Cross Chain Swaps with Preferences

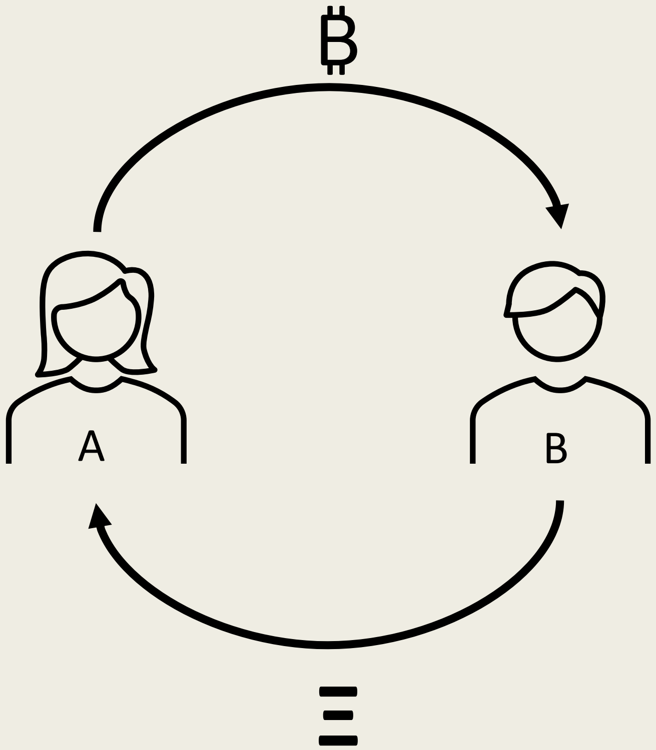
Eric Chan* Marek Chrobak Mohsen Lesani

University of California at Riverside, USA

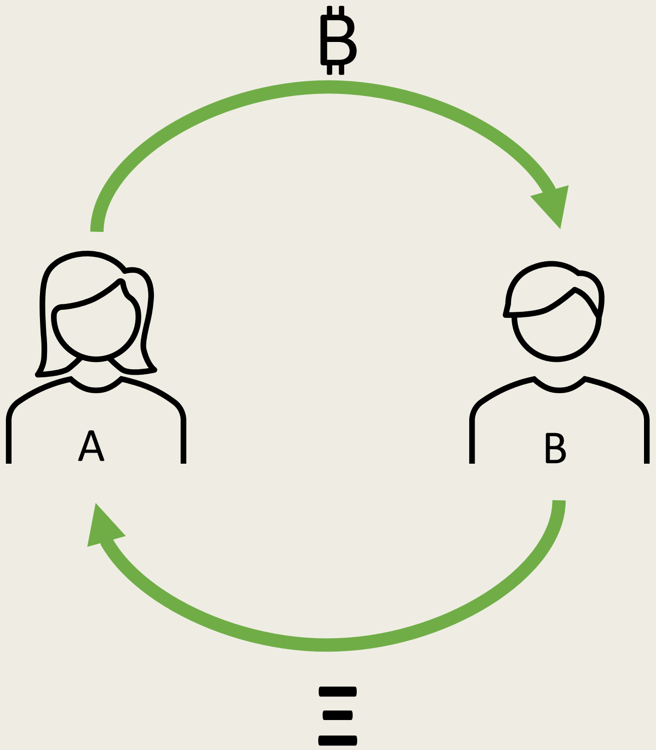
CSF 2023

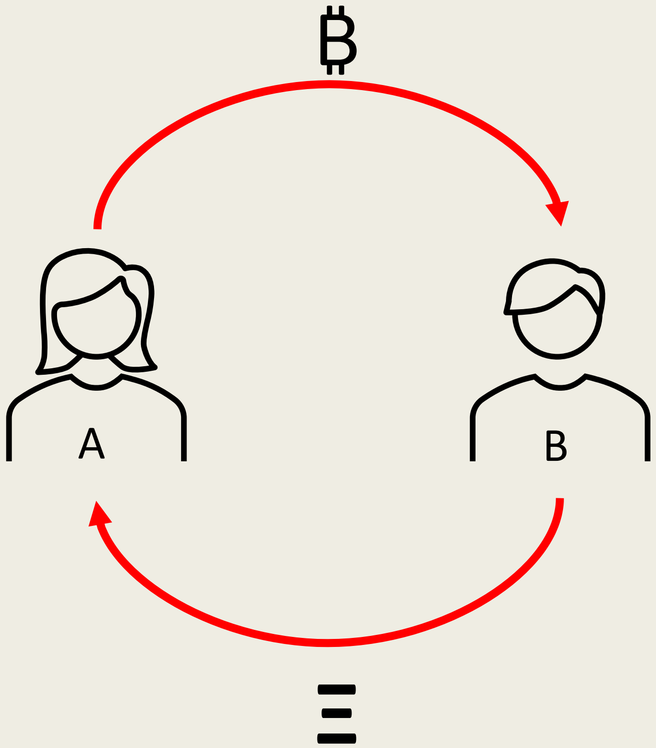
Cross Chain Swap

Cross Chain Swap

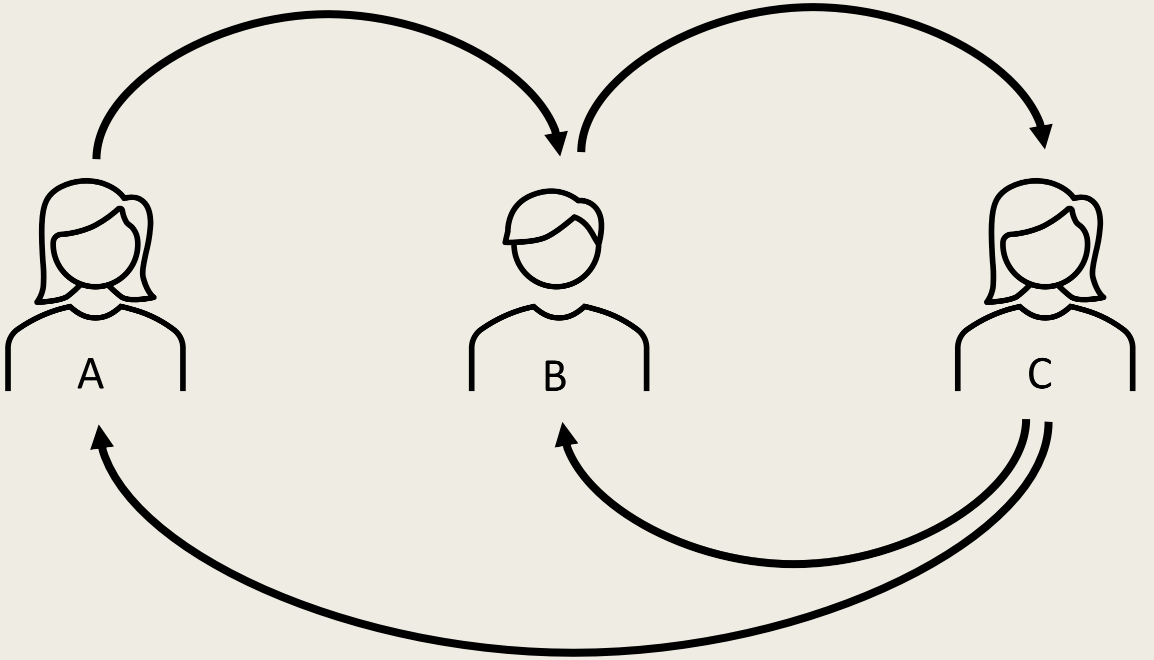


Cross Chain Swap – Fair Exchange



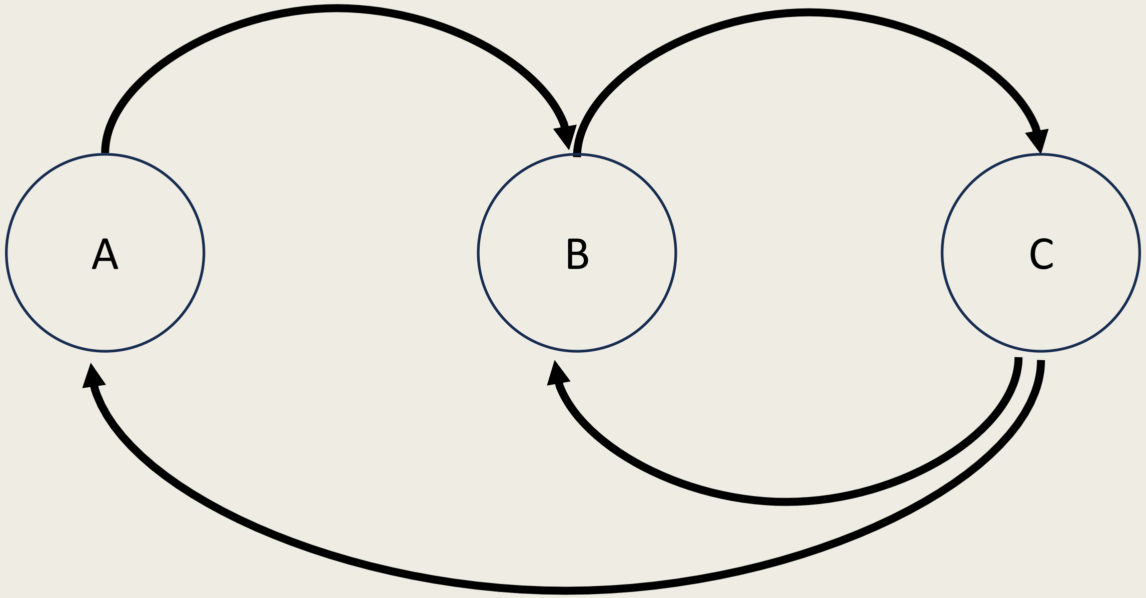


Cross Chain Swap – Fair Exchange

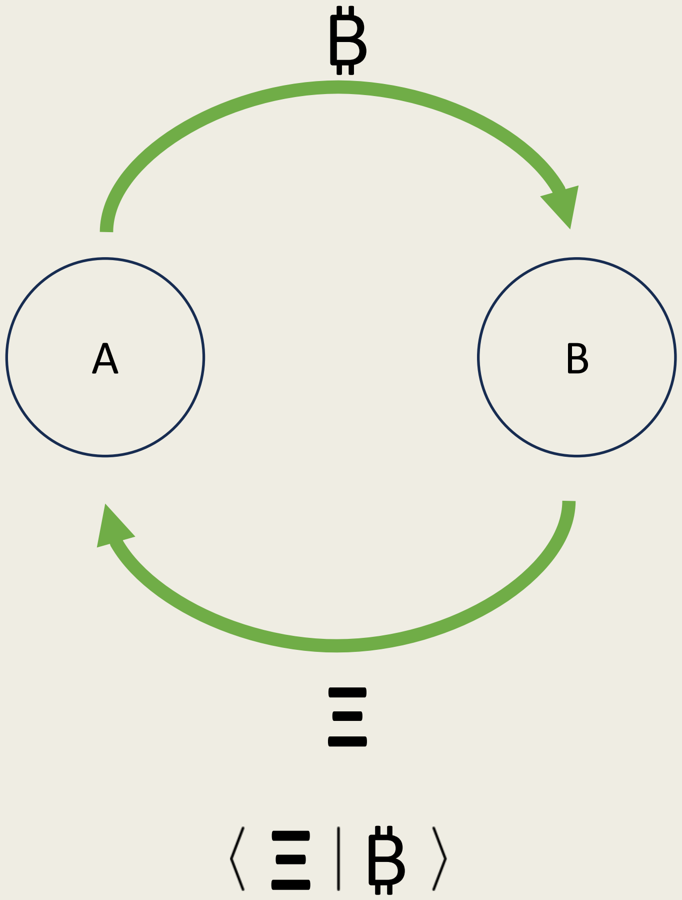


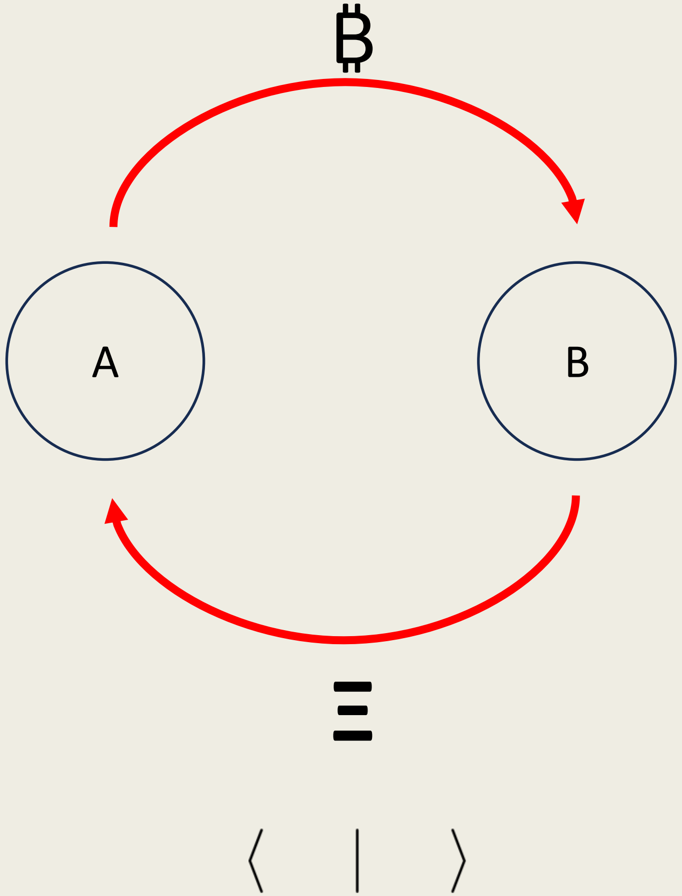
Formalization

Swap Digraph



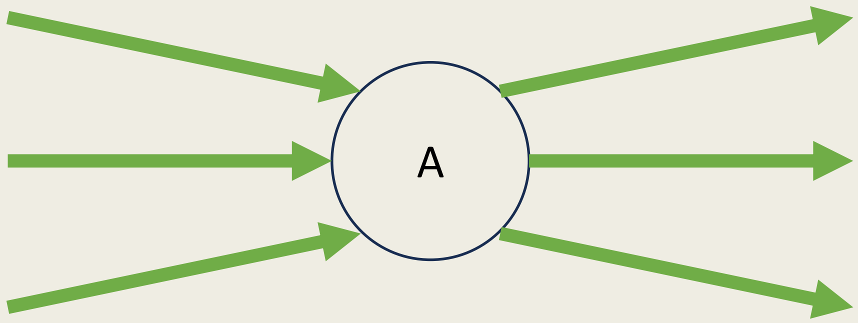
Outcomes





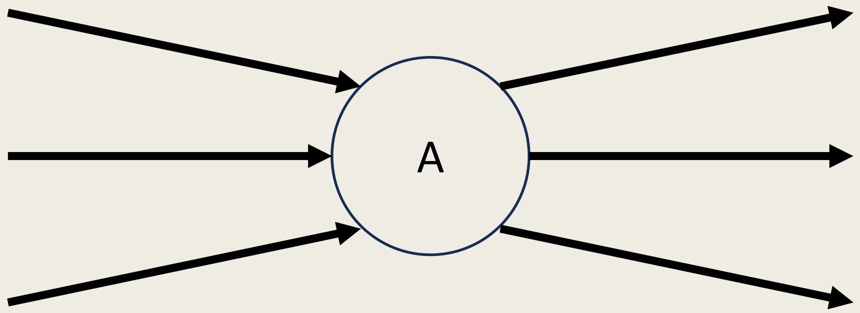
Outcomes

- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)



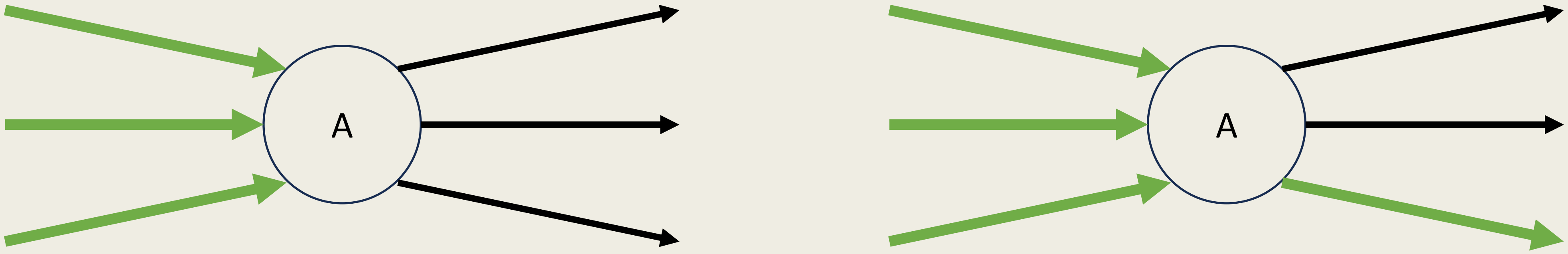
Outcomes

- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)



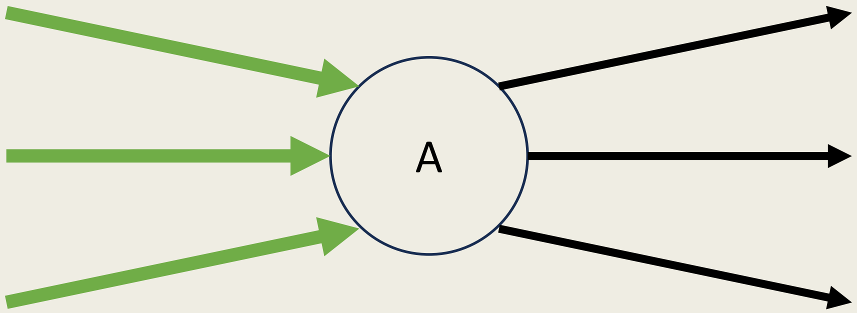
Outcomes

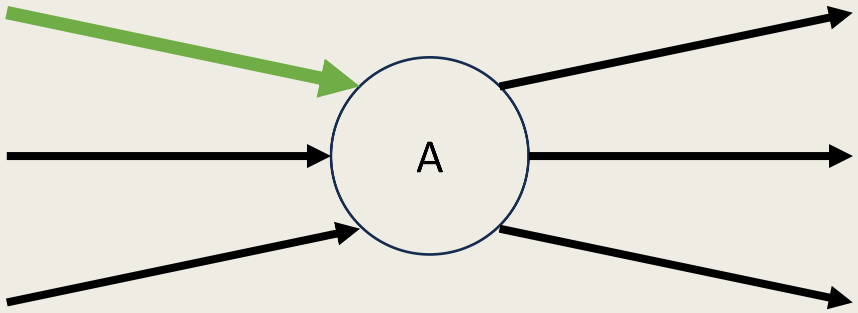
- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)



