Jak uratować demokrację

(wykład apolityczny)

Wojciech Jamroga

Instytut Podstaw Informatyki, Polska Akademia Nauk

Seminarium instytutowe, 9.01.2017

Weryfikacja modelowa własności bezpieczeństwa procedur wyborczych w logice temporalnej czasu alternującego z elementem epistemicznym

Wojciech Jamroga

Instytut Podstaw Informatyki, Polska Akademia Nauk

Seminarium instytutowe, 9.01.2017

Outline

Outline

Demokracja a technologie informatyczne

- **Demokracja**: forma sprawowania władzy, oparta o wolę większości obywateli $\leadsto$ wybory i głosowanie
- Reprezentatywność wyniku wyborów

Demokracja a technologie informatyczne

- **Demokracja**: forma sprawowania władzy, oparta o wolę większości obywateli $\leadsto$ wybory i głosowanie
- Reprezentatywność wyniku wyborów
- Krótka historia: prawa wyborcze, anonimowość wyborów cf. UK 1872 / Egipt 2010, różne procedury wyborcze

Krótka historia procedur wyborczych

Demokracja a technologie informatyczne

Zagrożenia dla reprezentatywności wyniku wyborów:

- Manipulacja i fałszowanie
- Niedbałość w realizacji procesu wyborczego (np. liczeniu głosów)
- Kupowanie głosów i przymuszanie wyborców
- Ograniczony dostęp do wyborów

Demokracja a technologie informatyczne

- Zagrożenia: rosną czy maleją przy użyciu technologii IT?

Demokracja a technologie informatyczne

- Zagrożenia: rosną czy maleją przy użyciu technologii IT?
- Głosowanie elektroniczne vs. głosowanie wspomagane elektronicznie

Demokracja a technologie informatyczne

- Zagrożenia: rosną czy maleją przy użyciu technologii IT?
- Głosowanie elektroniczne vs. głosowanie wspomagane elektronicznie
- Korzyści z użycia technologii informatycznych:
  - ułatwienia w dostępie
  - szybkość działania
  - nowe techniki zapewniania anonimowości
  - możliwości w zakresie walidacji wyniku
  - metody formalne w projektowaniu i analizie systemów
    $\rightsquigarrow$ specyfikacja, modelowanie, weryfikacja

Demokracja a technologie informatyczne

- Zagrożenia: rosną czy maleją przy użyciu technologii IT?
- Głosowanie elektroniczne vs. głosowanie wspomagane elektronicznie
- Korzyści z użycia technologii informatycznych:
  - ułatwienia w dostępie
  - szybkość działania
  - nowe techniki zapewniania anonimowości
  - możliwości w zakresie walidacji wyniku
  - metody formalne w projektowaniu i analizie systemów
    $\rightsquigarrow$ **specyfikacja, modelowanie, weryfikacja**

Outline

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie
- Anonimowość wyborcza: tylko wyborca wie, jak naprawdę zagłosował

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie
- Anonimowość wyborcza: tylko wyborca wie, jak naprawdę zagłosował (a właściwie po co nam to?)

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie
- Anonimowość wyborcza: tylko wyborca wie, jak naprawdę zagłosował (a właściwie po co nam to?)
- Odporność na kupowanie głosów i przymuszanie

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie
- Anonimowość wyborcza: tylko wyborca wie, jak naprawdę zagłosował (a właściwie po co nam to?)
- Odporność na kupowanie głosów i przymuszanie
- Sprawdzalność: wyborca ma możliwość sprawdzenia, czy jego głos został zarejestrowany i policzony prawidłowo

Własności procedur wyborczych

Aby wybierane gremia odzwierciedlały rozkład opinii i preferencji w społeczeństwie, system wyborczy powinien spełniać pewne podstawowe własności:

- Integralność wyniku: wynik wyborów wynika z sumy rzeczywiście złożonych głosów
  $\rightsquigarrow$ manipulacje kartami do głosowania i błędy w liczeniu
- Tajność głosu: karty do głosowania są wypełniane i składane tajnie
- Anonimowość wyborcza: tylko wyborca wie, jak naprawdę zagłosował (a właściwie po co nam to?)
- Odporność na kupowanie głosów i przymuszanie
- Sprawdzalność: wyborca ma możliwość sprawdzenia, czy jego głos został zarejestrowany i policzony prawidłowo

