Hybrid Voting Protocols and Hardness of Manipulation

Edith Elkind, U. of Liverpool

Helger Lipmaa, UCL

Manipulation: Example

- 99 voters, 3 candidates (Red, Blue, Green).
  - 49 voters: R > B > G.
  - 48 voters: B > R > G.
  - 2 voters (Edith and Helger): G > B > R.
- Aggregation rule: Plurality
  - each voter casts a vote for one candidate.
  - the candidate with the largest number of votes wins.
  - draws are resolved by a coin toss.

What Will Edith and Helger Do?

R: 49 votes
B: 48 votes

G > B > R

If I vote for G, R will get elected, so I'd rather vote for B

If Edith and Helger vote B > G > R,
they can guarantee that B is elected

Why Manipulation Is Bad

- Aggregation rules are designed with certain social welfare criteria in mind.
- Misrepresentation of preferences results in a suboptimal choice w.r.t. these criteria.
- Encourages dishonesty…

What If We Change Aggregation Rule?

- Single Transferable Vote:

1st round

R > B > ~~G~~ 49 votes

B > R > ~~G~~ 48 votes

~~G~~ > B > R 2 votes

⇒

2nd round

R > B 49 votes

B > R 50 votes

⇒

B wins

Formal Setup

- n voters
- m candidates $c_1, \ldots, c_m$
- Preference of a voter i:
  a permutation π_i of $c_1, \ldots, c_m$
  (best to worst).
- Aggregation rule S:

$$\pi_1, \ldots, \pi_n \rightarrow c_j.$$

Voting Schemes: Examples

- Borda: a candidate gets
  - m points for each voter who ranks him 1st,
  - m-1 point for each voter who ranks him 2nd, etc.
- Copeland:
  - candidate that wins the largest # of pairwise elections
- Maximin:
  - c's score against d: # of voters that prefer c to d;
  - c's # of points: min score in any pairwise election.
- many, many others…

Voting Schemes: Properties

- Pareto-optimality: if everyone prefers a to b, b does not win
- Condorcet-consistency: if there is a candidate that wins every pairwise election, this candidate wins
- Majority: if there is a candidate that is ranked first by a majority of voters, this candidate wins
- Monotonicity: it is impossible to cause a winning candidate to lose by moving it up in one's vote

Arrow's theorem: there is no perfect scheme

Manipulation: Definition

- A voter i can manipulate a voting scheme S if there is
  - a preference vector

$$\pi = (\pi_1, \ldots, \pi_i, \ldots, \pi_n)$$

  - a permutation π_i' s.t.

$$S(\pi_1, \ldots, \pi_i', \ldots, \pi_n) >_i S(\pi).$$

Theorem (Gibbard-Satterthwaite, 1971): every non-dictatorial aggregation rule with ≥ 3 candidates is manipulable.