Outcomes

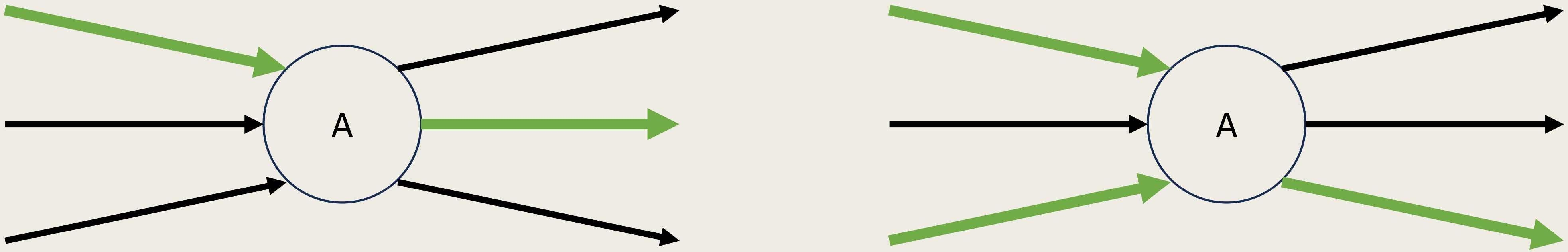
- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)





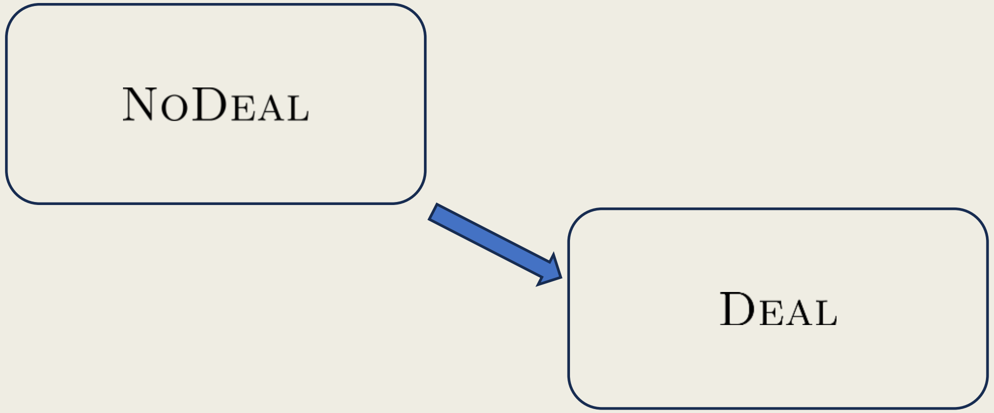
Outcomes

- $\textsc{Deal}$: $\langle all \mid all \rangle$
- $\textsc{NoDeal}$: $\langle none \mid none \rangle$
- $\textsc{Discount}$: $\langle all \mid \neg all \rangle$
- $\textsc{FreeRide}$: $\langle \neg none \mid none \rangle$
- $\textsc{Underwater}$: $\langle \neg all \mid \neg none \rangle$ (everything else)



Partial Ordering of Outcomes

- $\textsc{Deal}$: $\langle all \mid all \rangle$
- $\textsc{NoDeal}$: $\langle none \mid none \rangle$
- $\textsc{Discount}$: $\langle all \mid \neg all \rangle$
- $\textsc{FreeRide}$: $\langle \neg none \mid none \rangle$
- $\textsc{Underwater}$: $\langle \neg all \mid \neg none \rangle$ (everything else)

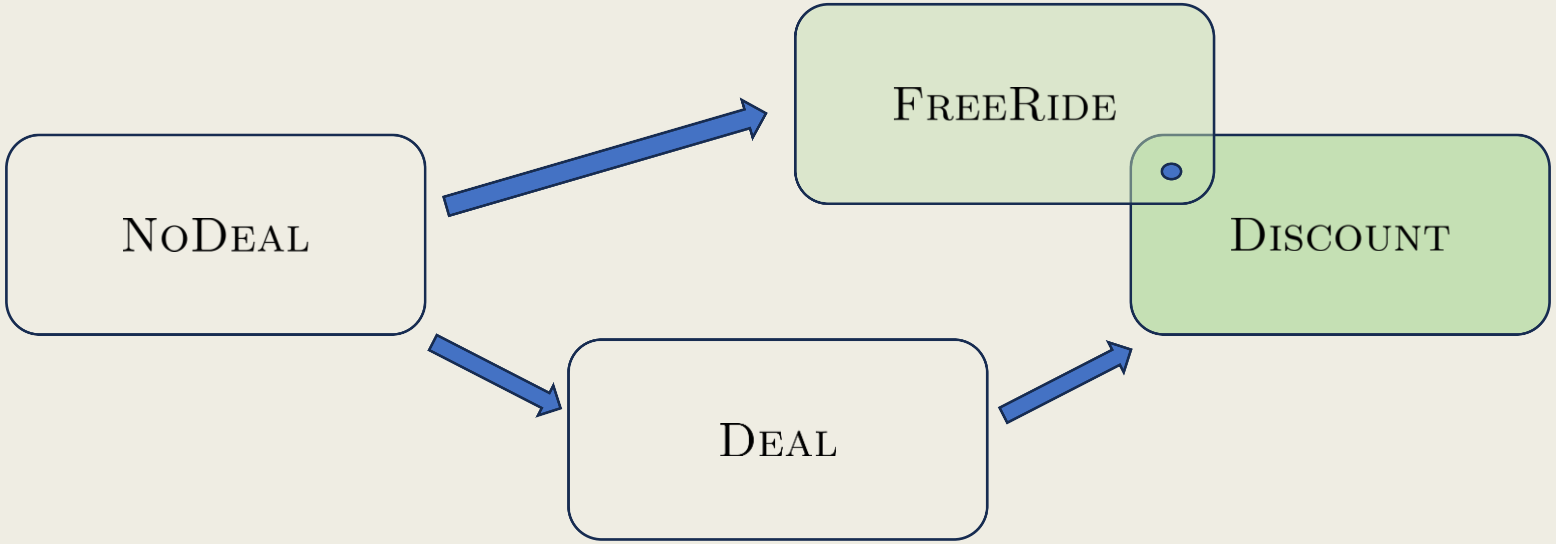


Partial Ordering of Outcomes

- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)

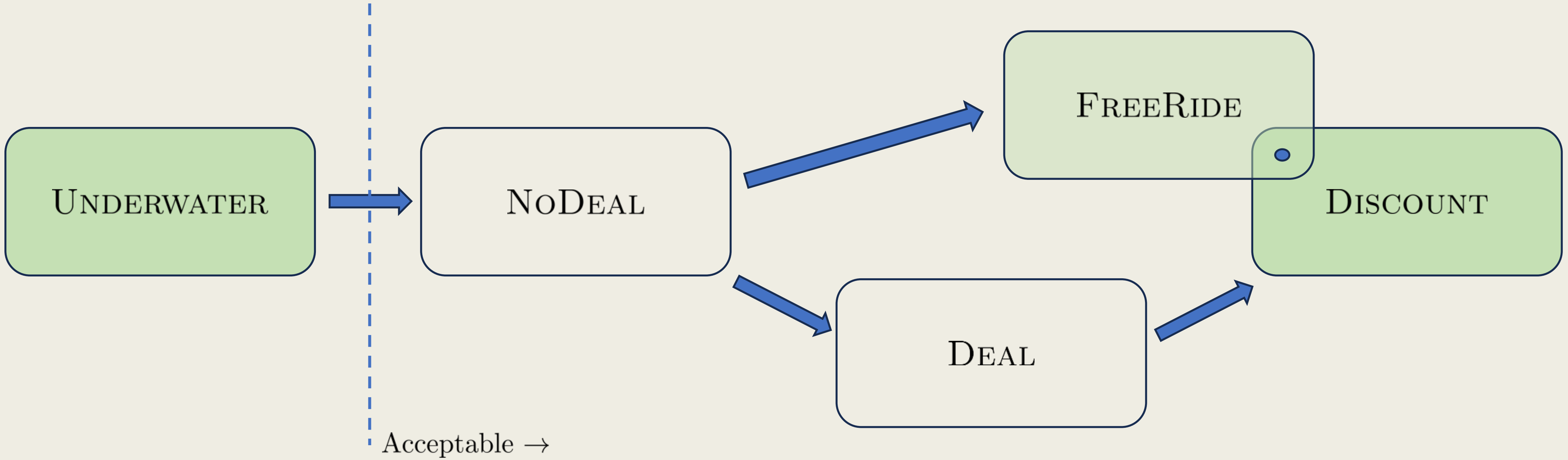
Partial Ordering of Outcomes

- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)



Partial Ordering of Outcomes

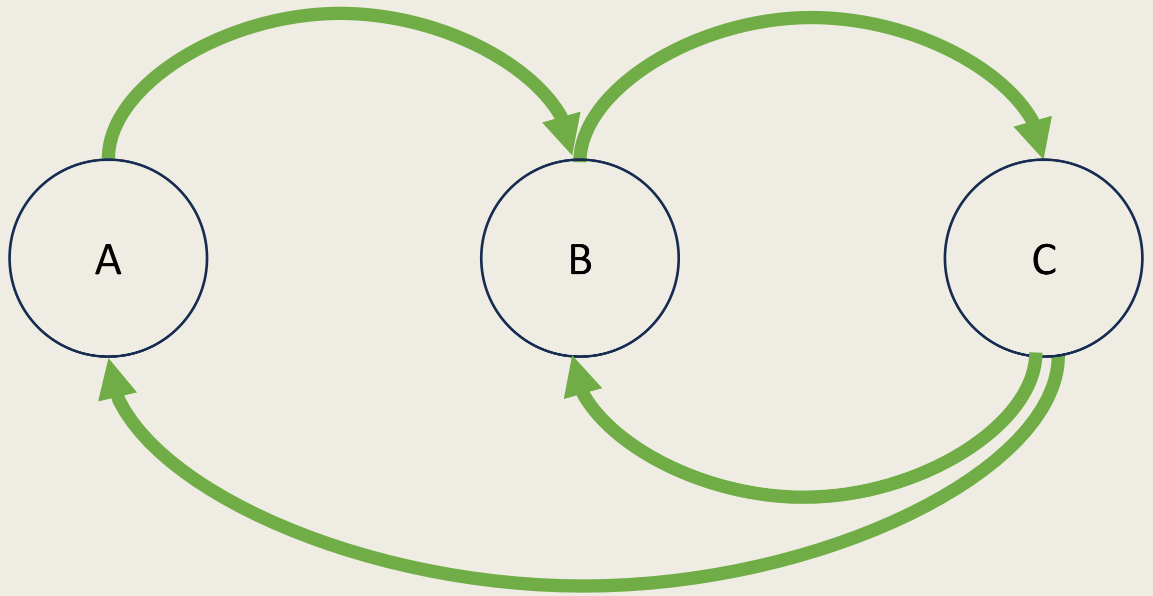
- DEAL: $\langle all \mid all \rangle$
- NODEAL: $\langle none \mid none \rangle$
- DISCOUNT: $\langle all \mid \neg all \rangle$
- FREERIDE: $\langle \neg none \mid none \rangle$
- UNDERWATER: $\langle \neg all \mid \neg none \rangle$ (everything else)



Protocol Properties

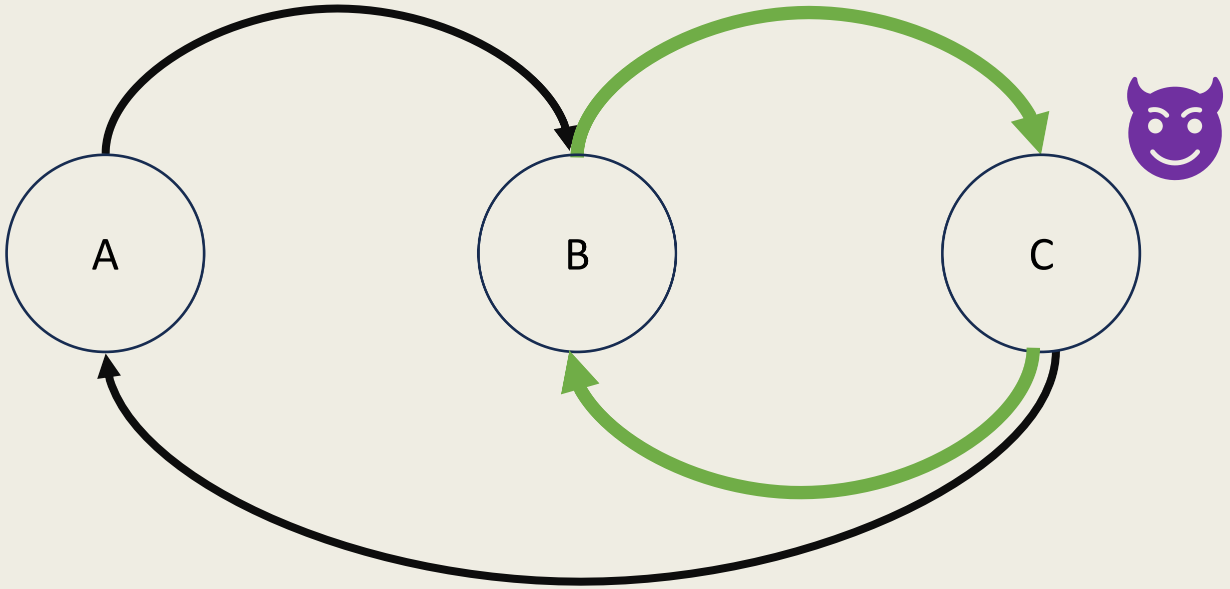
Atomic Protocol Properties

- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes DEAL
- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$



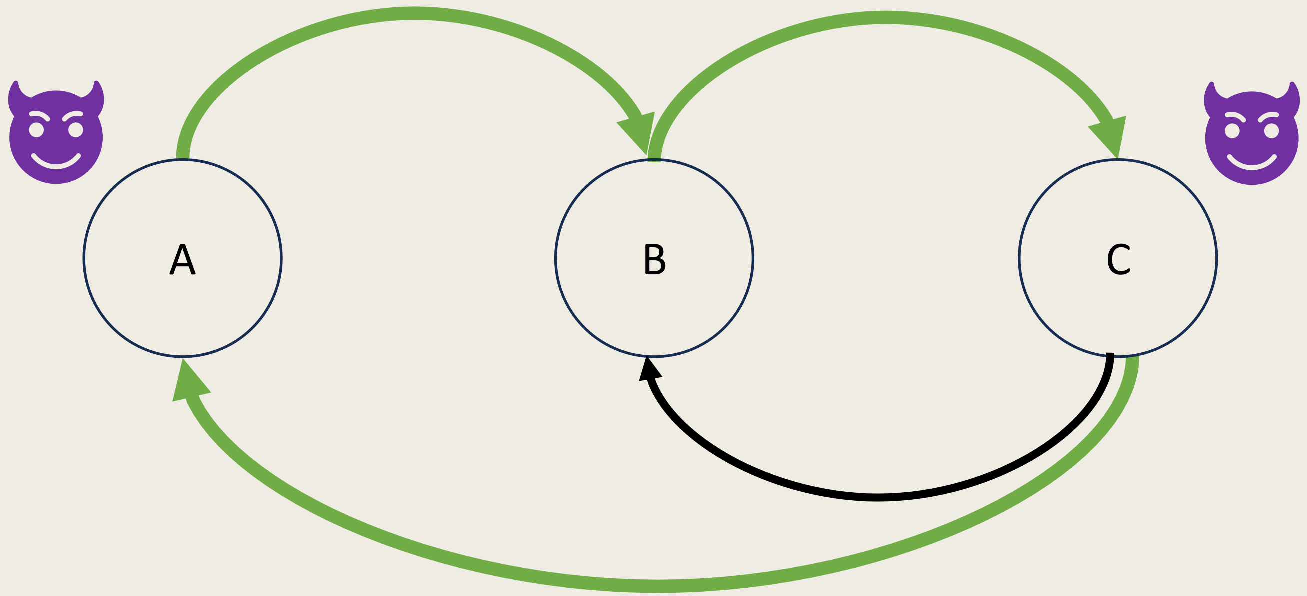
Atomic Protocol Properties

- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes DEAL
- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$



Atomic Protocol Properties

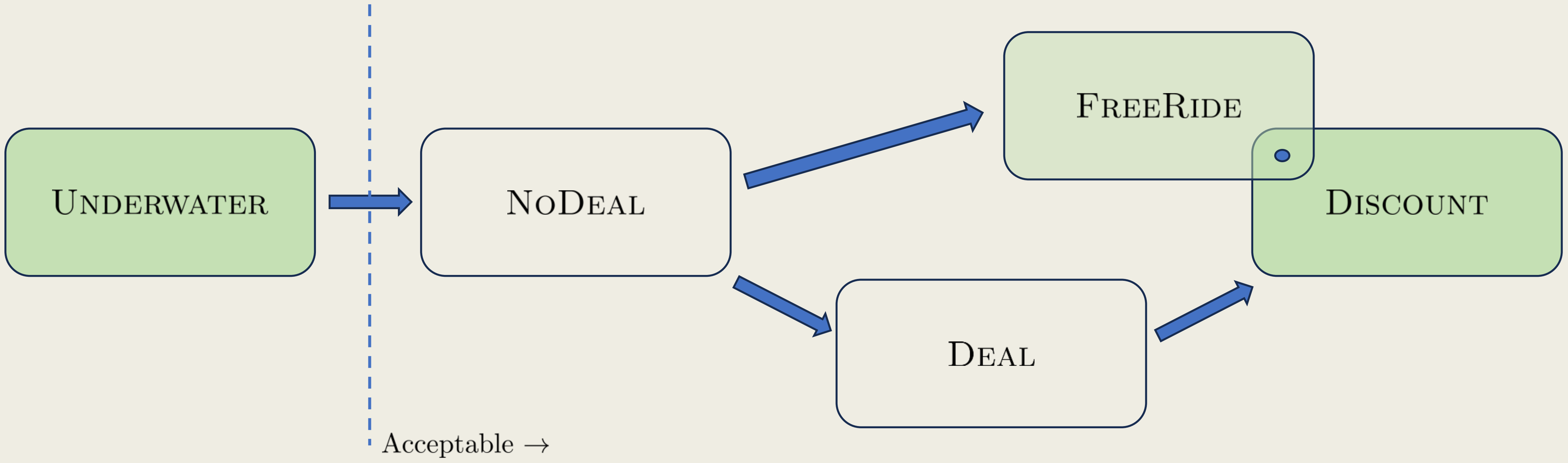
- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes DEAL
- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$