Jak specyfikować te własności? $\rightsquigarrow$ **logiki dla gier i strategii**

Logika strategiczna ATL

Logika strategiczna ATL

- ATL: logika temporalna czasu alternującego (koszmarna nazwa)
- Główny konstrukt: modalności strategiczne

Logika strategiczna ATL

- ATL: logika temporalna czasu alternującego (koszmarna nazwa)
- Główny konstrukt: modalności strategiczne

$\langle\langle A \rangle\rangle \varphi$: grupa agentów A ma wspólną strategię żeby osiągnąć φ

Logika strategiczna ATL

- ATL: logika temporalna czasu alternującego (koszmarna nazwa)
- Główny konstrukt: modalności strategiczne

$\langle\langle A \rangle\rangle \varphi$: grupa agentów A ma wspólną strategię żeby osiągnąć φ

$\rightsquigarrow$ φ zawiera 1 lub więcej operatorów temporalnych: X (w następnej chwili), F (kiedyś w przyszłości), G (zawsze w przyszłości), U (dopóki nie zajdzie określony warunek), itp.

Logika strategiczna ATL: przykłady

- $\langle\langle jamesbond \rangle\rangle \mathrm{F}\,(\mathsf{ski} \wedge \neg \mathsf{getBurned})$:
  "James Bond może wybrać się na narty i nie spłonąć"

Logika strategiczna ATL: przykłady

- $\langle\langle jamesbond \rangle\rangle \mathrm{F}\,(\mathsf{ski} \wedge \neg \mathsf{getBurned})$:
  "James Bond może wybrać się na narty i nie spłonąć"

Logika strategiczna ATL: przykłady

- $\langle\langle jamesbond \rangle\rangle \mathrm{F}\,(\mathsf{ski} \wedge \neg \mathsf{getBurned})$:
  "James Bond może wybrać się na narty i nie spłonąć"

- $\langle\langle jamesbond, bondsgirl \rangle\rangle \mathsf{fun}\ \mathrm{U}\ \mathsf{shot}$:
  "Agent 007 i jego dziewczyna mają strategię, by dobrze się bawić dopóki ktoś nie zacznie do nich strzelać"

Specyfikacja odporności na przymuszanie

Specyfikacja odporności na przymuszanie

For a voting system to be uncoercable, no voter should be able to convince any other participant of the value of its vote.

Specyfikacja odporności na przymuszanie

For a voting system to be uncoercable, no voter should be able to convince any other participant of the value of its vote.

$$\bigwedge_{v \in V} \bigwedge_{\substack{a \in \mathbb{A}\mathrm{gt} \\ v \neq a}} \bigwedge_{i \in Bal} \neg \langle\!\langle v \rangle\!\rangle \mathrm{F} \left(\mathsf{voted}_{\mathsf{v,i}} \wedge K_a \mathsf{voted}_{\mathsf{v,i}} \right).$$

Specyfikacja odporności na przymuszanie

An election protocol is receipt-free if a voter v cannot prove to a potential coercer c that she voted in a particular way. We assume that v wishes to cooperate with c; receipt-freeness guarantees that such cooperation will not be worthwhile, because it will be impossible for C to obtain proof about how A voted.

Specyfikacja odporności na przymuszanie

An election protocol is receipt-free if a voter v cannot prove to a potential coercer c that she voted in a particular way. We assume that v wishes to cooperate with c; receipt-freeness guarantees that such cooperation will not be worthwhile, because it will be impossible for C to obtain proof about how A voted.

$$\bigwedge_{v \in V \setminus \{c\}} \bigwedge_{i \in Bal} \neg \langle\langle c, v \rangle\rangle \mathrm{F} \left(\mathsf{voted_{v,i}} \wedge K_c \mathsf{voted_{v,i}} \right).$$

Specyfikacja odporności na przymuszanie

A voting system is coercion resistant, if there exists a counter-strategy for the voter such that the coercer cannot tell whether the coerced voter is in fact following the coercer's instructions or whether she is just running the counter-strategy, and hence, achieves her own goal.