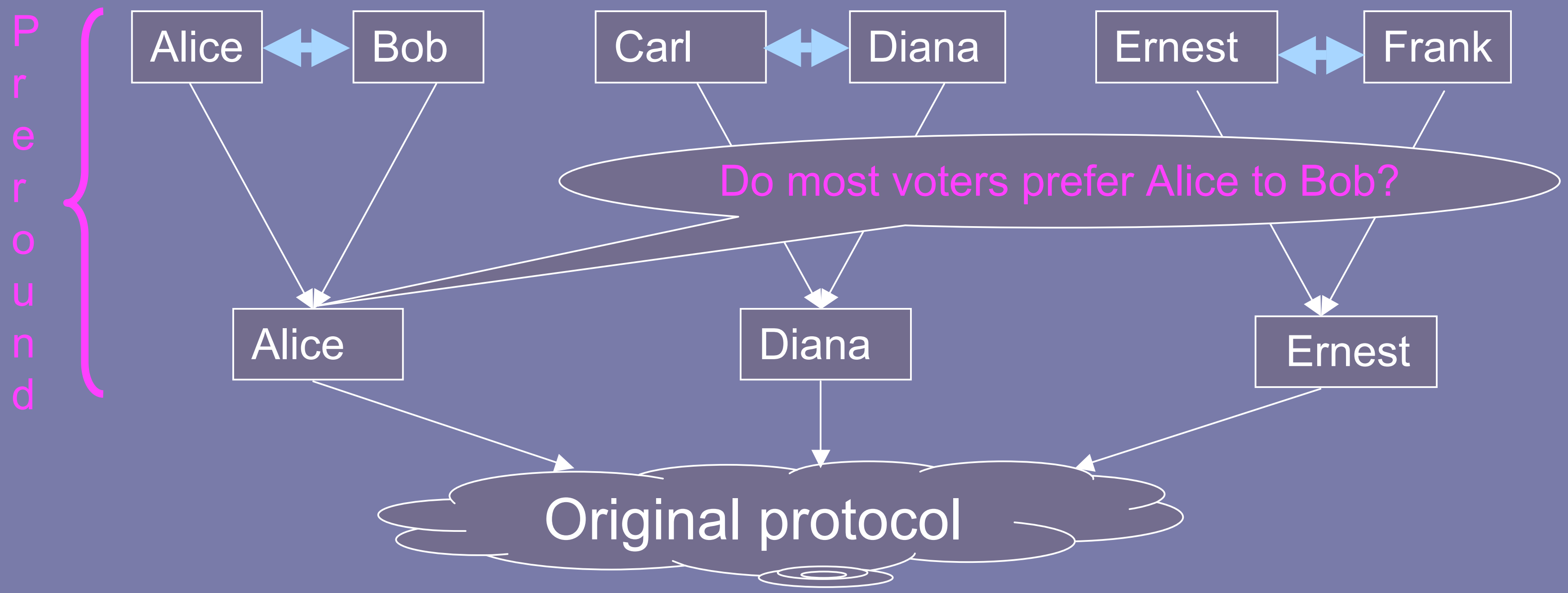
How Do We Get Around The Impossibility Result?

- We cannot make manipulation impossible…
- But we can try to make it hard!
- How do you manipulate Plurality?
  - vote for your favorite candidate among those tied for the top position.
- How do you manipulate Borda?
  - rank your favorite feasible candidate highest, move his competitors to the bottom of your vote.
- How do you manipulate STV?
  - try all m! possible ballots…

What Is Known?