Herlihy's Protocol

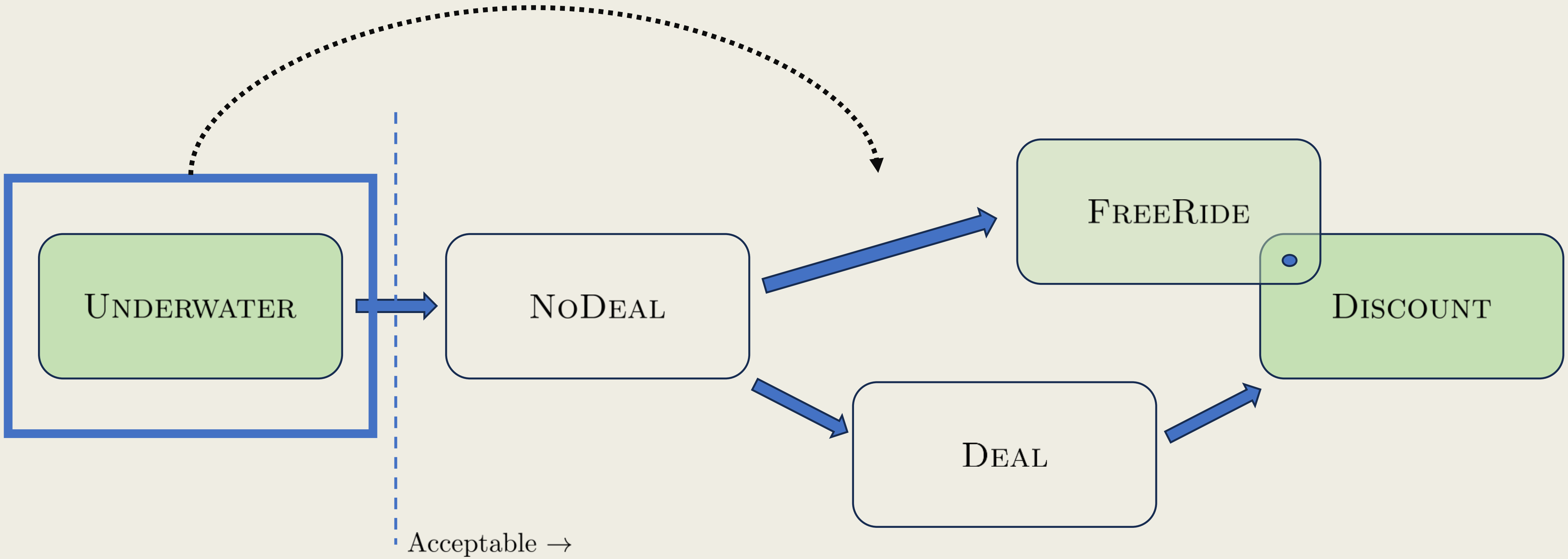
[Herlihy'18] gives an atomic protocol so long that:

- the swap digraph is strongly connected
- each party has the preference structure:

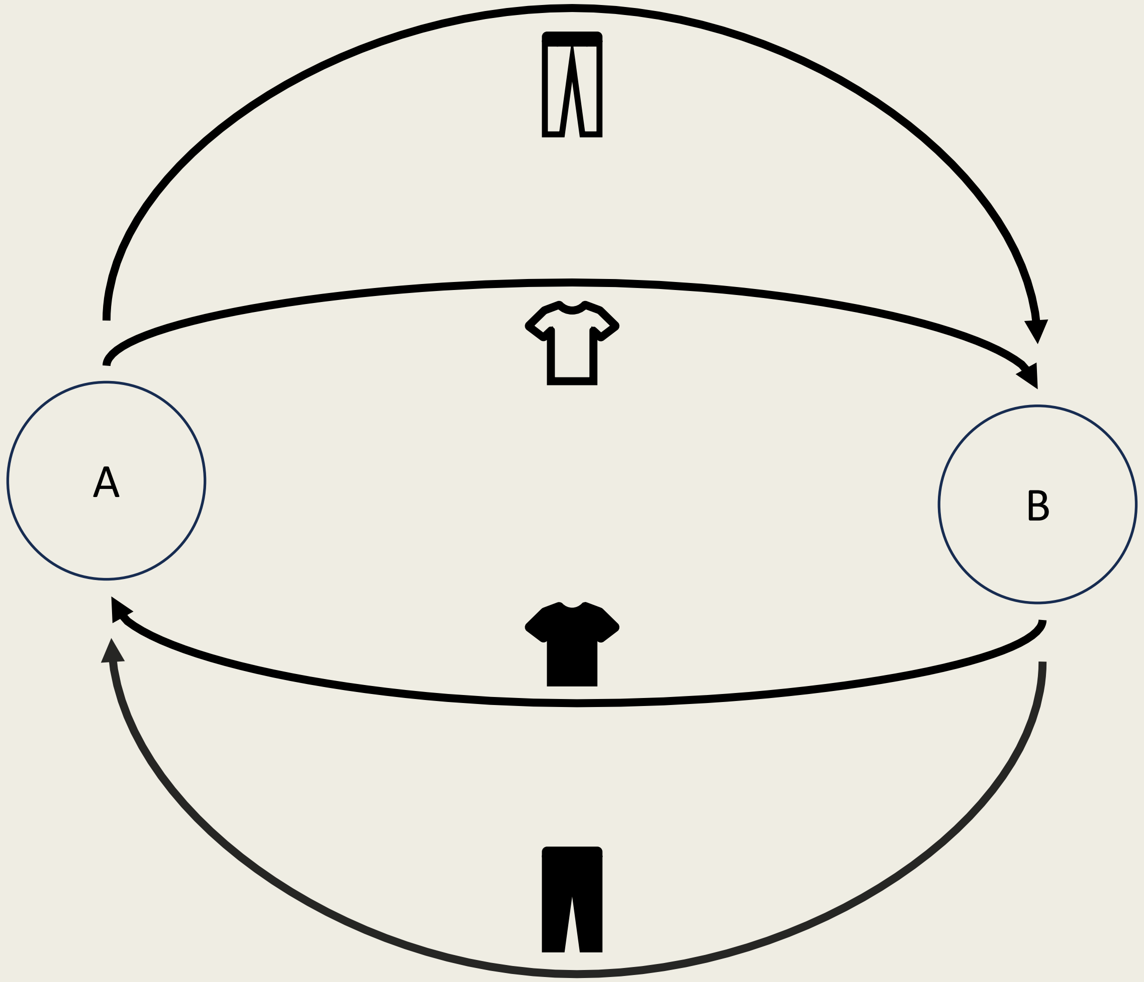


Can We Do Better?