Specyfikacja odporności na przymuszanie

A voting system is coercion resistant, if there exists a counter-strategy for the voter such that the coercer cannot tell whether the coerced voter is in fact following the coercer's instructions or whether she is just running the counter-strategy, and hence, achieves her own goal.

$$\bigwedge_{v \in V \setminus \{c\}} \bigwedge_{\substack{i,j \in Bal \\ i \neq j}} \langle\langle v \rangle\rangle \mathrm{F}\,(\mathsf{voted}_{\mathsf{v,i}} \wedge \mathrm{G}\,\neg K_c \neg \mathsf{voted}_{\mathsf{v,j}}).$$

Outline

Sprawdzalność

- **Sprawdzalność głosu przez głosującego** (ang. ***end-to-end voter verifiability***): wyborca ma możliwość sprawdzenia, czy jego głos został zarejestrowany i policzony prawidłowo
- Pozwala wykrywać nieprawidłowości niezależnie od ich źródła!
- Może pozwolić na zakwestionowanie nieprawidłowego wyniku wyborów (jeśli wyborca otrzymał jakiś dowód swego głosu)

Sprawdzalność

- **Sprawdzalność głosu przez głosującego** (ang. ***end-to-end voter verifiability***): wyborca ma możliwość sprawdzenia, czy jego głos został zarejestrowany i policzony prawidłowo
- Pozwala wykrywać nieprawidłowości niezależnie od ich źródła!
- Może pozwolić na zakwestionowanie nieprawidłowego wyniku wyborów (jeśli wyborca otrzymał jakiś dowód swego głosu)
- Historie motywujące: głosowanie internetowe w Estonii, polskie wybory samorządowe 2014

Głosowanie elektroniczne w Estonii

Polskie wybory samorządowe 2014

Sprawdzalność przez głosującego

Problem: jak pogodzić sprawdzalność i odporność na przymuszanie?

Sprawdzalność przez głosującego

Problem: jak pogodzić sprawdzalność i odporność na przymuszanie?

- ThreeBallot
- Pret-a-Voter
- Selene

Sprawdzalność przez głosującego

Problem: jak pogodzić sprawdzalność i odporność na przymuszanie?

- ThreeBallot
- **Pret-a-Voter**
- Selene

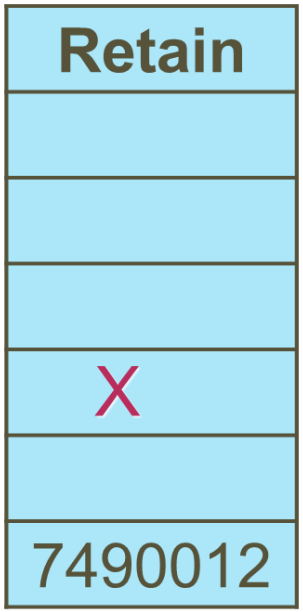
Sprawdzalność w protokole Pret-a-Voter

Destroy	Retain
Asterix	
Obelix	
Idefix	
Panoramix	
Abraroucourix	
	7490012

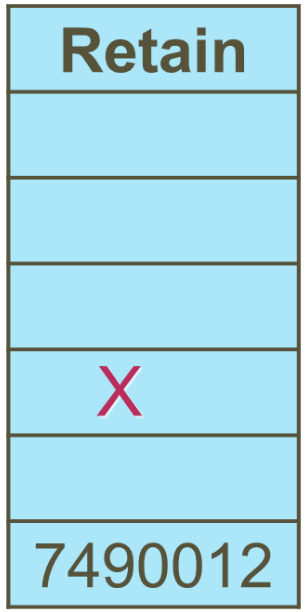
Sprawdzalność w protokole Pret-a-Voter

Destroy	Retain
Asterix	
Obelix	
Idefix	
Panoramix	X
Abraroucourix	
	7490012

Sprawdzalność w protokole Pret-a-Voter



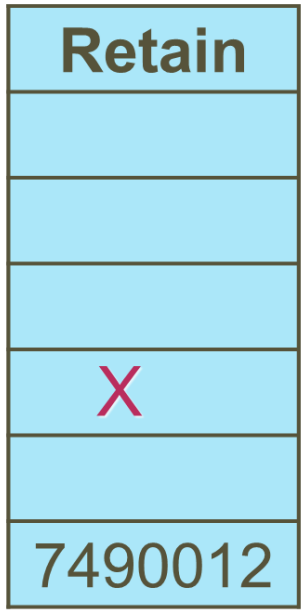
Sprawdzalność w protokole Pret-a-Voter



Specyfikacja sprawdzalności w logice ATL:

$$\bigwedge_{i \in Bal} (\mathsf{voted}_{\mathsf{v,i}} \wedge \mathsf{resultsPublished}) \rightarrow \langle\langle v \rangle\rangle \mathrm{F}\, (K_v \mathsf{registered}_{\mathsf{v,i}} \vee K_v \neg \mathsf{registered}_{\mathsf{v,i}}).$$

Sprawdzalność w protokole Pret-a-Voter



Specyfikacja sprawdzalności w logice ATL:

$$\bigwedge_{i \in Bal} (\mathsf{voted}_{\mathsf{v,i}} \wedge \mathsf{resultsPublished}) \rightarrow \langle\langle v \rangle\rangle \mathrm{F}\, (K_v \mathsf{registered}_{\mathsf{v,i}} \vee K_v \neg \mathsf{registered}_{\mathsf{v,i}}).$$

A może by tak **automatycznie sprawdzić sprawdzalność**?

Outline

Weryfikacja modelowa własności strategicznych

- **Weryfikacja modelowa** (ang. *model checking*): najbardziej znana metoda automatycznej weryfikacji

Weryfikacja modelowa własności strategicznych

- **Weryfikacja modelowa** (ang. *model checking*): najbardziej znana metoda automatycznej weryfikacji
- Stosowana do weryfikacji poprawności oprogramowania i sprzętu

Weryfikacja modelowa własności strategicznych

- **Weryfikacja modelowa** (ang. *model checking*): najbardziej znana metoda automatycznej weryfikacji
- Stosowana do weryfikacji poprawności oprogramowania i sprzętu
- ...wykrywania błędów

Weryfikacja modelowa własności strategicznych

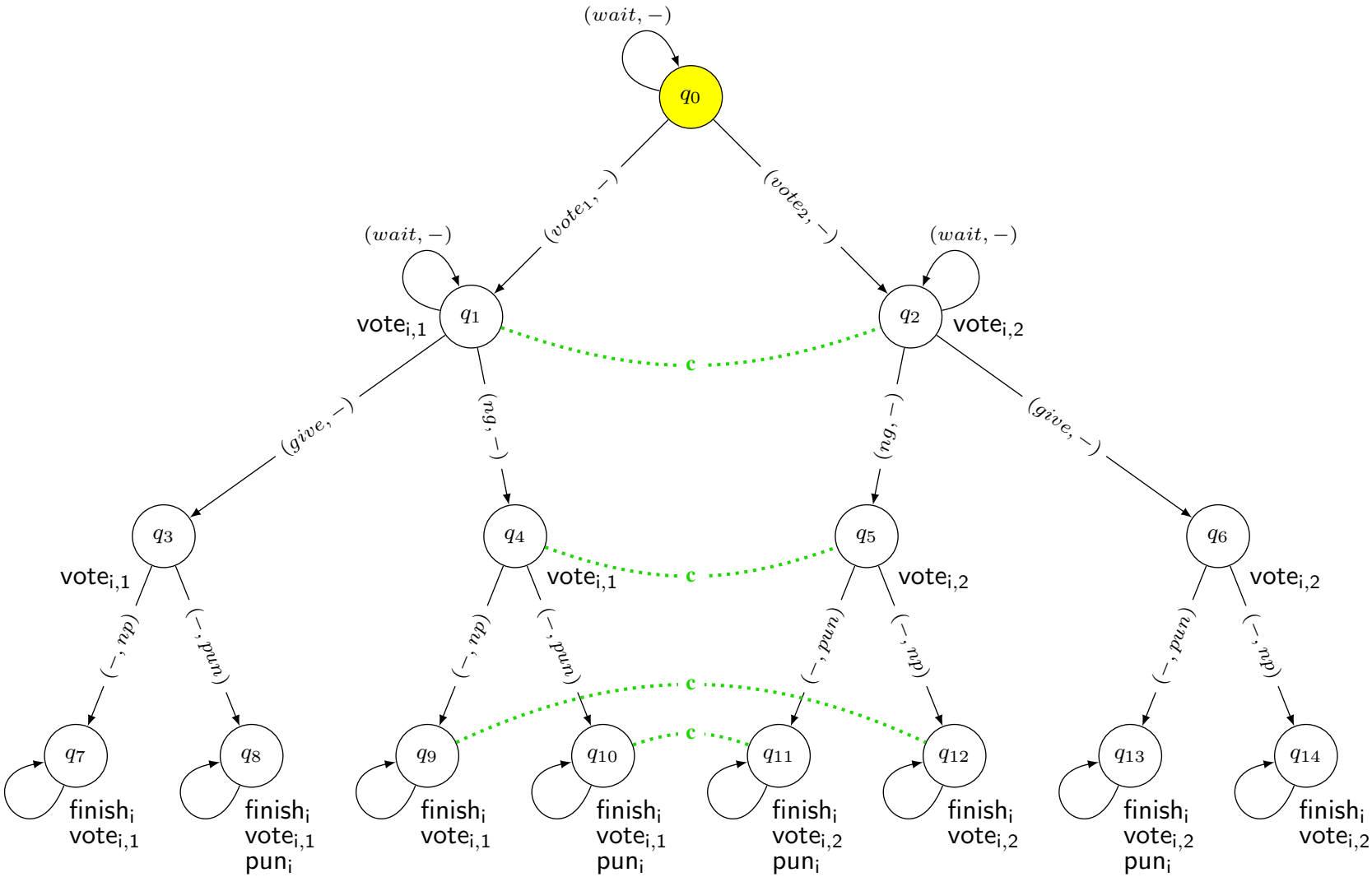
- **Weryfikacja modelowa** (ang. *model checking*): najbardziej znana metoda automatycznej weryfikacji
- Stosowana do weryfikacji poprawności oprogramowania i sprzętu
- ...wykrywania błędów
- ...a nawet automatycznego planowania