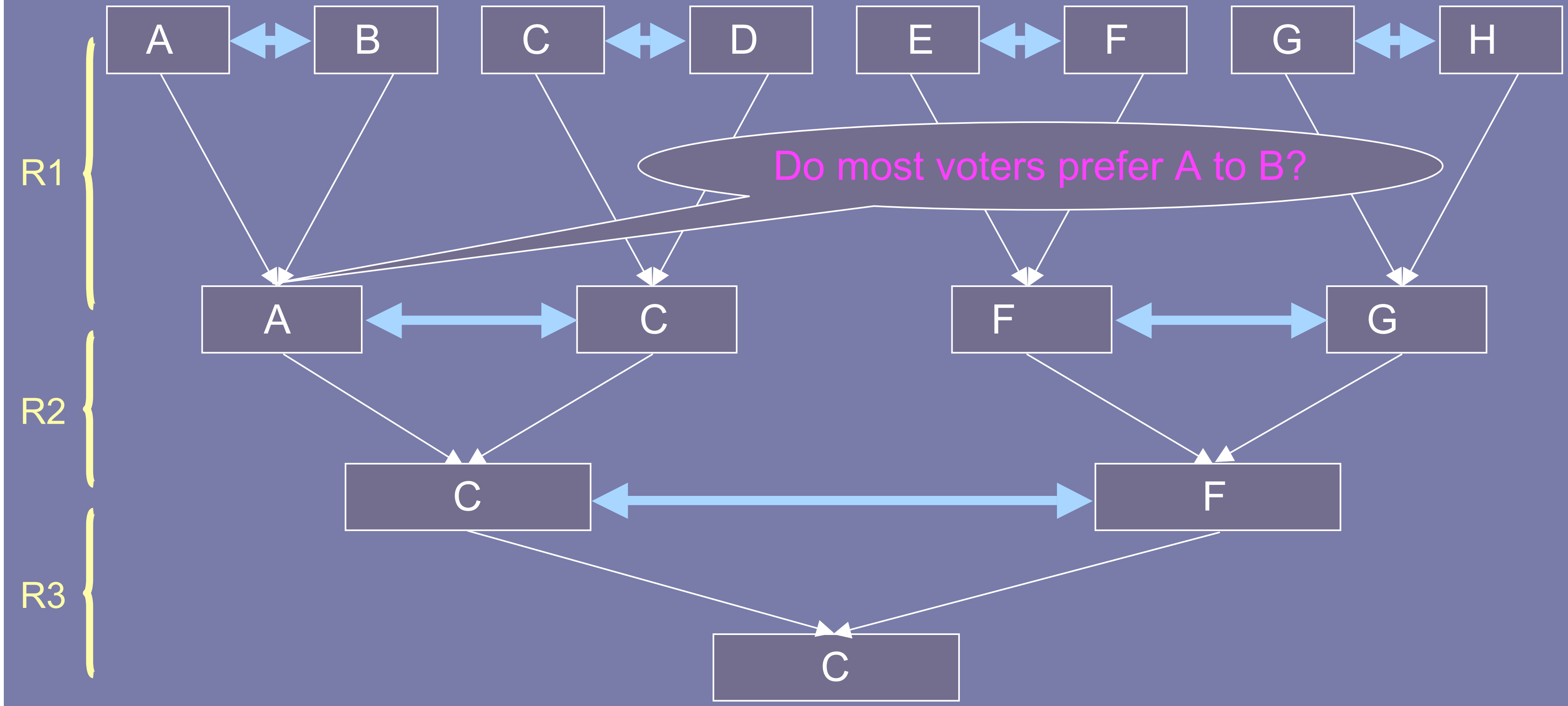
- 2nd order Copeland is NP-hard to manipulate (Bartholdi, Tovey, Trick 1989)
- STV is NP-hard to manipulate (Bartholdi, Orlin 1991)
- These rules may not reflect the welfare goals (why so many voting rules out there?)
- Want a universal method to turn any voting protocol into a hard-to-manipulate one.

Adding a Preround (Conitzer-Sandholm'03)



- Retains some of the flavor of the original protocol.
- Is NP-hard to manipulate for many base protocols.
- Still, the outcome may be very different from the original protocol…

Binary Cup



Binary Cup itself is easy to manipulate.

Our Work: Hybrid Protocols

- Protocols with a preround can be viewed as hybrids of BC and other protocols
  - how about other hybrids?
- Hyb(X_k, Y): execute k steps of X, then apply Y to the remaining candidates.
  - step: protocol-dependent
    - round of STV or BinaryCup
    - eliminating the lowest scoring candidate for Plurality, Borda
  - Hyb($Plurality_k$, Borda):
    - eliminate k candidates with the lowest Plurality scores
    - compute Borda scores w.r.t. survivors.

New Protocols

- Hyb(X_k, STV), Hyb(STV_k, Y) are NP-hard to manipulate (for any reasonable X, Y)
  - is Hyb(X_k, Y) non-manipulable for any X (or Y) that is non-manipulable?
- Hyb($Borda_k$, Plurality) is NP-hard to manipulate
- Hyb($Maximin_k$, Plurality) is NP-hard to manipulate

Hybrid of a Protocol with Itself

- Generally, Hyb(X_k, X) ≠ X
  – (and may be much harder to manipulate)
- Hyb($Plurality_k$, Plurality):
  – eliminate k lowest-scoring candidates
  – recompute the scores
  – select Plurality winner wrt new scores
- Hyb($Plurality_1$, …, $Plurality_m$) =
- Hyb($Borda_k$, Borda)
  is NP-hard to manipulate

Limitations and Extensions

- Is Hyb(X_k, Y) hard to manipulate for any X, Y?
  - NO: Hyb($Plurality_k$, Y) is almost as easy to manipulate as Y
- Utlity-based voting (voters rate candidates rather that rank them)
  - HighScore: the candidate with max total score wins
  - manipulating Hyb($HighScore_k$, HighScore) is NP-hard