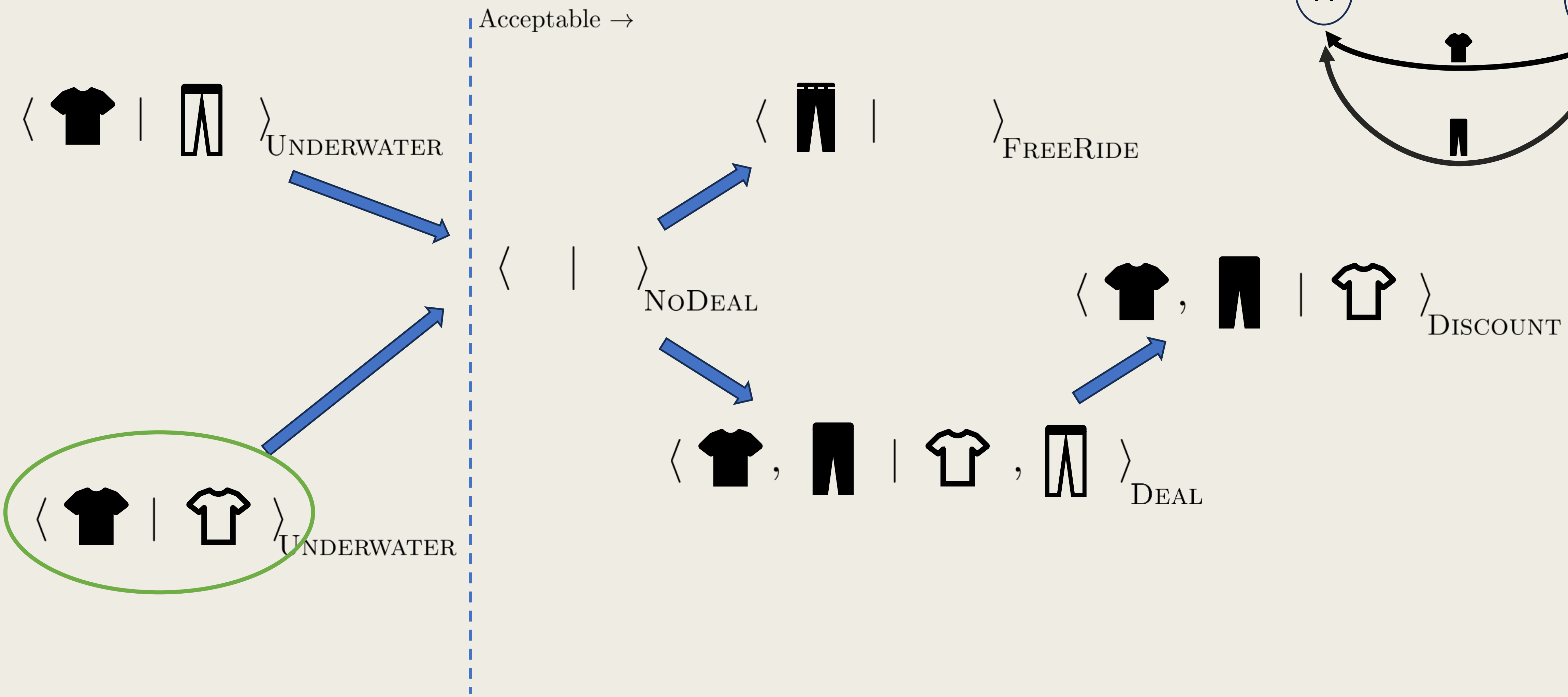
The Underwater Class

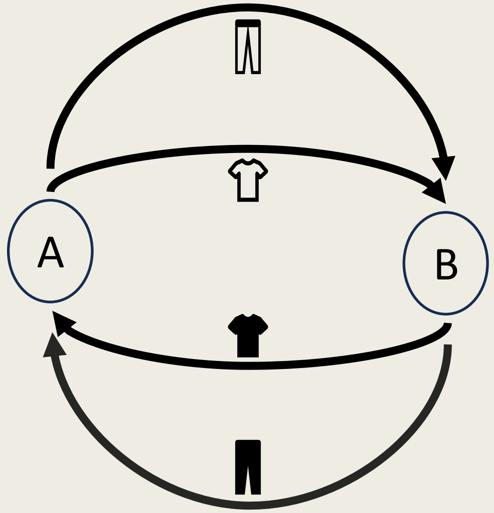


Preferences

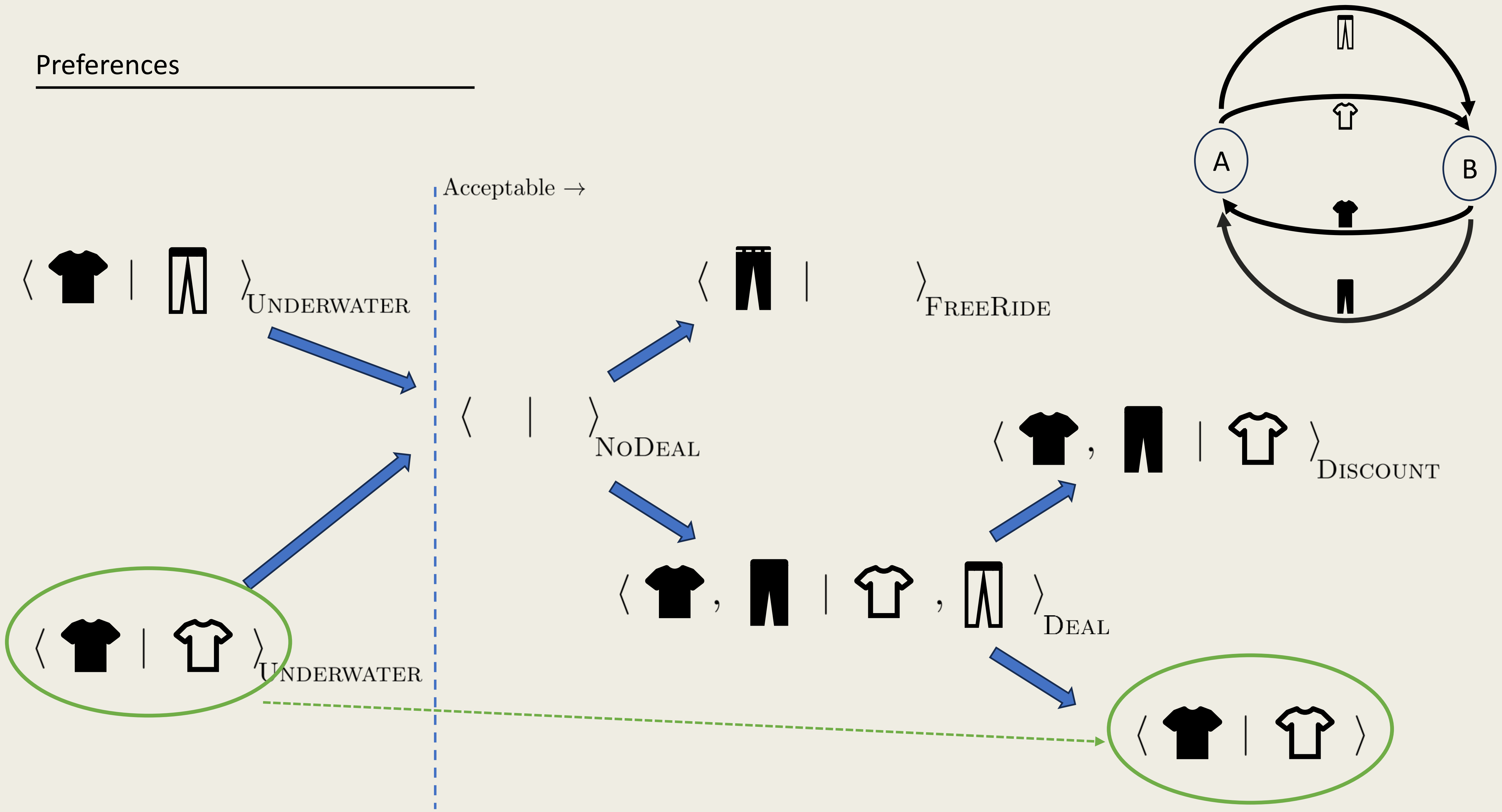


Preferences

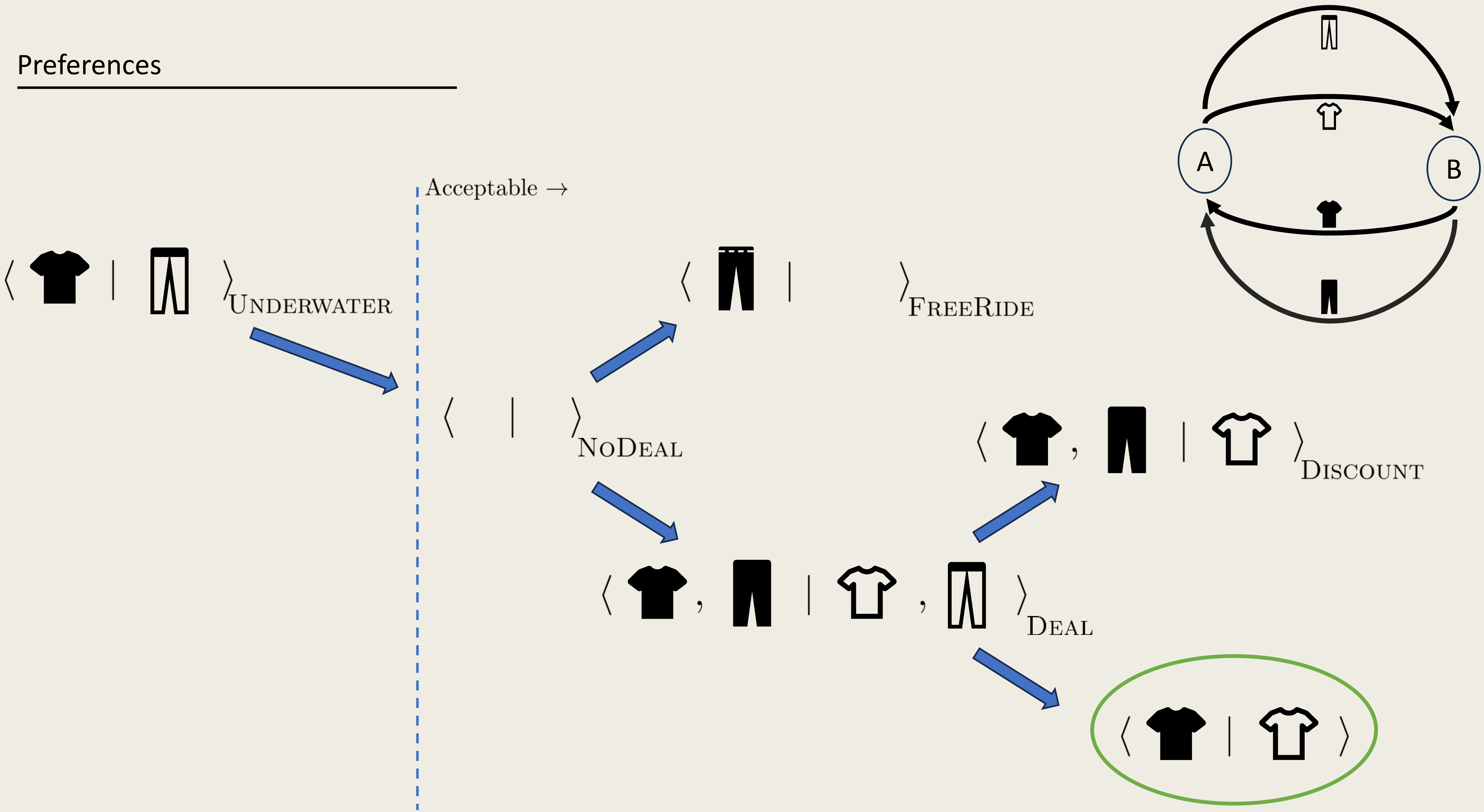




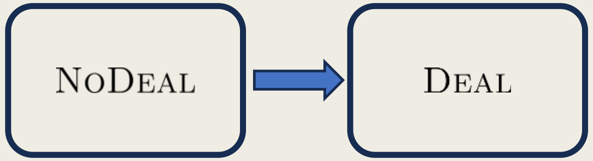
Preferences



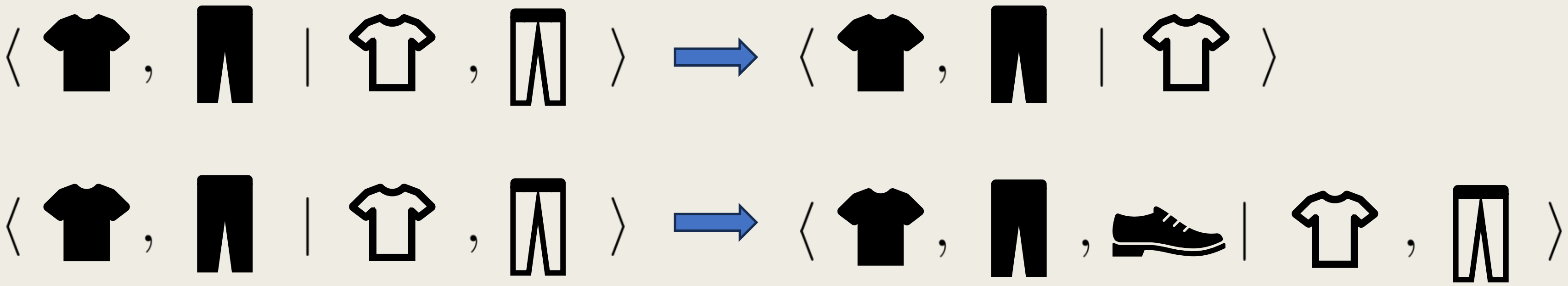
Preferences



User-defined Preferences

- 

- *Inclusive Monotonicity*:



General Atomic Protocol?

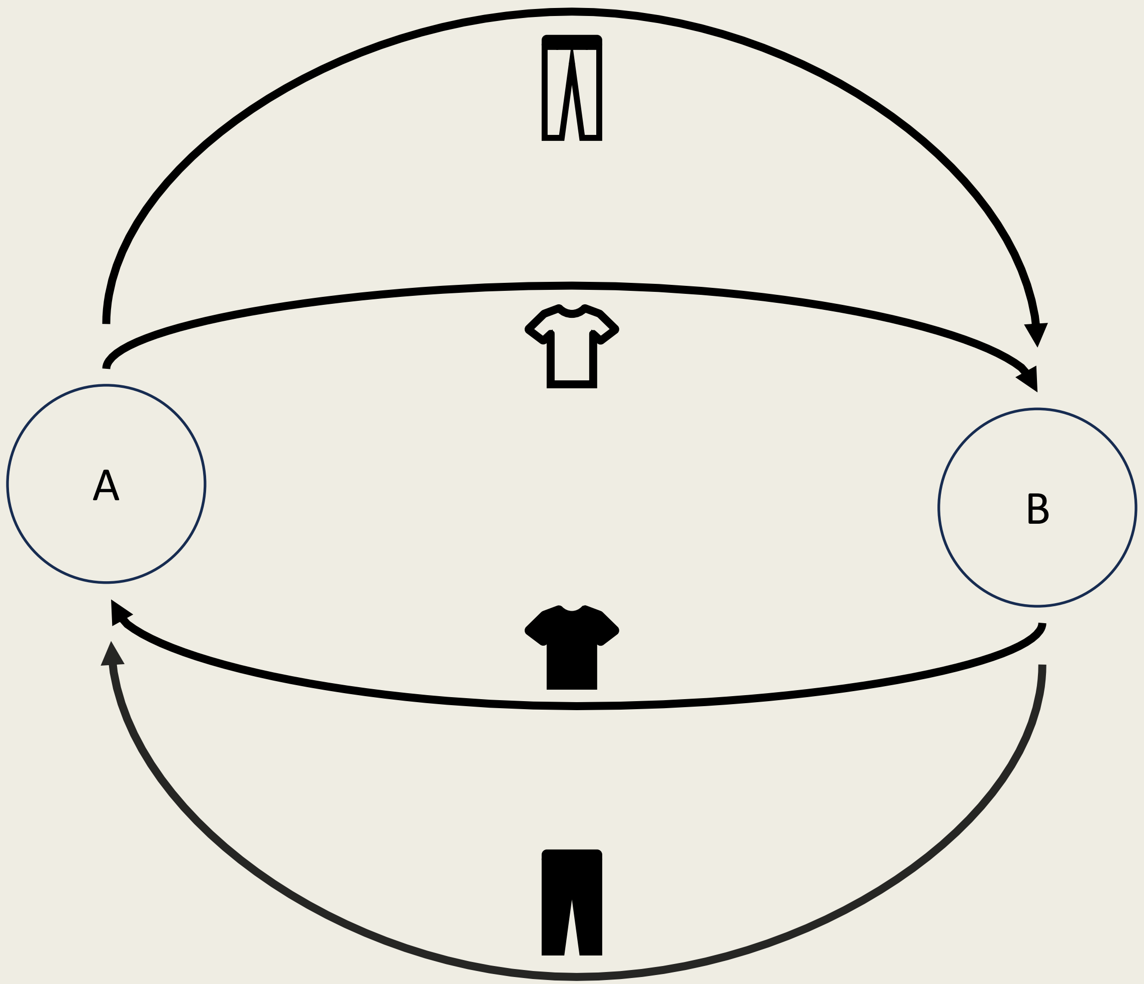
- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes DEAL *or better*
- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$

General Atomic Protocol?

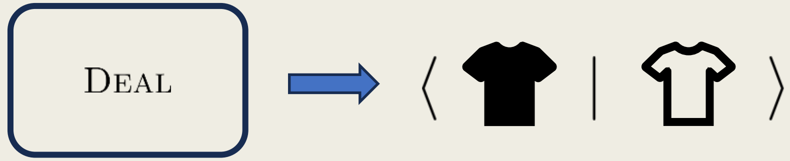
- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes DEAL *or better*
- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$

No, there is no atomic protocol (scheme) that works for every swap system.

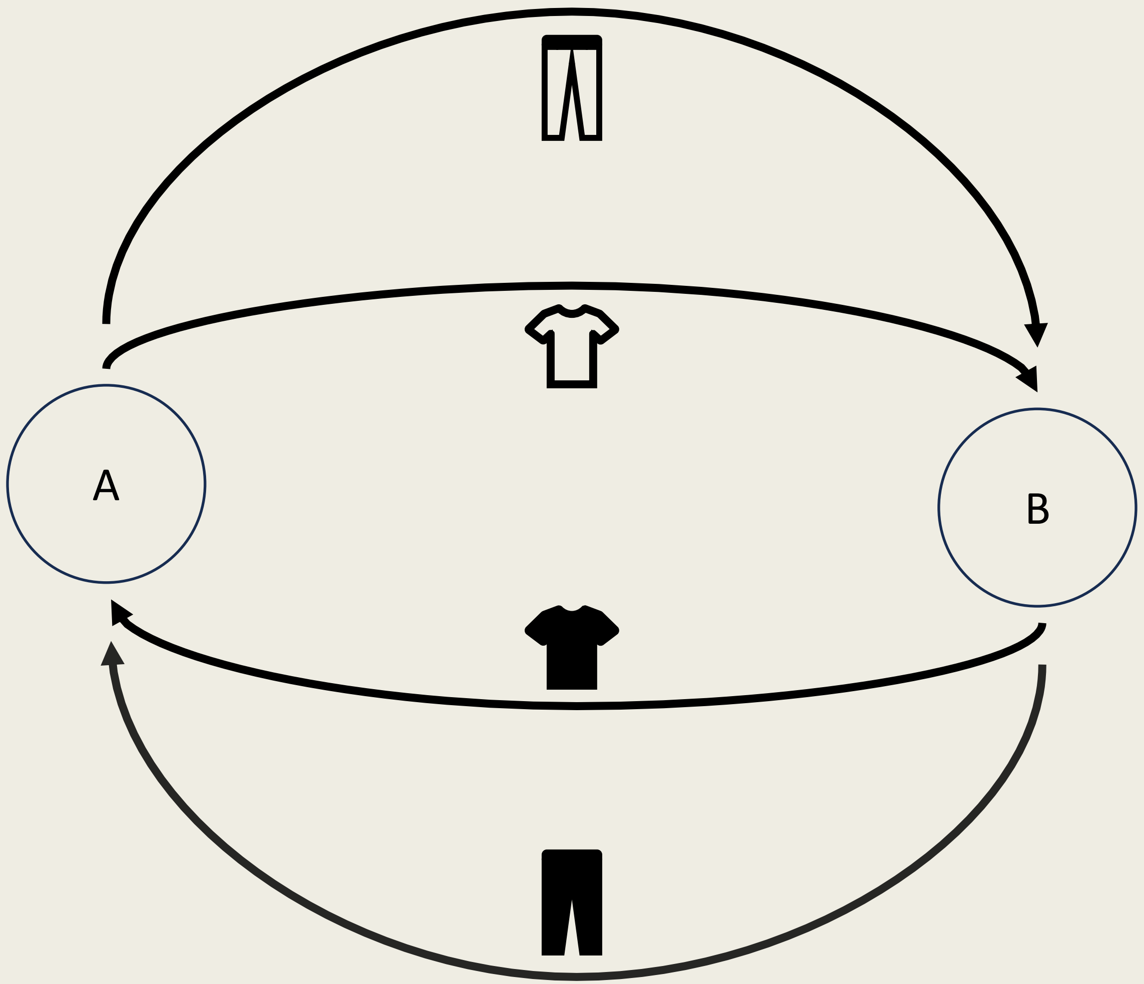
No General Atomic Protocol



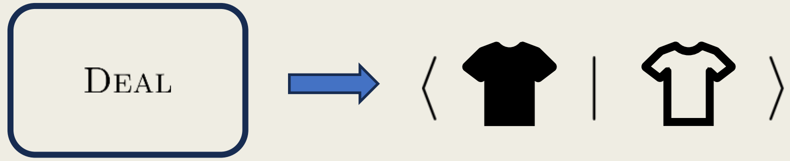
Preference of A:



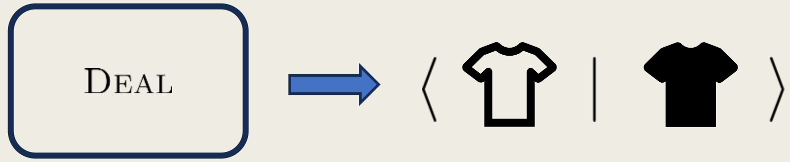
No General Atomic Protocol



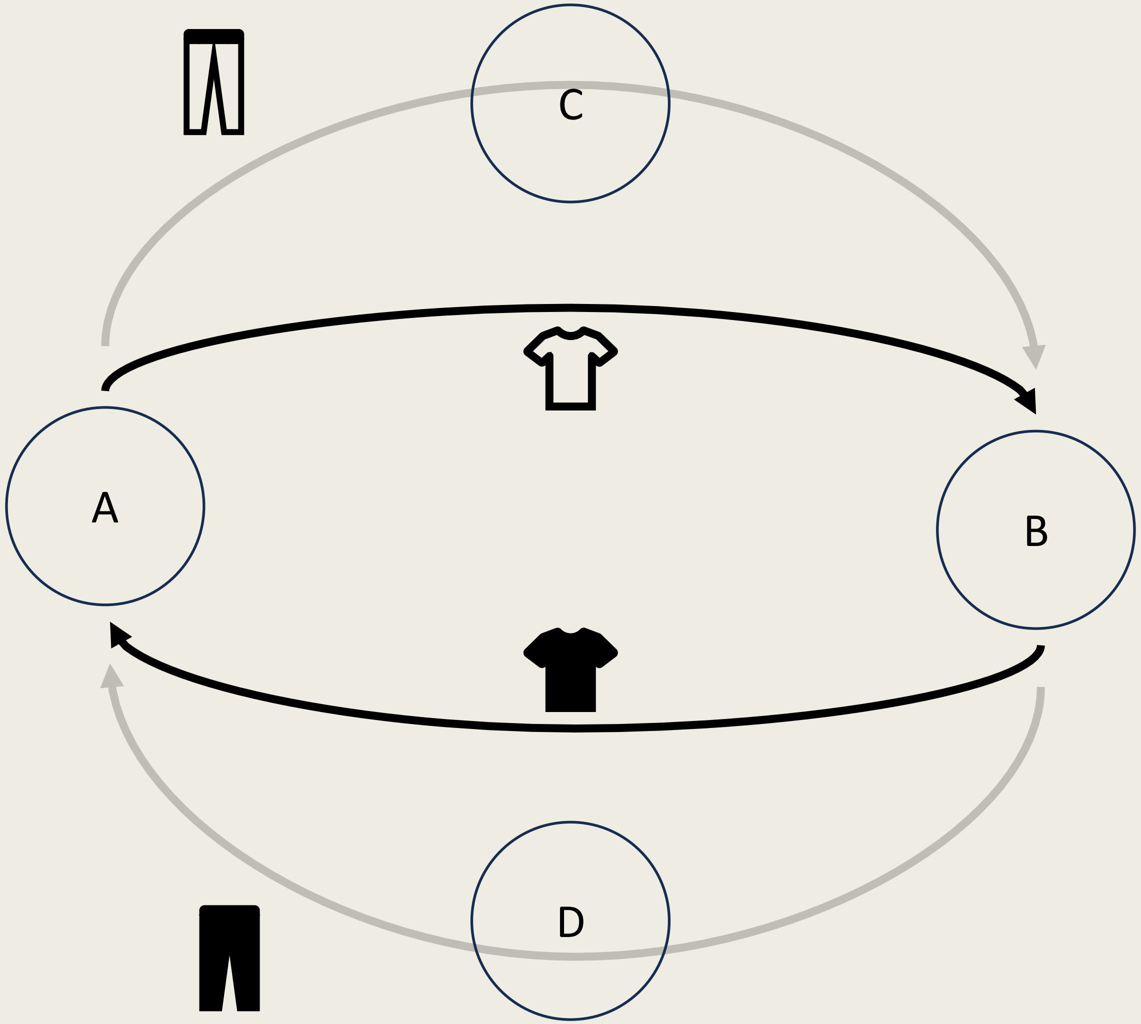
Preference of A:



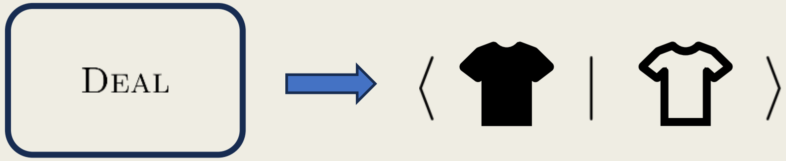
Preference of B:



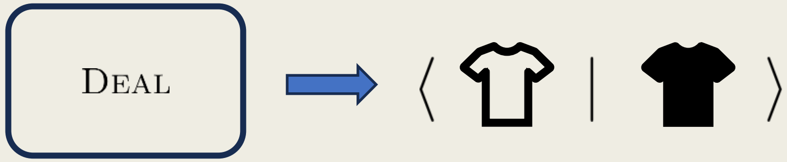
No General Atomic Protocol



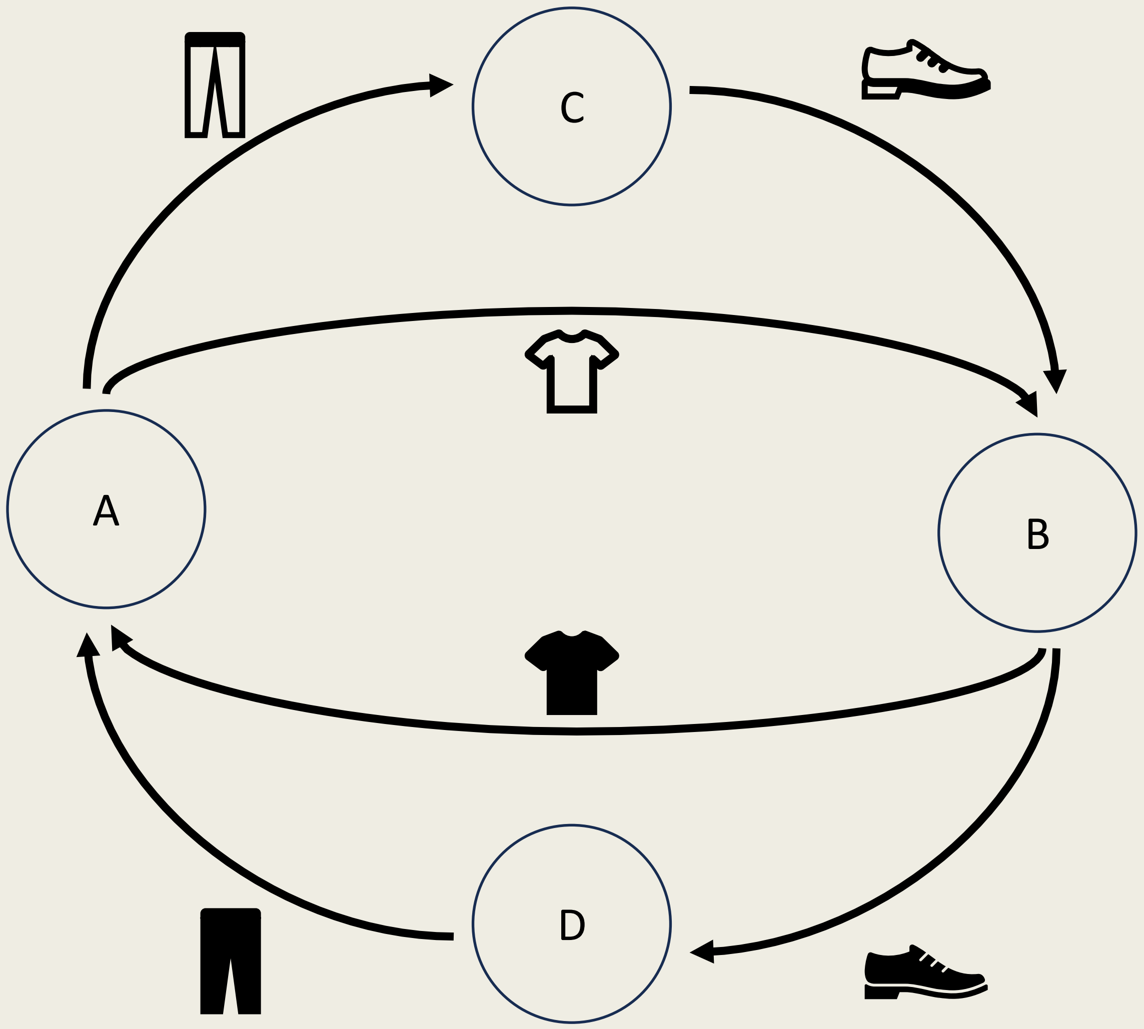
Preference of A:



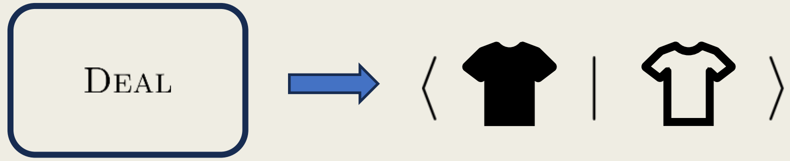
Preference of B:



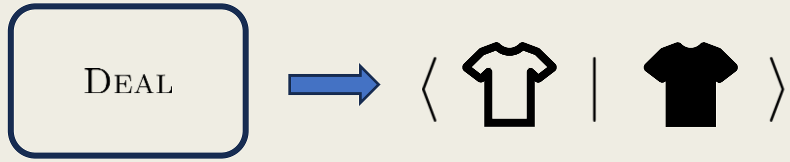
No General Atomic Protocol



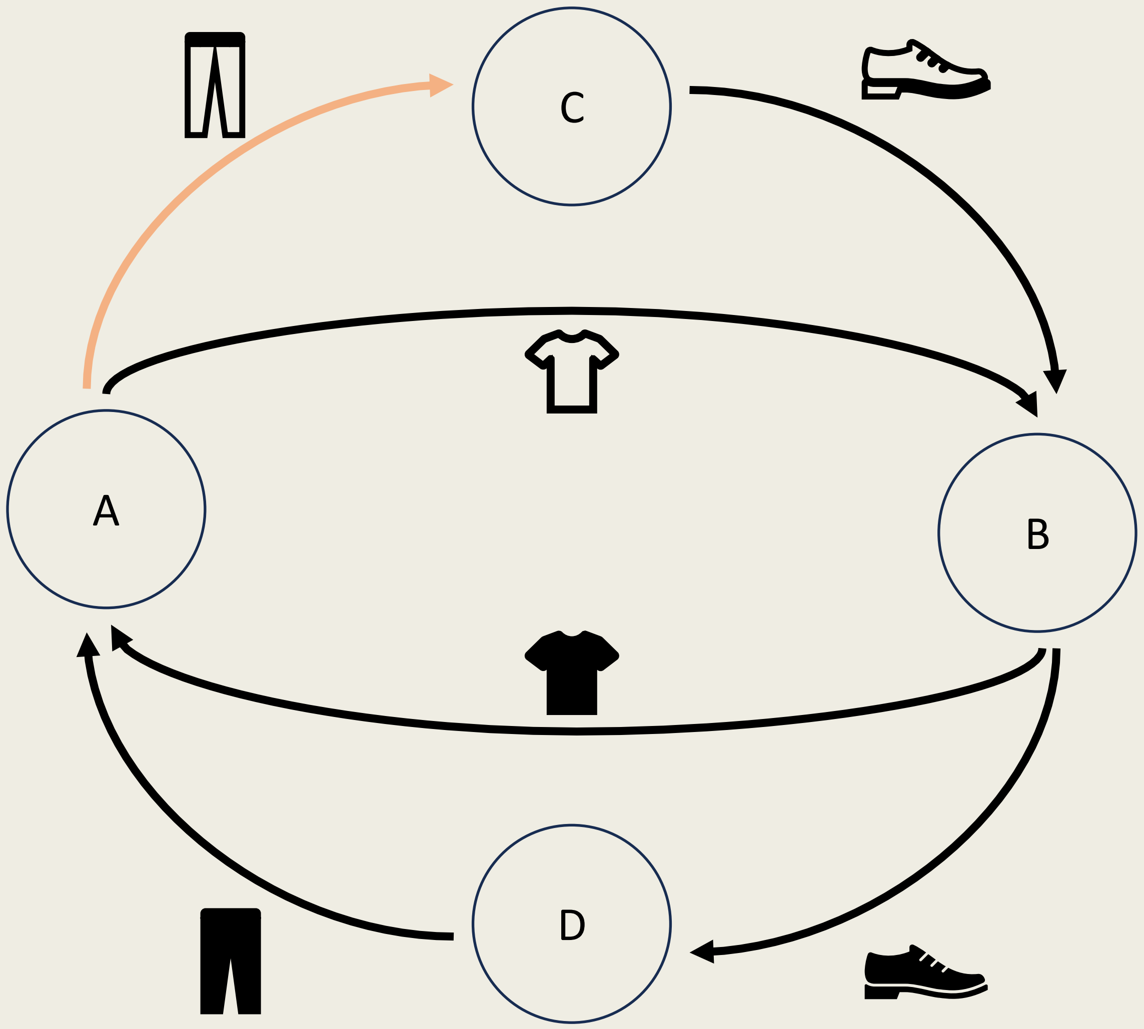
Preference of A:



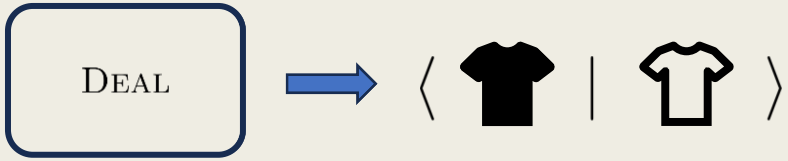
Preference of B:



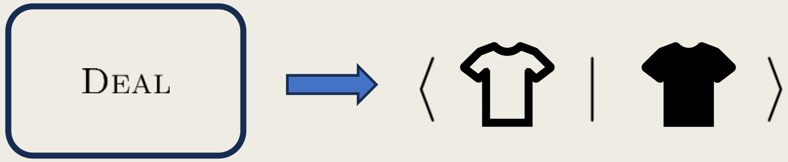
No General Atomic Protocol – Case 1



Preference of A:

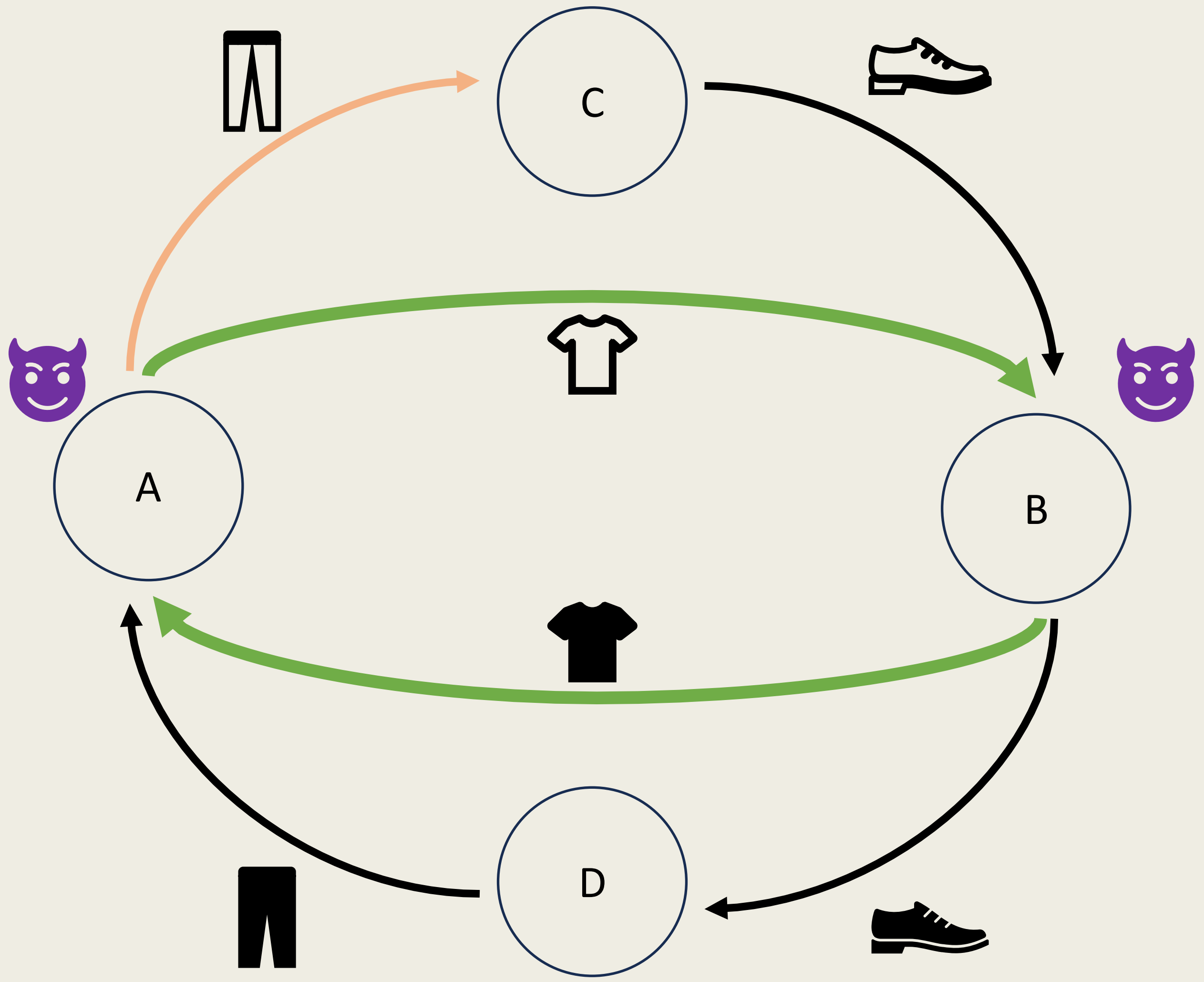


Preference of B:

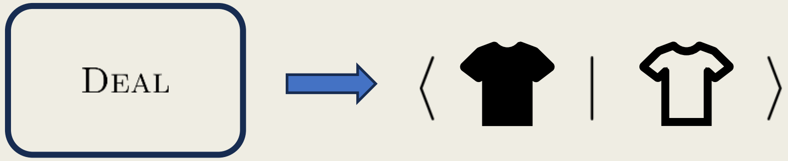


Case 1

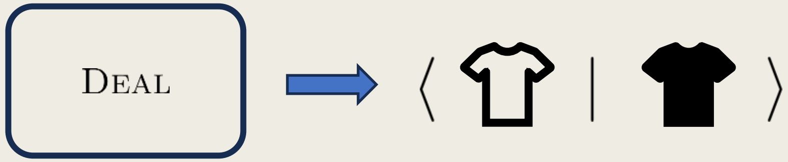
No General Atomic Protocol – Case 1



Preference of A:

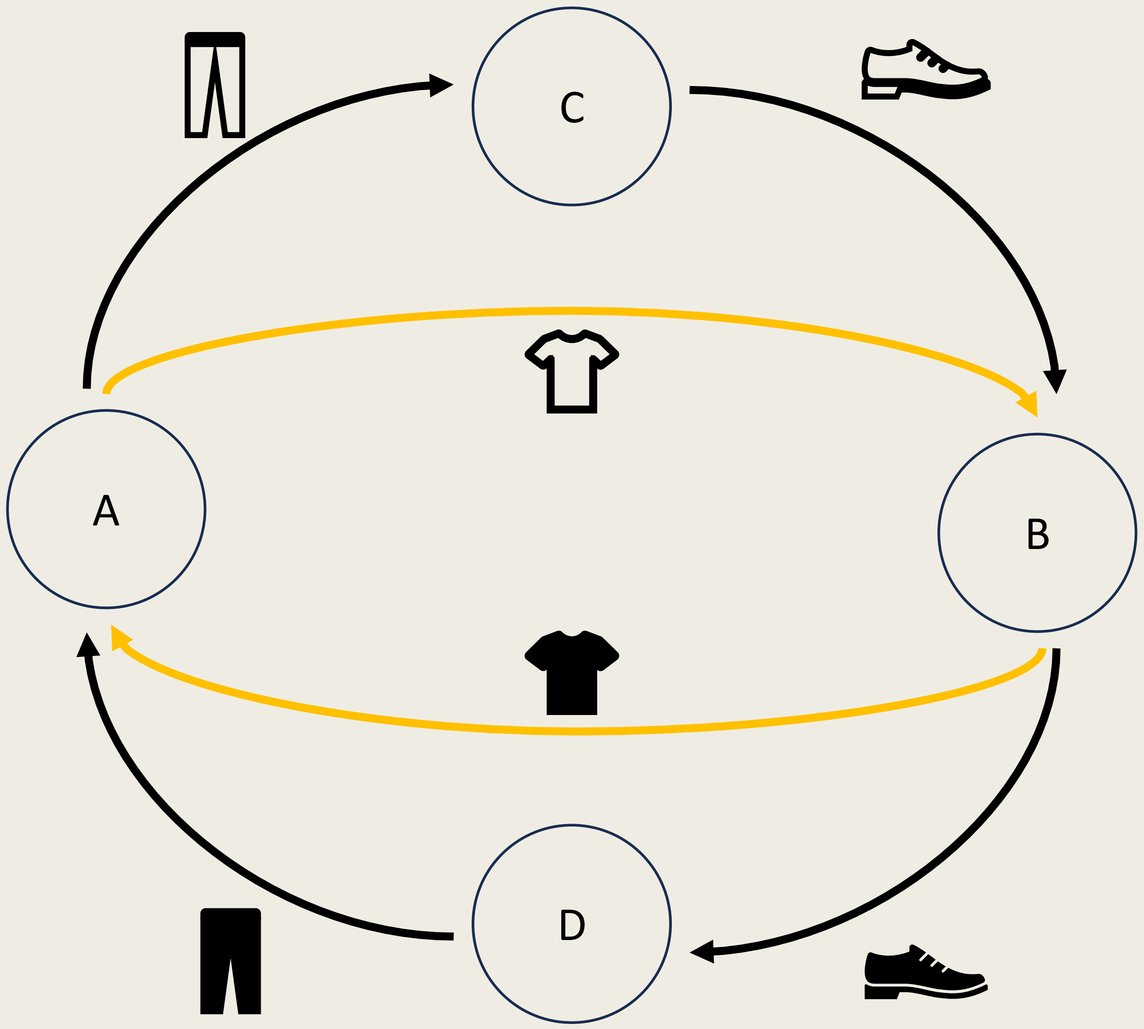


Preference of B:

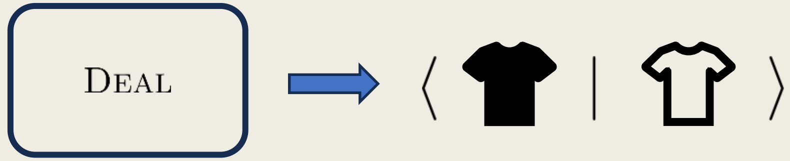


Case 1: Not strong Nash equilibria

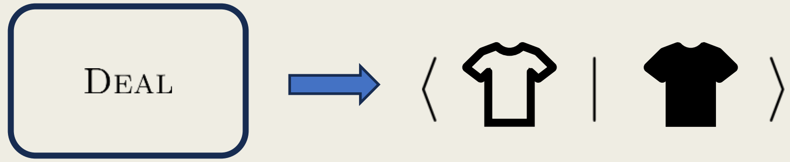
No General Atomic Protocol – Case 2



Preference of A:

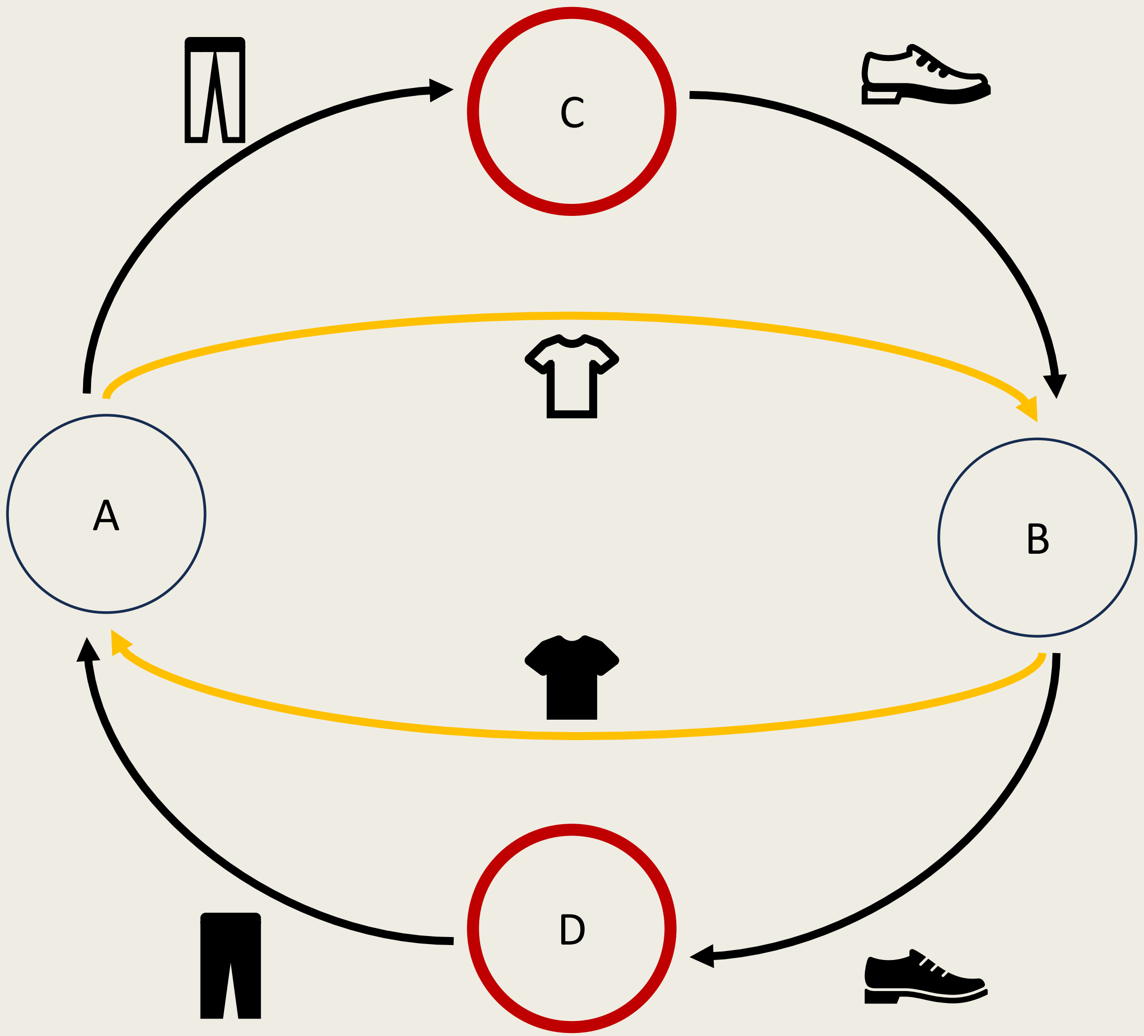


Preference of B:

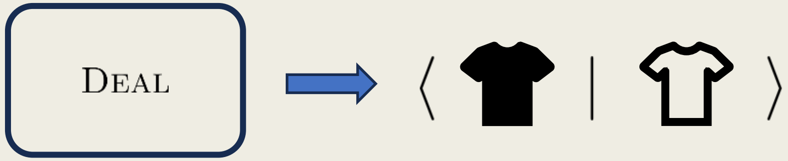


Case 2

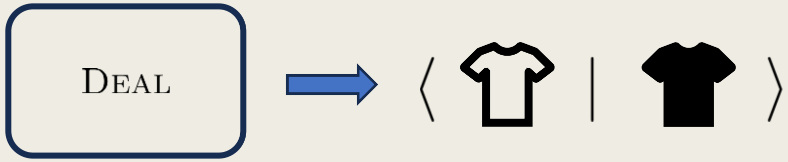
No General Atomic Protocol – Case 2



Preference of A:



Preference of B:



Case 2: Not live

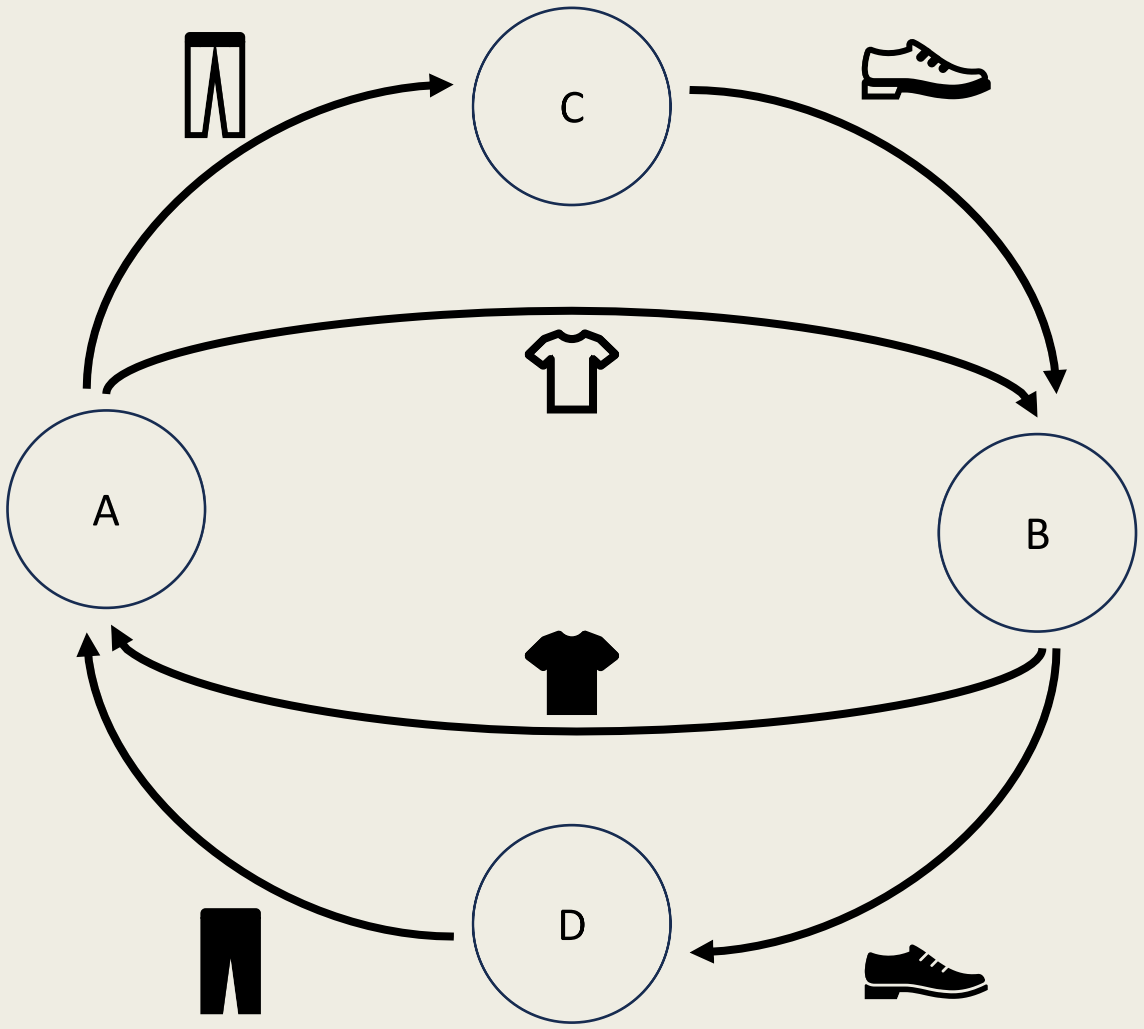
Sometimes, There Is a Protocol

Theorem

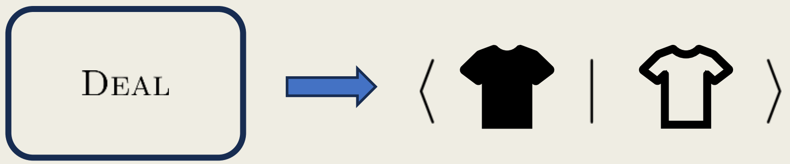
Theorem. $S = (D, P)$ has an atomic protocol **iff** there exists a spanning subgraph G of D such that:

- G is piece-wise strongly connected and has no isolated vertices
- G dominates D
- no subgraph H of D strictly dominates G

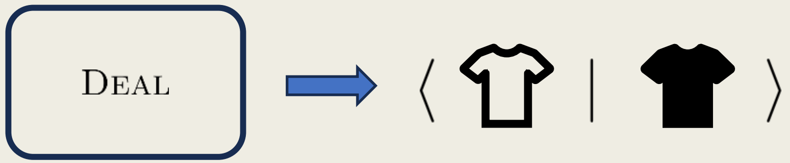
Example



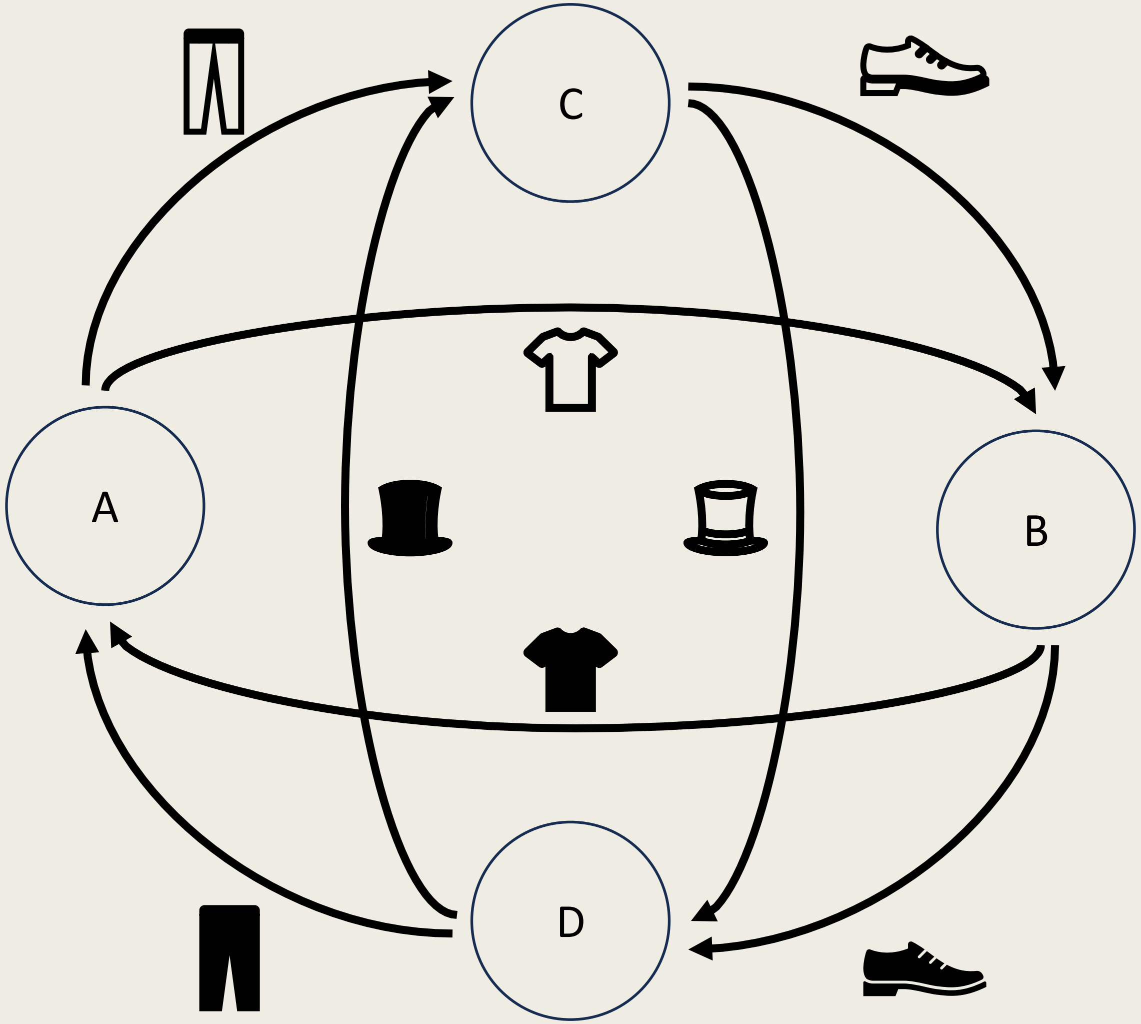
Preference of A:



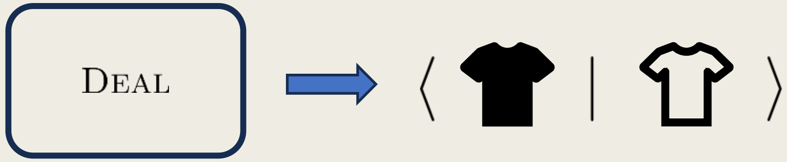
Preference of B:



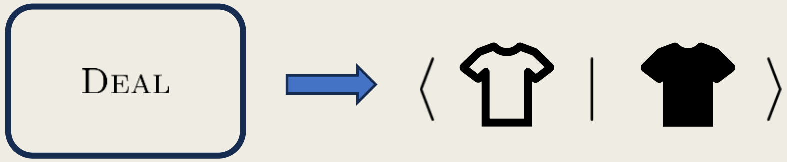
Example



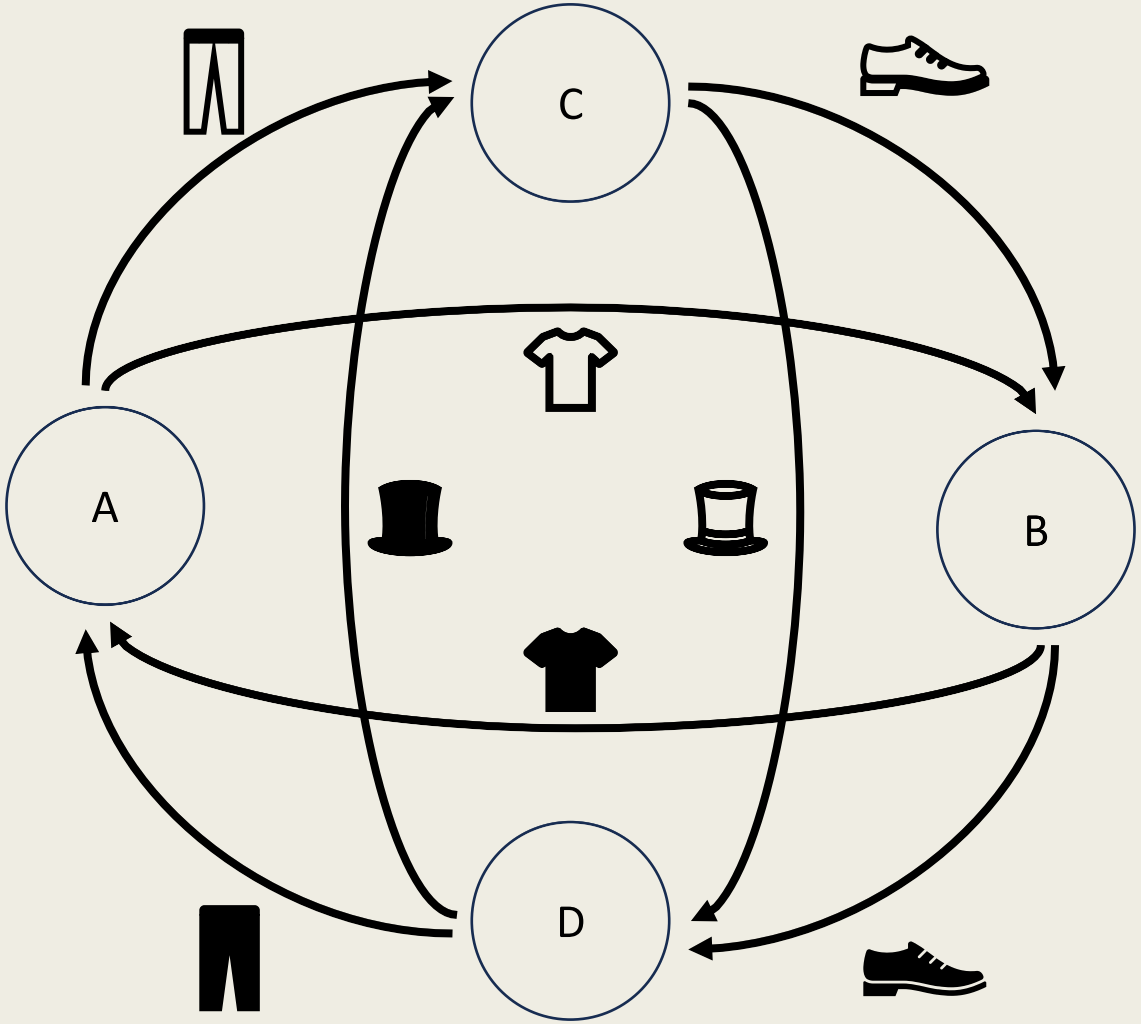
Preference of A:



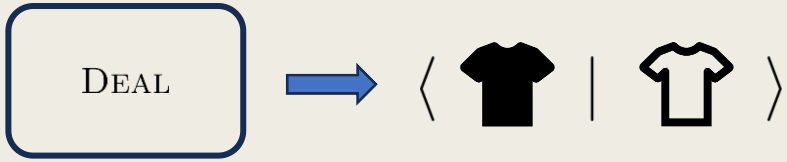
Preference of B:



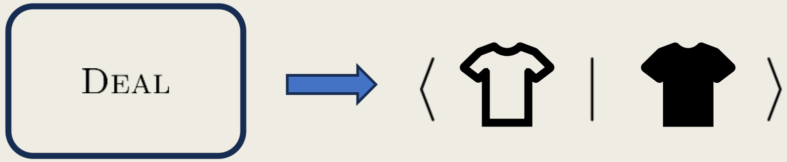
Example



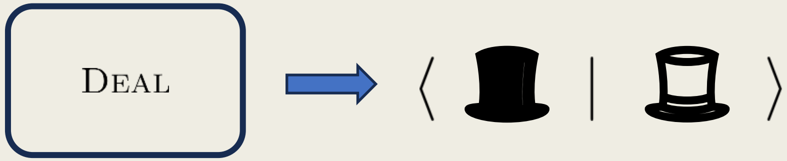
Preference of A:



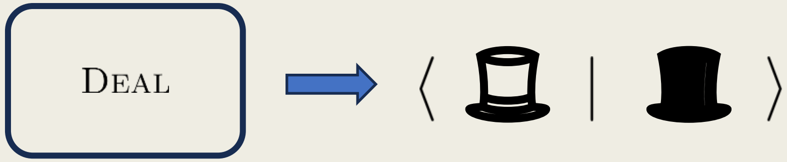
Preference of B:



Preference of C:

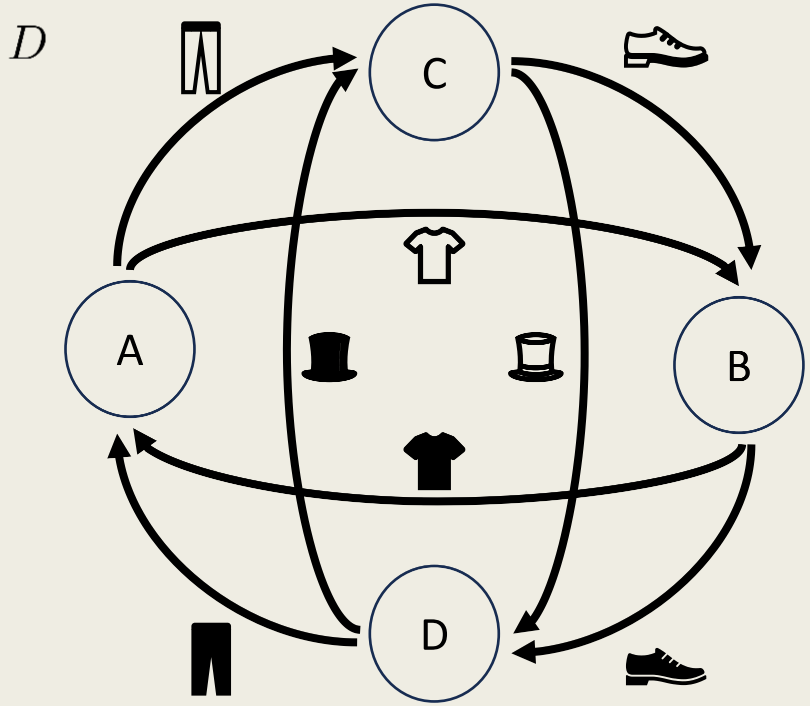


Preference of D:



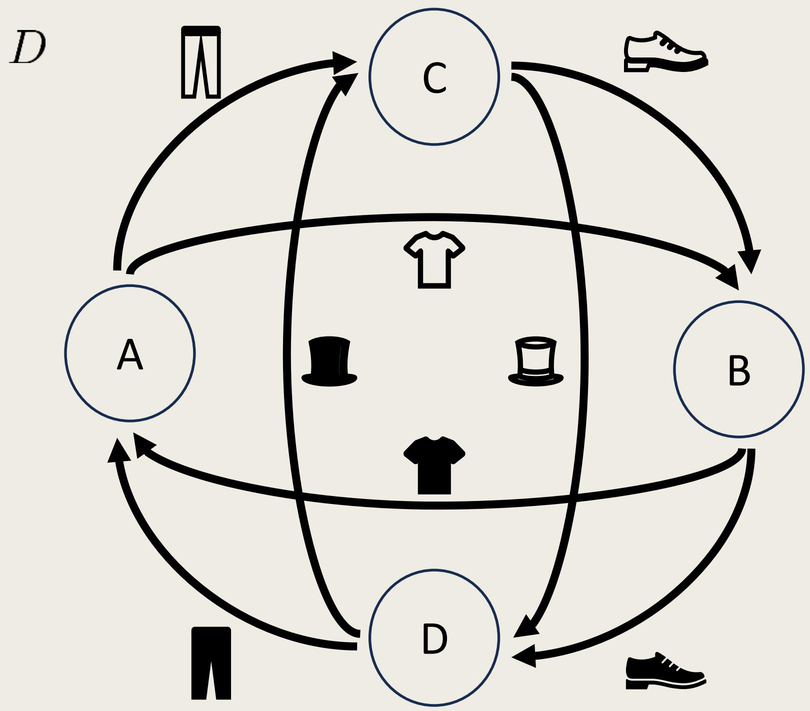
Condition 1

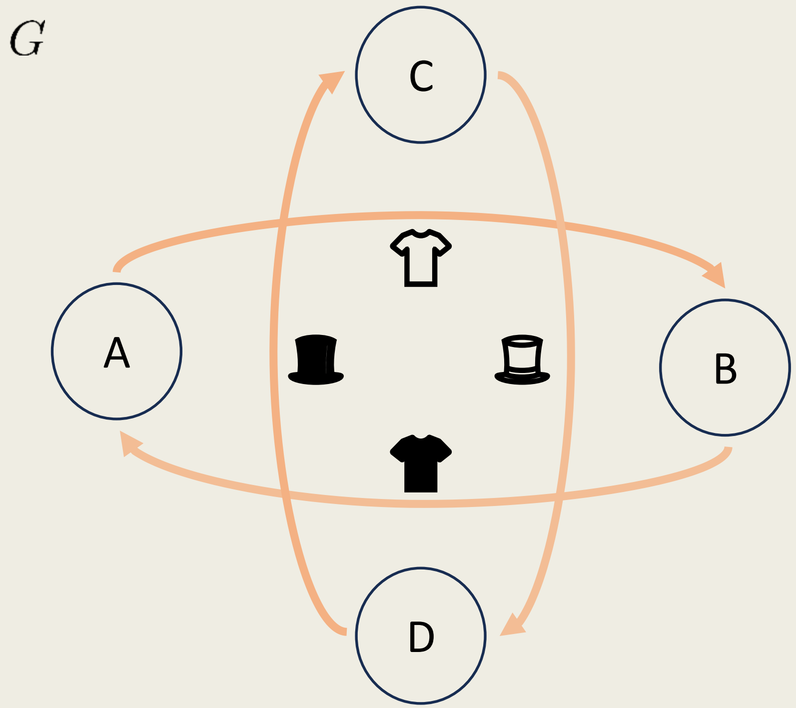
G is piece-wise strongly connected and has no isolated vertices



Condition 1

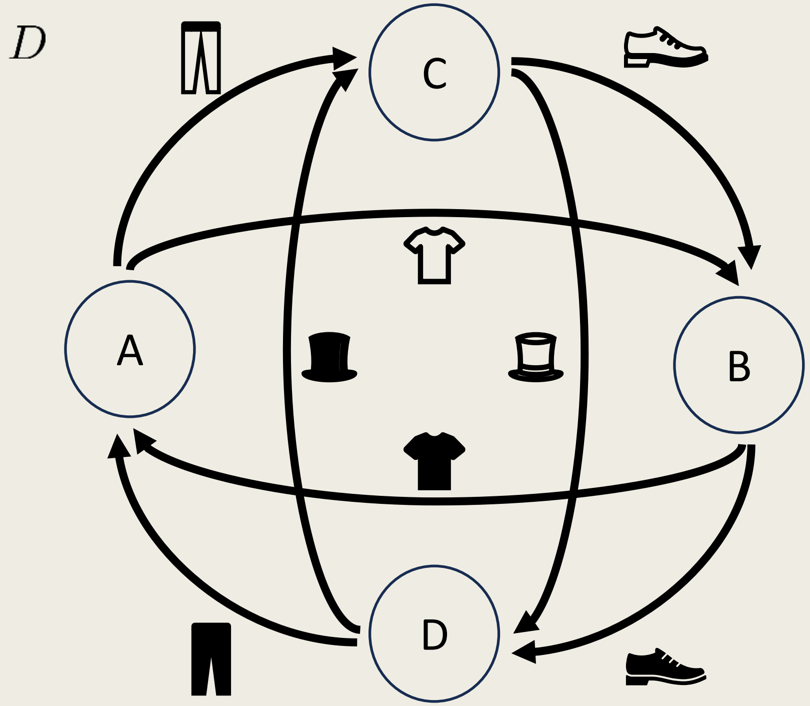
G is piece-wise strongly connected and has no isolated vertices

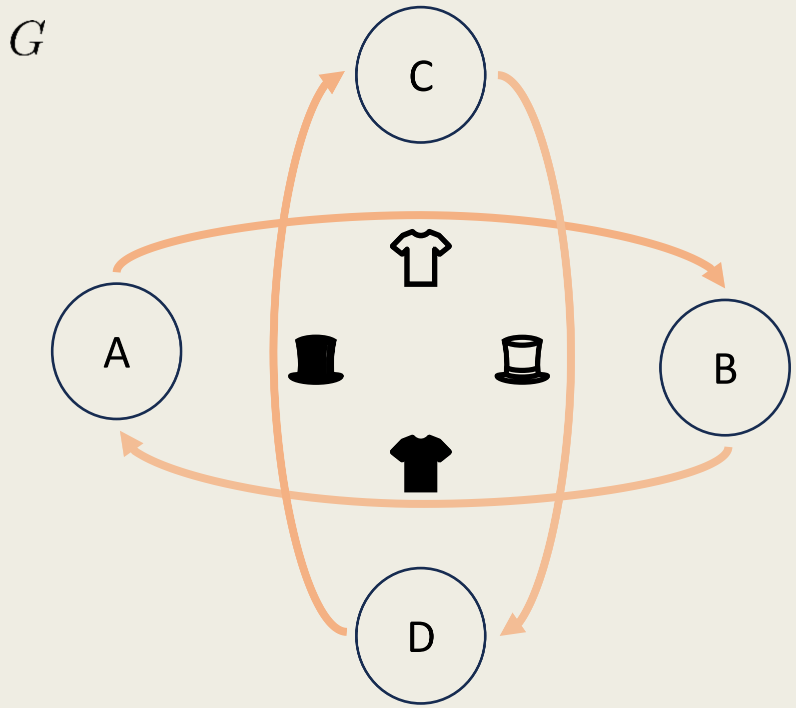




Condition 2

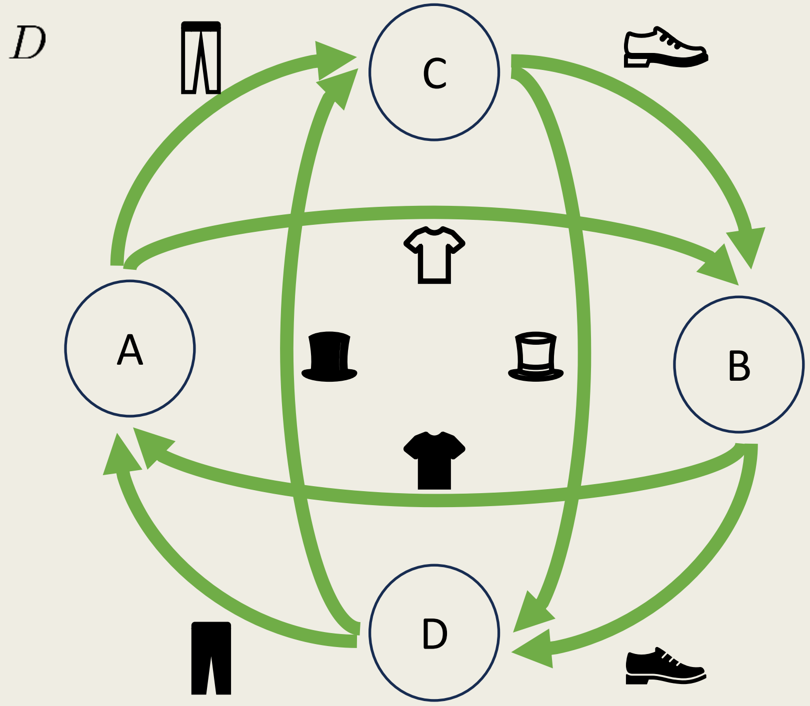
G dominates D: each party in G ends at least as good as they do in D

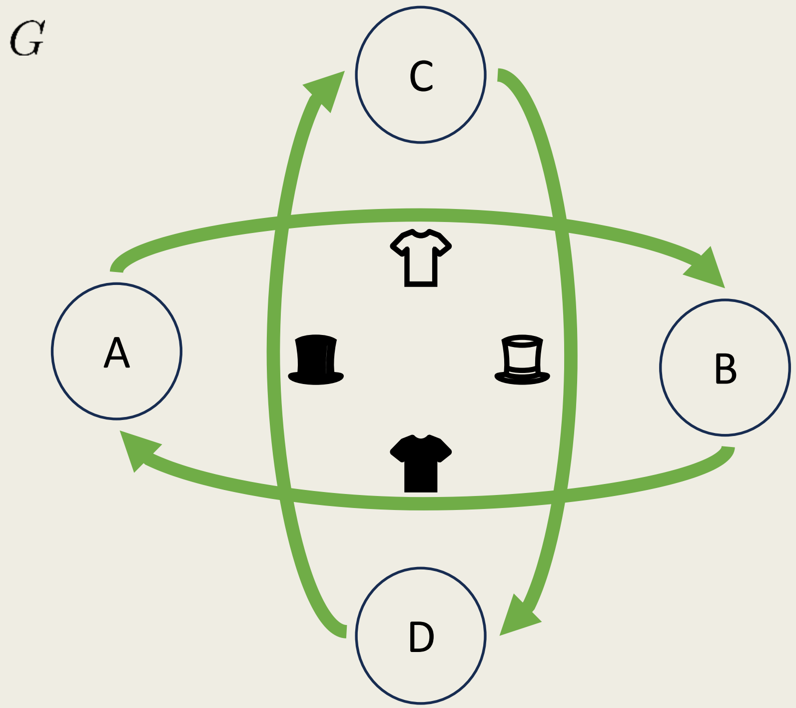




Condition 2

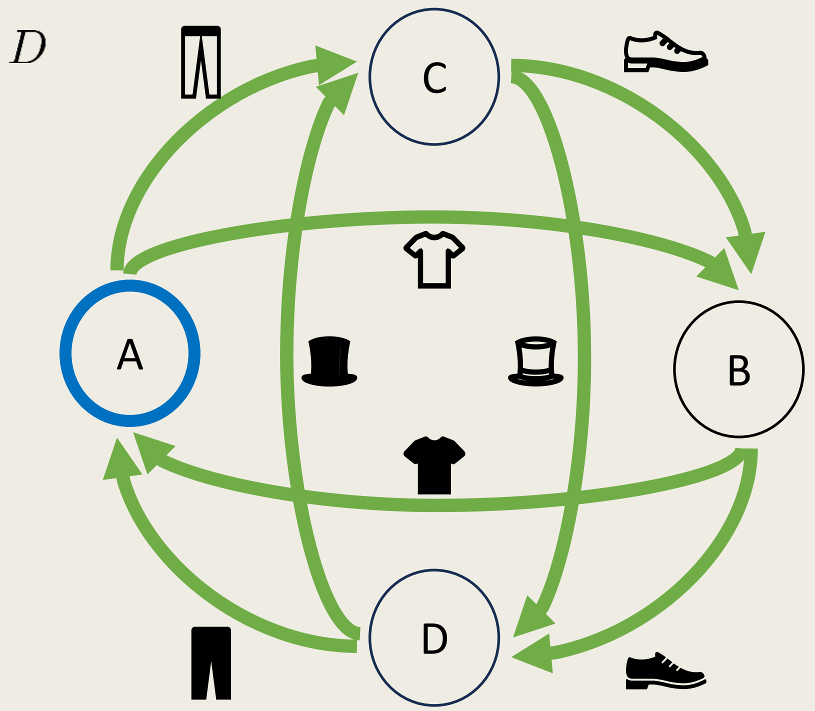
G dominates D: each party in G ends at least as good as they do in D