Weryfikacja modelowa własności strategicznych

- **Weryfikacja modelowa** (ang. *model checking*): najbardziej znana metoda automatycznej weryfikacji
- Stosowana do weryfikacji poprawności oprogramowania i sprzętu
- ...wykrywania błędów
- ...a nawet automatycznego planowania
- Idea: dany jest model systemu (graf, program, schemat blokowy) oraz formuła logiczna opisująca poprawne działanie systemu
- Algorytm weryfikacji zwraca odpowiedź:

  TAK jeśli ta formuła jest spełniona w danym modelu,
  NIE w przeciwnym przypadku.

Prosty model głosowania



Weryfikacja modelowa własności strategicznych

Weryfikacja modelowa własności strategicznych

- Problem: weryfikacja własności temporalnych jest kosztowna obliczeniowo

Weryfikacja modelowa własności strategicznych

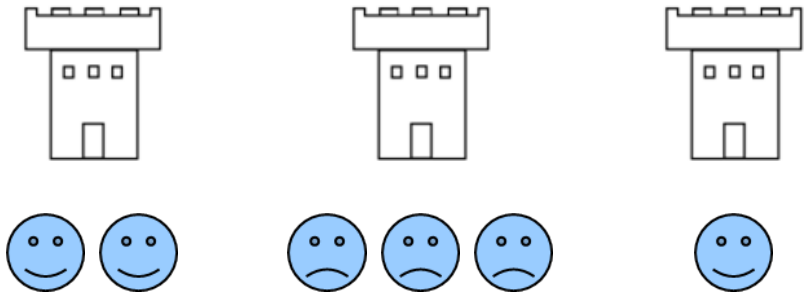
- Problem: weryfikacja własności temporalnych jest kosztowna obliczeniowo
- ...weryfikacja istnienia strategii jest **bardzo kosztowna obliczeniowo**

Weryfikacja modelowa własności strategicznych

- Problem: weryfikacja własności temporalnych jest kosztowna obliczeniowo
- ...weryfikacja istnienia strategii jest **bardzo kosztowna obliczeniowo**
- ...a dla strategii z niepełną informacją jeszcze bardziej 

