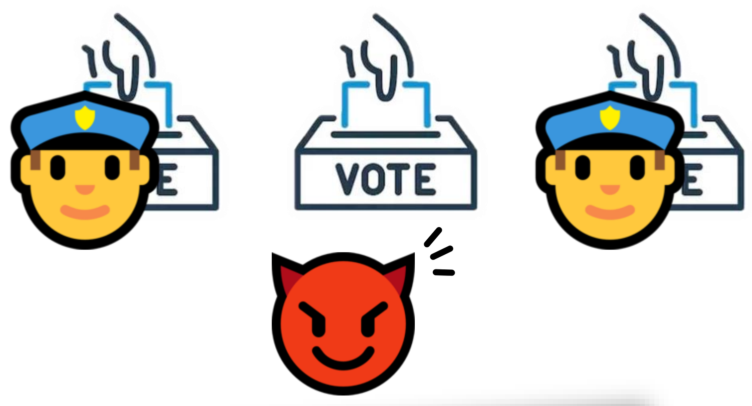
Protecting Elections by Recounting Ballots

Edith Elkind[1], Jiarui Gan[1], Svetlana Obraztsova[2], Zinovi Rabinovich[2], Alexandros A. Voudouris[1]

[1]*University of Oxford,* [2]*Nanyang Technological University*

Election & Election Frau

- Hack voting machine, manipulate demography, bribe voters, burn down polling station, **incorrectly count ballots**…
- Counteract incorrect counting:
  - Send observers to polling stations [Yin et al. 2016 & 2018; Li et al 2017; Chen et al 2018]
  - <u>Alternatively, **Recount ballots!**</u>
  - 👍 Second mover advantage



In the 2008 United States Senate election in Minnesota the Democratic candidate Al Franken won the seat after a recount revealed that 953 absentee ballots were wrongly rejected.

In the 2004 race for governor in Washington the Democratic candidate Gregoire was declared the winner after three consecutive recounts.

How to optimally recount using **limited** recounting resources?

How to optimally manipulate, given that defender will recount optimally?

A Complete View of Complexity

- Problem definitions

PV/PD-RECounting
Given a vote profile v, a distorted vote profile $\boldsymbol{v}$, a candidate $a \in C$, a budget B_D, district weights w_i, can defender recount B_D districts to get a elected?

PV/PD-MANipulation
Given a vote profile $\boldsymbol{v}$, a preferred candidate $p \in C$, a budget B_A, district weights w_i and number γ_i of votes that can be changed, can attacker manipulate B_A districts to get p elected (assuming defender will recount optimally)?

- Result overview

	PV	PD *unweighted*	PD *weighted*
REC	NP-c ③ NP-c Ⓤ $O(n^{m+2})$ (by DP)	P (reduct. to non-uniform bribery)	NP-c ③ NP-c Ⓤ $O(n^{m+2})$ (by DP)
MAN	NP-hard ③+⓪+∞ NP-hard Ⓤ+⓪+∞	NP-c Ⓤ	Σ_2^P-c ③ NP-h Ⓤ+⓪

Results with Ⓤ holds even when the input vote profile is given in unary (binary by default); with ③ hold even when there are only three candidates; with ⓪ hold even when the defender's budget is zero; with ∞ hold even when the attacker can change as many votes as she wants in every district. DP means Dynamic Programming.

A Stackelberg Game Model

- A set C of candidates, n voters in k disjoint districts $D_1, \dots, D_k$
- Two voting rules considered
  - **Plurality over Voters (PV),** 🏆 $a^* = \operatorname{argmax}_{a \in C} \sum_{i \in [k]} v_{ia}$
  - **Plurality over Districts (PD)**, weight w_i for each D_i

    🏆 $a^* = \operatorname{argmax}_{a \in C} \sum_{i \in [k]} w_i \cdot \mathbb{1}_{a = a_i^*}$, where $a_i^* = \operatorname{argmax}_{a \in C} v_{ia}$
- Tie-breaking rule: $\succ$

Attacker 😈 (leader)
- Can manipulate B_A districts
- Goal: make a favorite candidate $p \in C$ win
- Knows that the defender will recount optimally

VS

Defender 👮 (follower)
- Observes manipulated districts
- Can recount $B_D < B_A$ districts
- Goal: maximize social welfare:

  $\mathrm{SW}^{\mathrm{PV}}(a) = \sum_{i \in [k]} v_{ia}$

  $\mathrm{SW}^{\mathrm{PD}}(a) = \sum_{i \in [k]} w_i \cdot \mathbb{1}_{a = a_i^*}$

<u>Example</u>

- $C = \{a, b, p\}$, tie breaking: $p \succ a \succ b$
- 23 voters in 5 districts
- $B_D = 1, B_A = 2, \gamma_i = n_i$
- $w_i = (n_i)^2$

👉 No winning manip. under **PV**
👉 Winning under **PD**: $\{D_1, D_2\}$

	a🏆	b	p⭐
D_1	7	0	0
D_2	7	0	0
D_3	0	3	0
D_4	0	3	0
D_5	0	3	0
$\mathrm{SW}^{\mathrm{PV}}$	14	9	0
$\mathrm{SW}^{\mathrm{PD}}$	98	27	0

Regular Manipulation (RM)

A manipulation strategy is said to be *regular* if:
- **PV**: votes are transferred only **from other candidates to** p (the attacker's preferred candidate)
- **PD**: no candidate other than p is made the winner in manipulated districts

- Is RM w.l.o.g.? (Why transfer votes to others?) 😈 No!

<u>Example:</u> when no optimal manipulation is RM

- $C = \{a, b, p\}$, tie breaking: $p \succ a \succ b$
- $B_D = 1, B_A = 2, \gamma_i = n_i$
- $w_i = n_i$

👉 RM cannot win: $\mathrm{SW}(a) \geq 8$ and $\mathrm{SW}(p) \leq 7$ after recounting
👉 A winning non-RM: D_1: $p \to b$, and D_2: $a \to p$

	a🏆	b	p⭐
D_1	0	0 ⟵	6
D_2	3 ⟶	0	0
$D_3, \dots, D_8$	1	0	0
$D_9, \dots, D_{12}$	0	1	0
$\mathrm{SW}^{\mathrm{PV/PD}}$	9	4	6

- RM complexity results

	PV-RM	PD-RM
REC	Inapprox. in ½ + ϵ unless P=NP ③, but ½-approx. via Greedy	
MAN	NP-c ③ NP-c Ⓤ	P

Presented at IJCAI'19, Macao