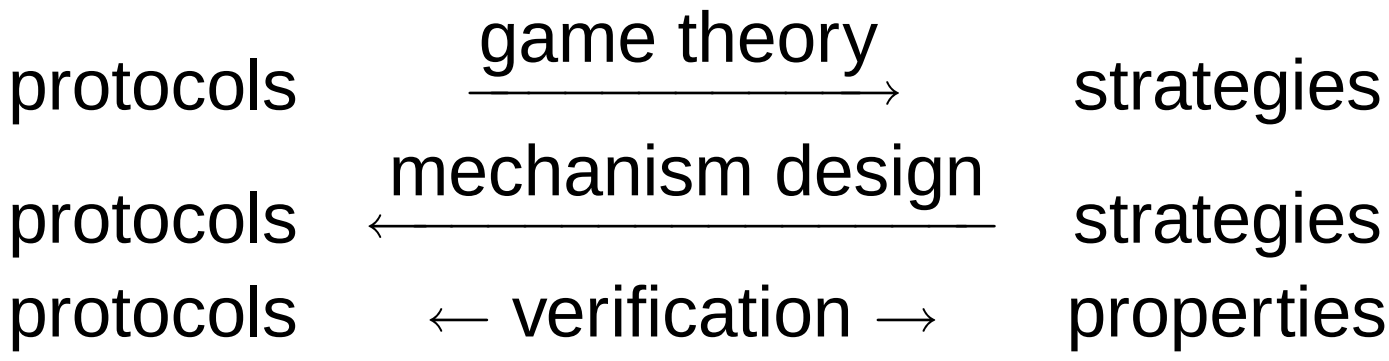
Games and Logic for Mechanism Verification

Sieuwert van Otterloo

sieuwert@csc.liv.ac.uk

Ljubljana, March 2005

Protocol Analysis



A Voting Problem

Three agents A, B and C have to jointly decide on either option x, y or z. They want to use a majority decides voting protocol.

$$M \models \Box(x \vee y \vee z)$$

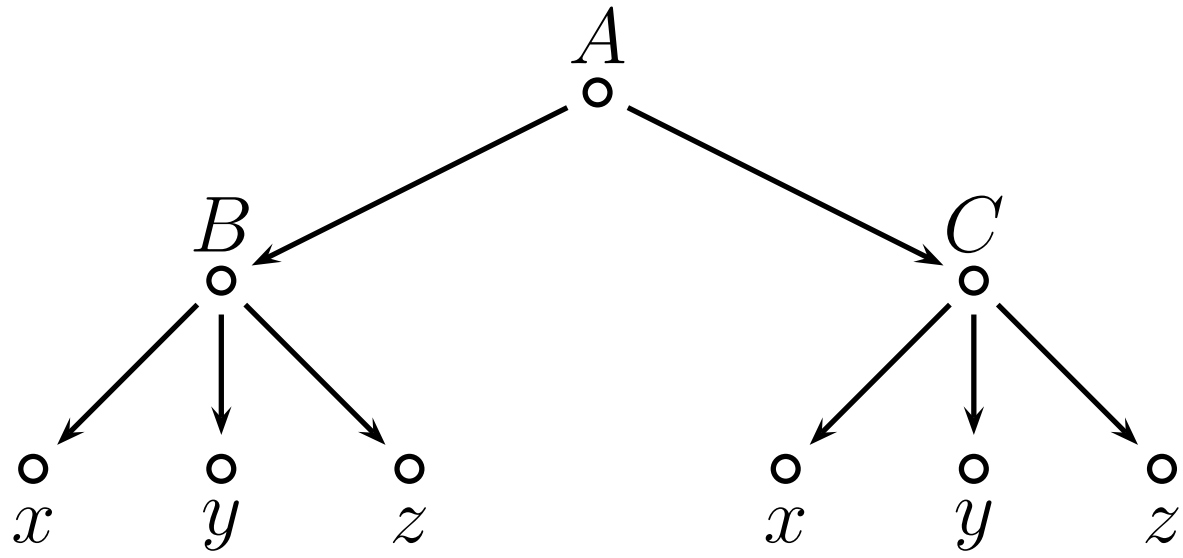
$$M \models \Box\neg((x \wedge y) \vee (x \wedge z) \vee (y \wedge z))$$

$$M \models [AB : x]\Box x$$

$$M \models [AC : x]\Box x$$

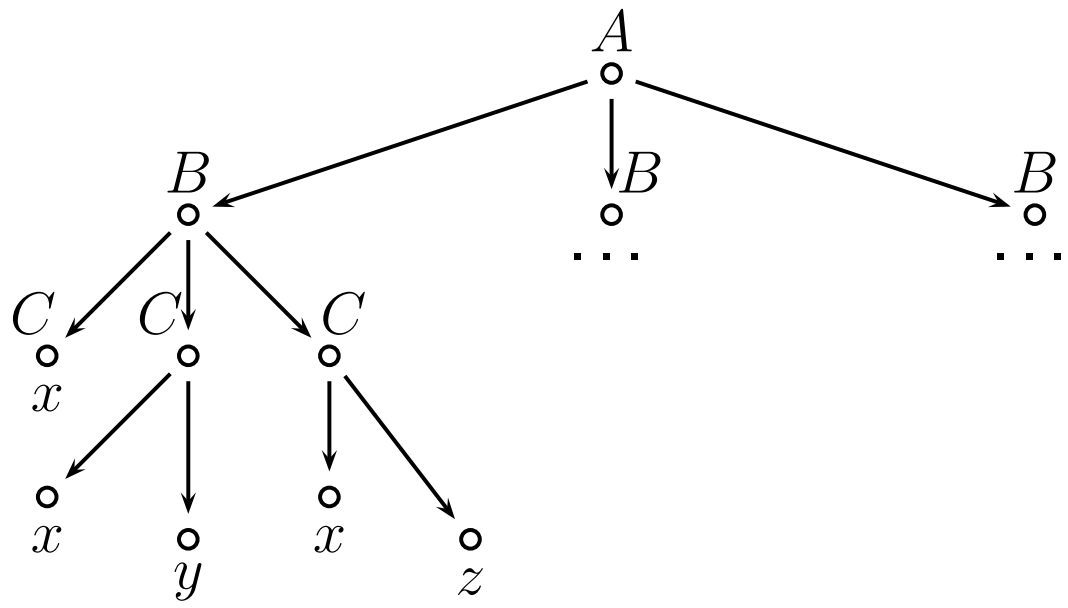
$$M \models [BC : x]\Box x$$

Solution 1



$$R_1^A = A \xrightarrow{X \in \{B,C\}} X \xrightarrow{p \in P} \{p\}$$

Solution 2



$$R_2^{ABC} = A \xrightarrow{a \in P} (B \xrightarrow{b \in P \setminus \{a\}} C \xrightarrow{c \in \{a,b\}} \{c\}) || (B \xrightarrow{a} \{a\})$$

Results

- There are logics that can differentiate these protocols
- Verification in polynomial time
- Linear notation is very compact

But

- Any protocol is unfair or biased
- Still hard to choose between protocols.

Future Challenges

Protocol verification is possible.

- Complete logics: mechanism design
- Soft approaches
- Adding knowledge