Weryfikacja modelowa własności strategicznych

- Problem: weryfikacja własności temporalnych jest kosztowna obliczeniowo
- ...weryfikacja istnienia strategii jest **bardzo kosztowna obliczeniowo**
- ...a dla strategii z niepełną informacją jeszcze bardziej 
- Jak bardzo? Sprawdzimy to eksperymentalnie na prostej klasie modeli $\rightsquigarrow$ Castles



Wyniki eksperymentów

N	czas łączny	1. krok	2. krok	zajętość pamięci
4 (1 1 1)	130	100	29	15
5 (1 1 2)	6 686	336	6 349	198
6 (2 1 2)	4 508	548	3 957	606
7 (2 2 2)	3 366	2 637	728	77
8 (3 2 2)	255 549	27 040	228 505	454

Formuła: $\langle\langle c12 \rangle\rangle \mathrm{F}\,\mathsf{castle3Defeated}$

Czas podano w ms, zajętość pamięci w MB

Porównanie dla strategii z pełną i niepełną informacją

N	pełna informacja (MCMAS)	niepełna informacja (SMC)	niepełna informacja (MCMAS)
4 (1 1 1)	43	130	72 000
5 (1 1 2)	70	6 686	timeout
6 (2 1 2)	250	4 508	timeout
7 (2 2 2)	954	3 366	timeout
8 (3 2 2)	1 996	255 549	timeout

Formuła: $\langle\langle c12 \rangle\rangle \mathrm{F}$ castle3Defeated

Czas w ms, timeout = 2h

Outline

Przybliżona weryfikacja własności strategicznych

- Idealna weryfikacja dla niepełnej informacji jest bardzo trudna obliczeniowo
- Pomysł: spróbujmy znaleźć formuły, które przybliżają prawdziwość zadanej specyfikacji z góry i z dołu

Przybliżona weryfikacja własności strategicznych

- Idealna weryfikacja dla niepełnej informacji jest bardzo trudna obliczeniowo
- Pomysł: spróbujmy znaleźć formuły, które przybliżają prawdziwość zadanej specyfikacji z góry i z dołu
- ...i które łatwiej się liczy 

Przybliżona weryfikacja własności strategicznych

- Idealna weryfikacja dla niepełnej informacji jest bardzo trudna obliczeniowo
- Pomysł: spróbujmy znaleźć formuły, które przybliżają prawdziwość zadanej specyfikacji z góry i z dołu
- ...i które łatwiej się liczy 
- Jeśli **górna aproksymacja = dolna aproksymacja**, dostajemy dokładny wynik!

Przybliżona weryfikacja własności strategicznych

Z ostatniej chwili...

$$
\begin{aligned}
&tr(p) = p,\\
&tr(\neg\phi) = \neg TR(\phi),\\
&tr(\phi \wedge \psi) = tr(\phi) \wedge tr(\psi),\\
&tr(\langle A\rangle\phi) = \langle A\rangle tr(\phi),\\
&tr(\langle\!\langle A\rangle\!\rangle \mathrm{G}\,\phi) = \nu Z.(C_A tr(\phi) \wedge \langle A\rangle^{\bullet} Z),\\
&tr(\langle\!\langle A\rangle\!\rangle \psi\,\mathrm{U}\,\phi) = \mu Z.\big(E_A tr(\phi) \vee (C_A tr(\psi) \wedge \langle A\rangle^{\bullet} Z)\big).
\end{aligned}
$$

$$
\begin{aligned}
&TR(p) = p,\\
&TR(\neg\phi) = \neg tr(\phi),\\
&TR(\phi \wedge \psi) = TR(\phi) \wedge TR(\psi),\\
&TR(\langle A\rangle\phi) = E_A \langle\!\langle A\rangle\!\rangle_{\mathrm{Ir}} \mathrm{X}\; TR(\phi),\\
&TR(\langle\!\langle A\rangle\!\rangle \mathrm{G}\,\phi) = E_A \langle\!\langle A\rangle\!\rangle_{\mathrm{Ir}} \mathrm{G}\; TR(\phi),\\
&TR(\langle\!\langle A\rangle\!\rangle \psi\,\mathrm{U}\,\phi) = E_A \langle\!\langle A\rangle\!\rangle_{\mathrm{Ir}}\; TR(\psi)\,\mathrm{U}\; TR(\phi).
\end{aligned}
$$

Przybliżona weryfikacja własności strategicznych

- Aproksymacje działają tylko w części przypadków
- W szczególności, nasza aproksymacja działa tylko w modelach gdzie uczestnicy mają wystarczająco dobrą pamięć
- Na przykład, daje słabe wyniki w modelach Castles (agenci zbyt wiele zapominają...)

