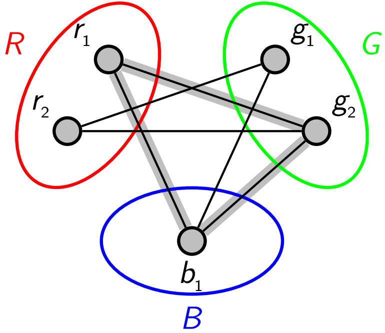
- $\mathcal{R}_R, \mathcal{R}_G, \mathcal{R}_B$ decreases by 1
- $c_{r_1}, c_{g_2}, c_{b_1}$ decreases by 2

Example: Multicolored Clique to PV-Man



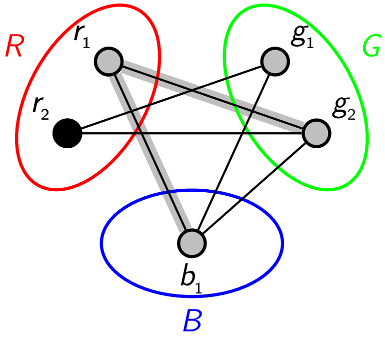
- $\mathcal{R}_{RG}$ and $\mathcal{R}_{GR}$ decreases by 1
- $\mathcal{R}_{RB}, \mathcal{R}_{BR}, \mathcal{R}_{GB}$ and $\mathcal{R}_{BG}$ also decrease by 1

Example: Multicolored Clique to PV-Man



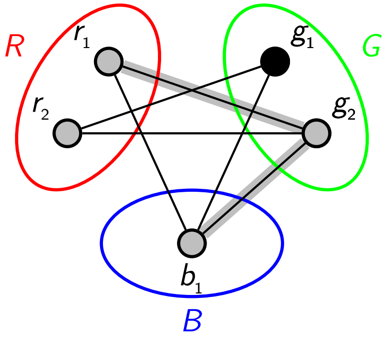
- $\mathcal{R}_{RG}$ and $\mathcal{R}_{GR}$ decreases by 1
- $\mathcal{R}_{RB}, \mathcal{R}_{BR}, \mathcal{R}_{GB}$ and $\mathcal{R}_{BG}$ also decrease by 1

Example: Multicolored Clique to PV-Man



- c_{r_2} loses 2 votes.
- c_{g_1} also loses 2 votes.

Example: Multicolored Clique to PV-Man



- c_{r_2} loses 2 votes.
- c_{g_1} also loses 2 votes.

Proof of Reduction

Forward Direction:

- Multi-colored clique S of size k.
- Select the k primary districts and $2\binom{k}{2}$ secondary districts corresponding to vertices and edges of S.
- Transfer all ℓ votes in each district to w.
- All challenger candidates lose 1 vote each.
- Dummy candidates may have 0 or 1 vote.

Proof of Reduction

Forward Direction:

- Main candidates corresponding to S lose $k-1$ votes from their corresponding primary district.
- Let $S \cap V_i = \{v_i\}$. For any other $u \in V_i$, c_u loses 1 vote each from the districts corresponding to the $k-1$ edges of v_i in S. Thus, c_u loses $k-1$ votes too.
- w has $\ell k^2 = F$ votes while everyone else has $\leqslant F-1$ votes. Hence, w wins.

Proof of Reduction

Reverse Direction:

- Attacker has strategy $\mathcal{Z}$ s.t $|\mathcal{Z}| \leqslant B_{\mathcal{A}} = k^2$.
- Observe that max score possible for w is $\ell k^2 = F$
- $\mathcal{R}_i's$ must lose at least 1 vote, as they have F votes and are above w in order.
- There must be at least one primary district corresponding to a vertex from V_i, for all $i \in [k]$.
- Attacker is forced to manipulate in $k(k-1)$ secondary districts to drop the votes of candidates $\mathcal{R}_{ij}'s$ by 1.
- This completes the budget: k primary districts and $k(k-1)$ secondary districts.

Proof of Reduction

Reverse Direction:

- **Claim:** The selected districts must correspond to a multicolored clique in G.
- Let $\{v_1, \ldots v_k\}$ be the vertices whose corresponding primary district is attacked, $v_i \in V_i$.
- Suppose $(v_i, v_j) \notin E(G)$. Challenger candidates $\mathcal{R}_{ij}$ and $\mathcal{R}_{ji}$ force attack in secondary districts corresponding to edge with endpoints in V_i and V_j.
- Suppose $\mathcal{D}_{xy}$ was attacked, with $x \in V_i$ and $y \in V_j$ to reduce the votes of $\mathcal{R}_{ij}$.

Proof of Reduction

Reverse Direction:

- Suppose, wlog, $x \neq v_i$.
- It is required that c_x loses at least $k-1$ votes. But, c_x doesn't lose votes in primary districts, and it loses votes in atmost $k-2$ secondary districts, as it loses no votes in $\mathcal{D}_{xy}$.
- Score of c_x decreases by at most $k-2$.
- c_x has a clear chance of winning over w. Definitely, w doesn't win. **Contradiction!**

Other Results

- All FPT results for PV-Rec and PV-Man carry over to PD-Rec and PD-Man respectively.
- PD-Rec is W[1]-hard with defender budget as parameter. (Reduction from Multi-colored Clique)
- PD-Man is W[1]-hard with attacker budget as parameter. (Reduction from PD-Rec)

Future Work

- PV/PD-MAN parameterized by no. of districts.
- Identifying and working with structural parameters.
- Working with structured profiles like single-peakedness.

Questions?

References i

- Downey, R. G., and Fellows, M. R.
  Parameterized Complexity.
  Springer, 1999.
- Elkind, E., Gan, J., Obraztsova, S., Rabinovich, Z., and Voudouris, A. A.
  Protecting elections by recounting ballots.
  In *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI)* (2019), pp. 259–265.

References ii

Fellows, M. R., Hermelin, D., Rosamond, F. A., and Vialette, S.
On the parameterized complexity of multiple-interval graph problems.
Theor. Comput. Sci 410, 1 (2009), 53–61.

Pietrzak, K.
On the parameterized complexity of the fixed alphabet shortest common supersequence and longest common subsequence problems.
J. Comput. Syst. Sci 67, 4 (2003), 757–771.