Przybliżona weryfikacja własności strategicznych

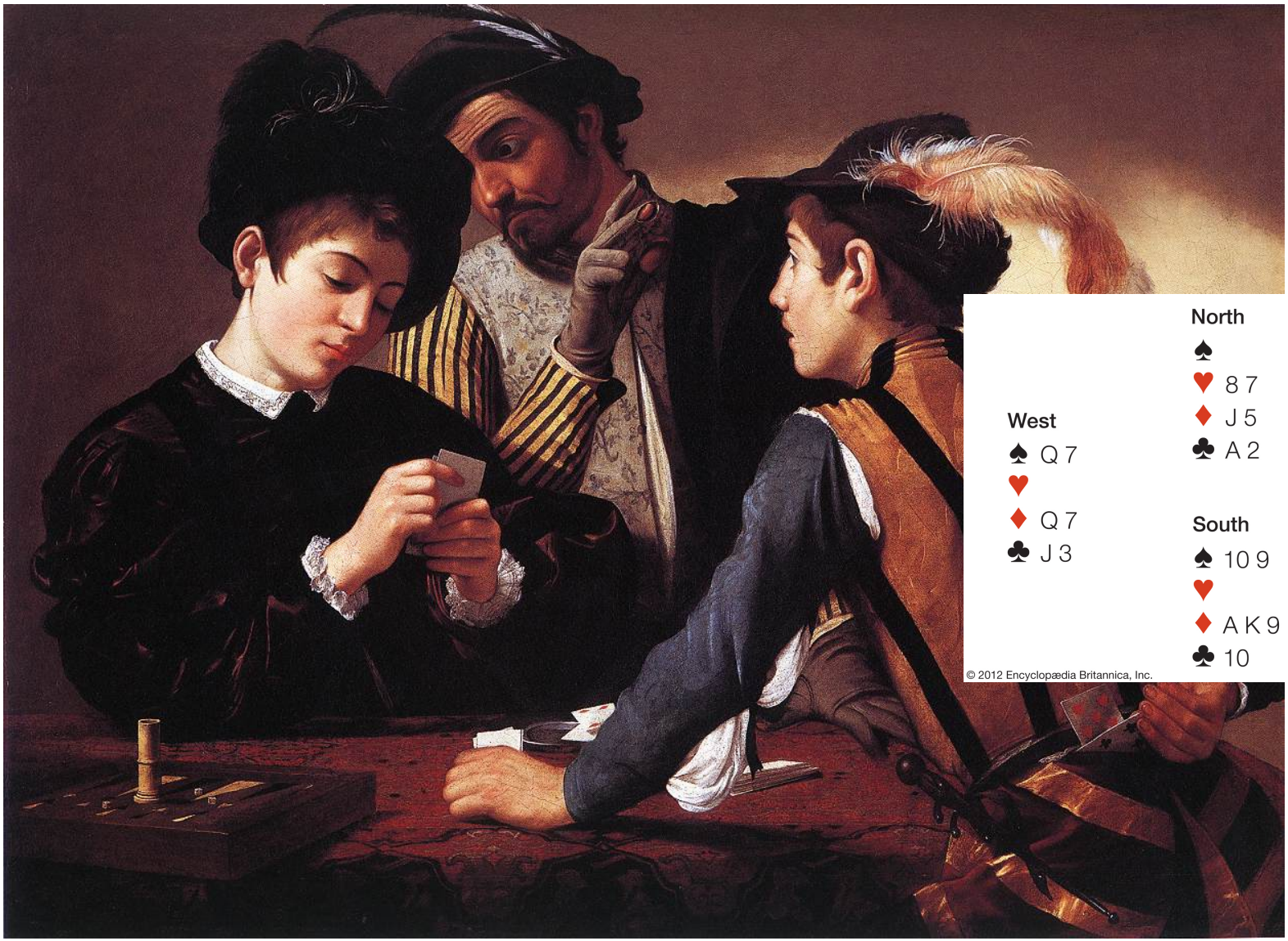
- Aproksymacje działają tylko w części przypadków
- W szczególności, nasza aproksymacja działa tylko w modelach gdzie uczestnicy mają wystarczająco dobrą pamięć
- Na przykład, daje słabe wyniki w modelach Castles (agenci zbyt wiele zapominają...)
- Jednakże w protokołach bezpieczeństwa zazwyczaj zakłada się, że **atakujący pamięta wszystkie istotne obserwacje**

Przybliżona weryfikacja własności strategicznych

- Aproksymacje działają tylko w części przypadków
- W szczególności, nasza aproksymacja działa tylko w modelach gdzie uczestnicy mają wystarczająco dobrą pamięć
- Na przykład, daje słabe wyniki w modelach Castles (agenci zbyt wiele zapominają...)
- Jednakże w protokołach bezpieczeństwa zazwyczaj zakłada się, że **atakujący pamięta wszystkie istotne obserwacje**
- Nowy benchmark: rozgrywka w grach karcianych (ma podobną strukturę matematyczną, co przymuszanie w protokole głosowania!)

Weryfikacja modelowa własności strategicznych

Weryfikacja modelowa własności strategicznych



Wyniki eksperymentów

Ilość kart	Weryfikacja przybliżona			Weryfikacja idealna
	z dołu	z góry	dokładność	
4	0.0001	7e-05	100%	0.14
8	0.002	0.001	100%	2.42 h
12	0.16	0.05	100%	timeout
16	172.07	2.61	100%	timeout
20	76 h	1929	100%	timeout

Formuła do weryfikacji: $\langle\langle \mathbf{S} \rangle\rangle \mathrm{F}\,\mathrm{win}$

Czas w sekundach, chyba że podano inaczej
timeout $\approx$ 45h

Wyniki eksperymentów dla roztargnionego rozgrywającego

Ilość kart	Weryfikacja przybliżona			Weryfikacja idealna
	z dołu	z góry	dokładność	
4	0.0003	0.0003	100%	14.59 h
8	0.01	0.02	90%	timeout
12	29.31	2.45	80%	timeout

Formuła do weryfikacji: $\langle\langle \mathbf{S} \rangle\rangle \mathrm{F}\,\mathrm{win}$

Czas w sekundach, chyba że podano inaczej
timeout $\approx$ 45h

Outline

Podsumowanie

- Żyjemy w czasach rosnących napięć wewnętrznych i międzynarodowych
- Zagrożenie dla demokracji: ingerencja poprzez manipulację wyborami

Podsumowanie

- Żyjemy w czasach rosnących napięć wewnętrznych i międzynarodowych
- Zagrożenie dla demokracji: ingerencja poprzez manipulację wyborami
- Technologie informatyczne otwierają szereg nowych zagrożeń
- ...ale pozwalają też skuteczniej wykrywać zagrożenia

Podsumowanie

- Żyjemy w czasach rosnących napięć wewnętrznych i międzynarodowych
- Zagrożenie dla demokracji: ingerencja poprzez manipulację wyborami
- Technologie informatyczne otwierają szereg nowych zagrożeń
- ...ale pozwalają też skuteczniej wykrywać zagrożenia
- Szczególnie obiecujące: protokoły sprawdzalnego głosowania

Podsumowanie

- Żyjemy w czasach rosnących napięć wewnętrznych i międzynarodowych
- Zagrożenie dla demokracji: ingerencja poprzez manipulację wyborami
- Technologie informatyczne otwierają szereg nowych zagrożeń
- ...ale pozwalają też skuteczniej wykrywać zagrożenia
- Szczególnie obiecujące: protokoły sprawdzalnego głosowania
- Projekt **VoteVerif**: specyfikacja, modelowanie i weryfikacja protokołów sprawdzalnego głosowania
- Współpraca pomiędzy IPIPAN, PJATK i Uniwersytetem Luksemburskim


Thank you