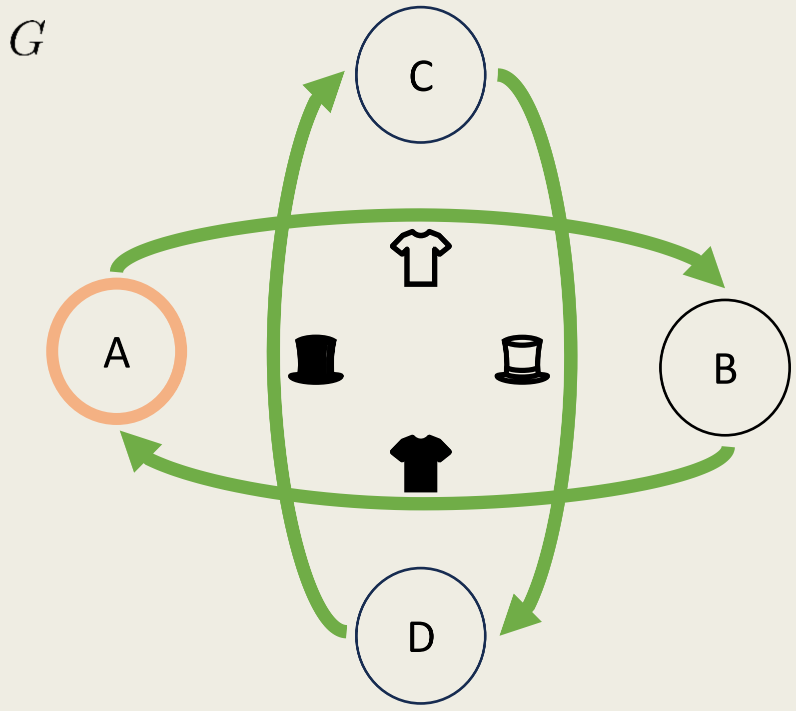




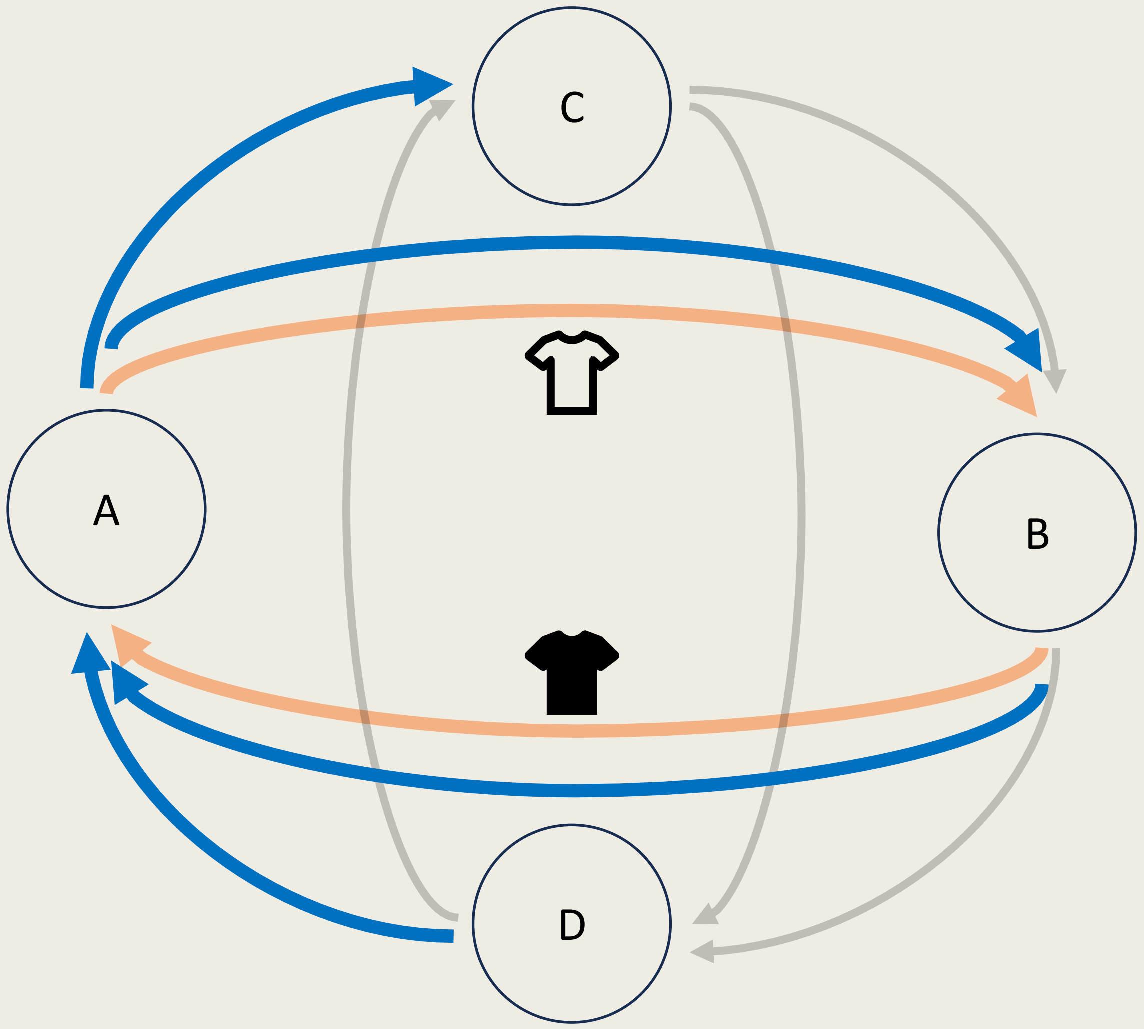
Condition 2

G dominates D: each party in G ends at least as good as they do in D

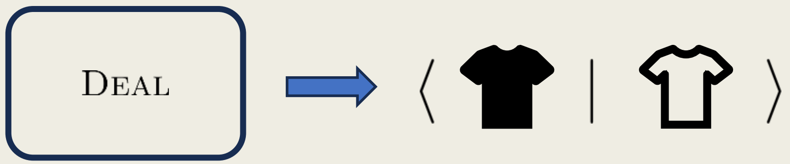




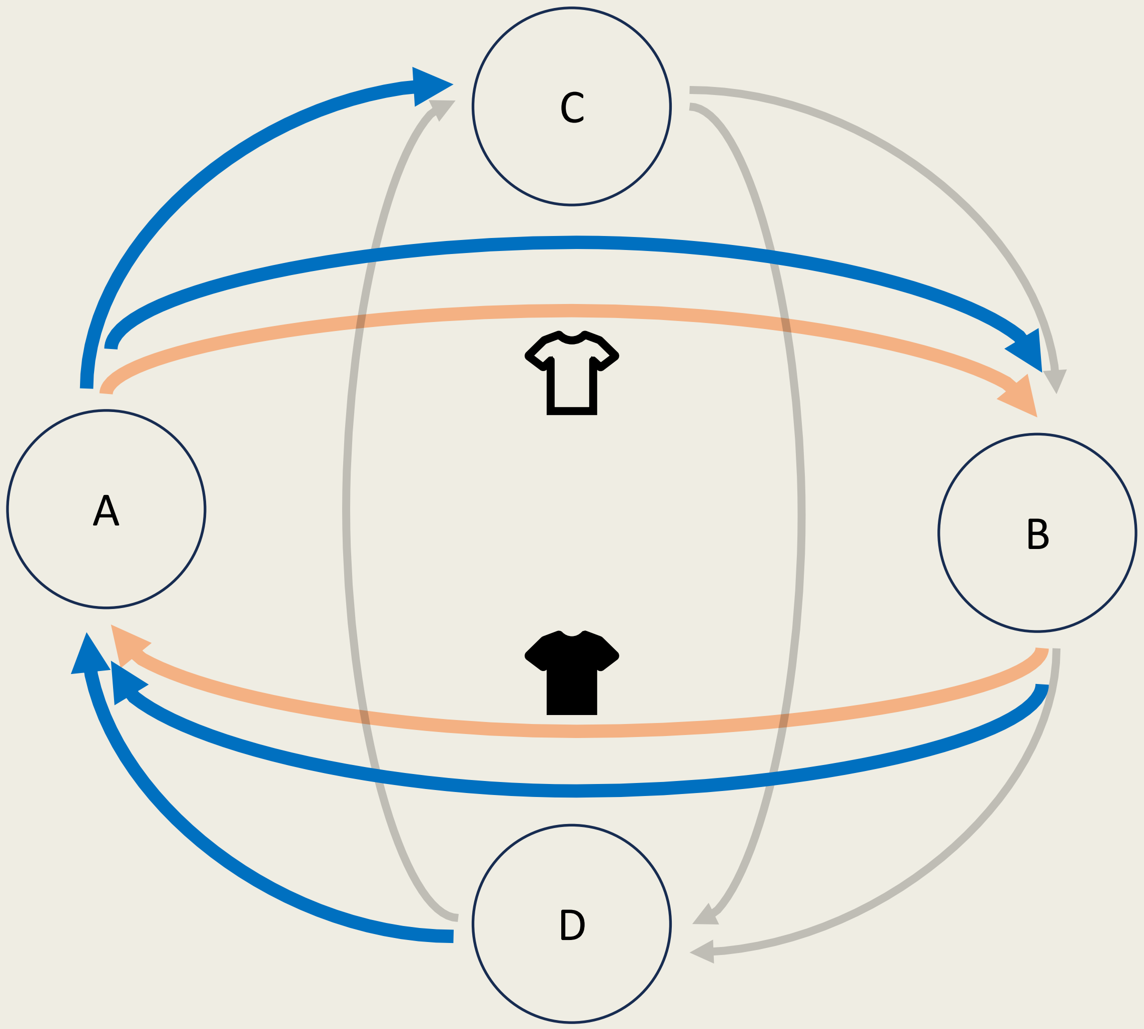
Condition 2



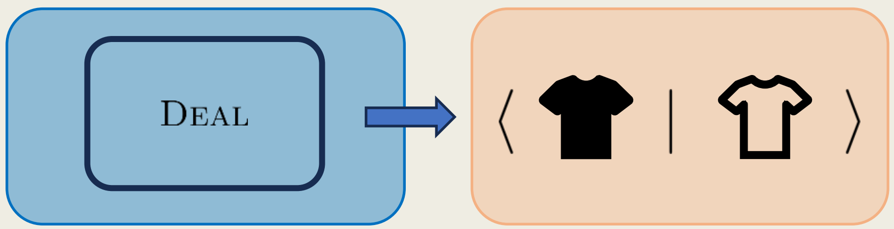
Preference of A:



Condition 2

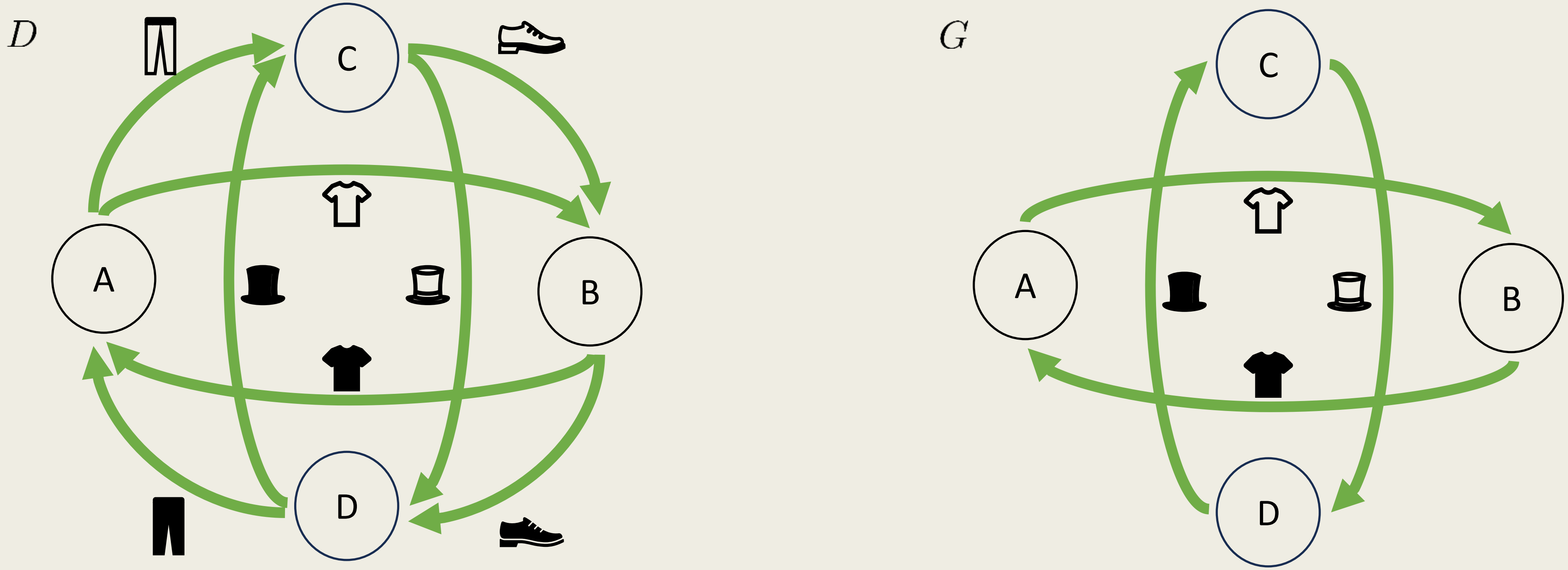


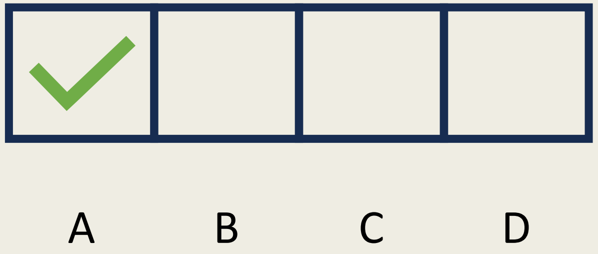
Preference of A:



Condition 2

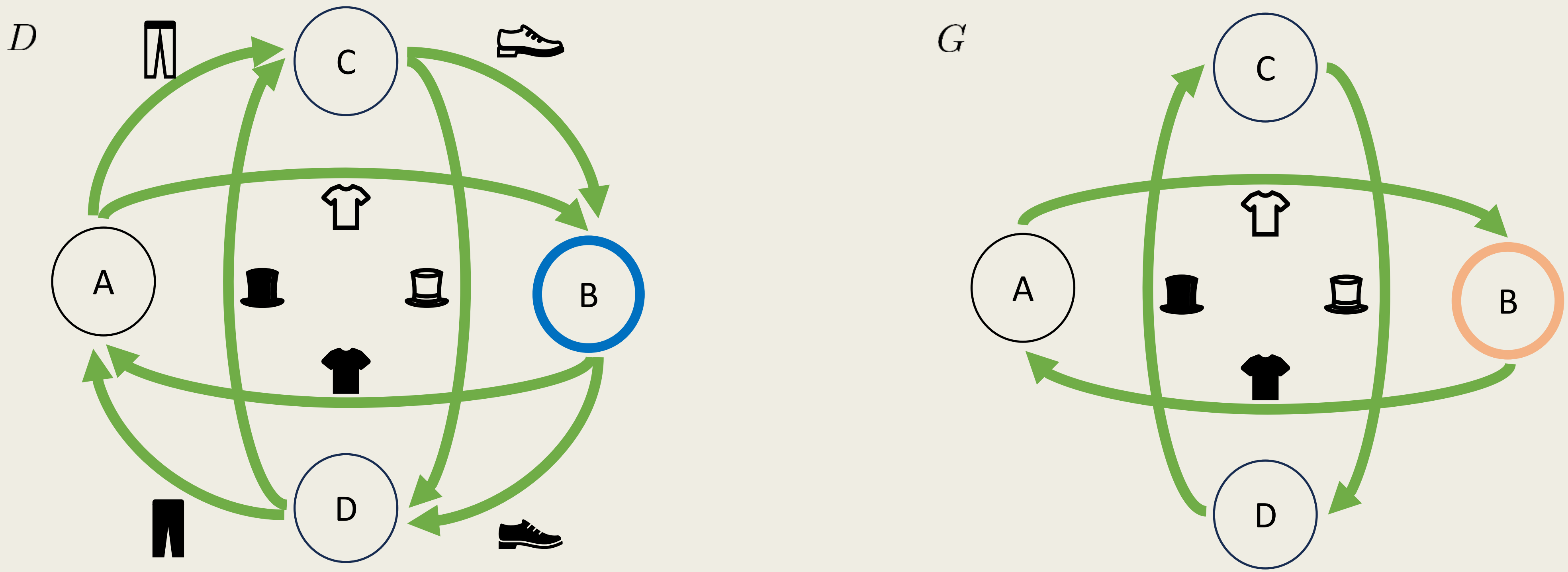
G dominates D: each party in G ends at least as good as they do in D



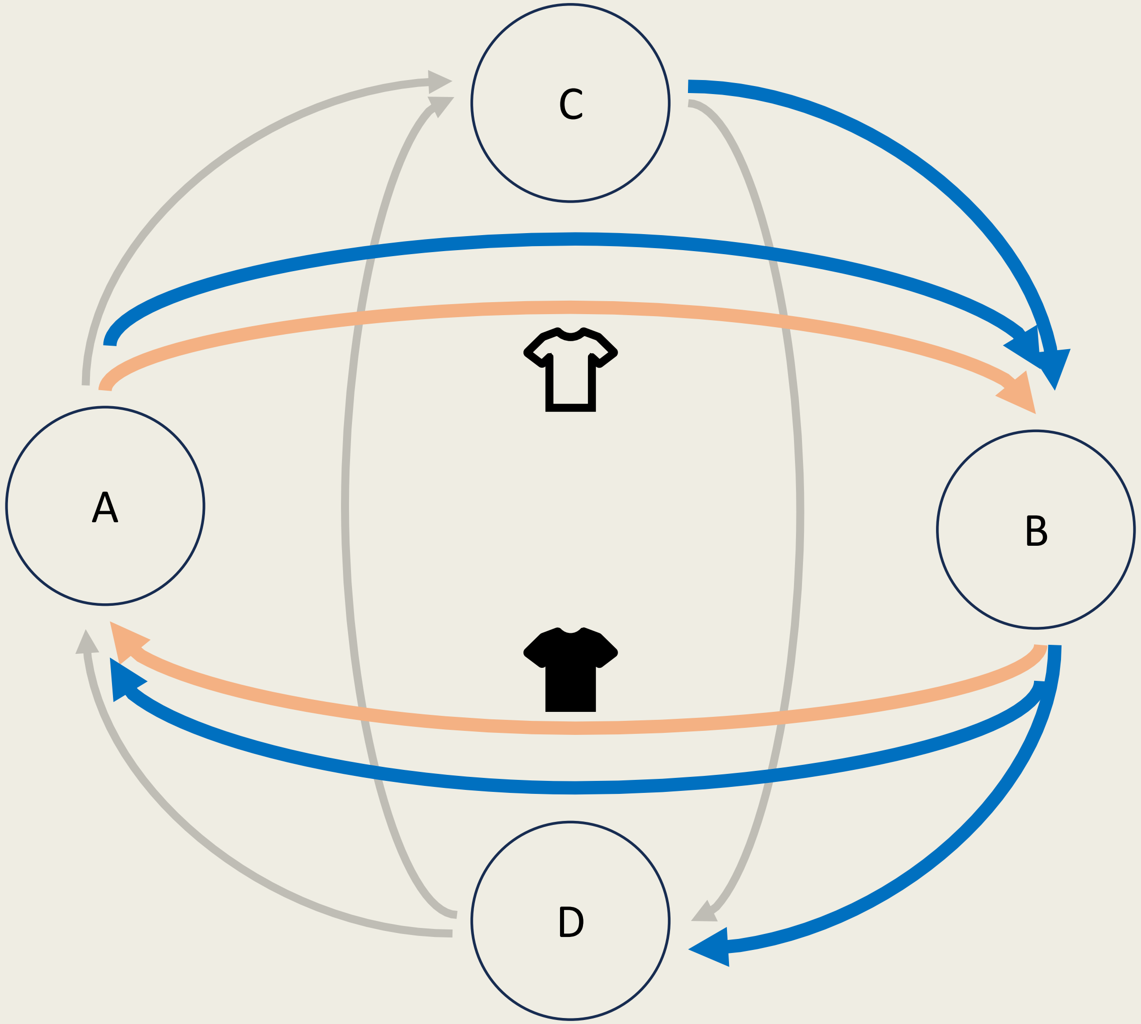


Condition 2

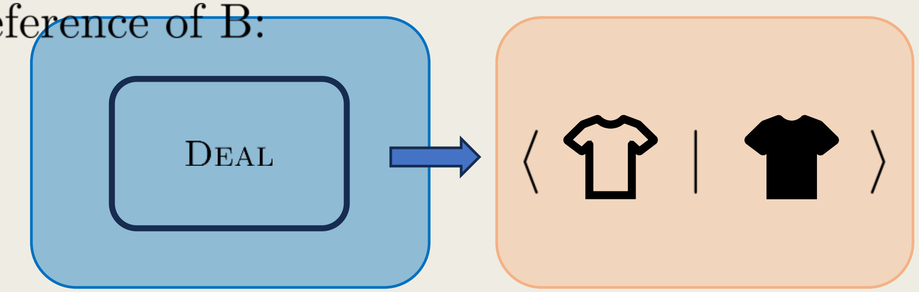
G dominates D: each party in G ends at least as good as they do in D



Condition 2

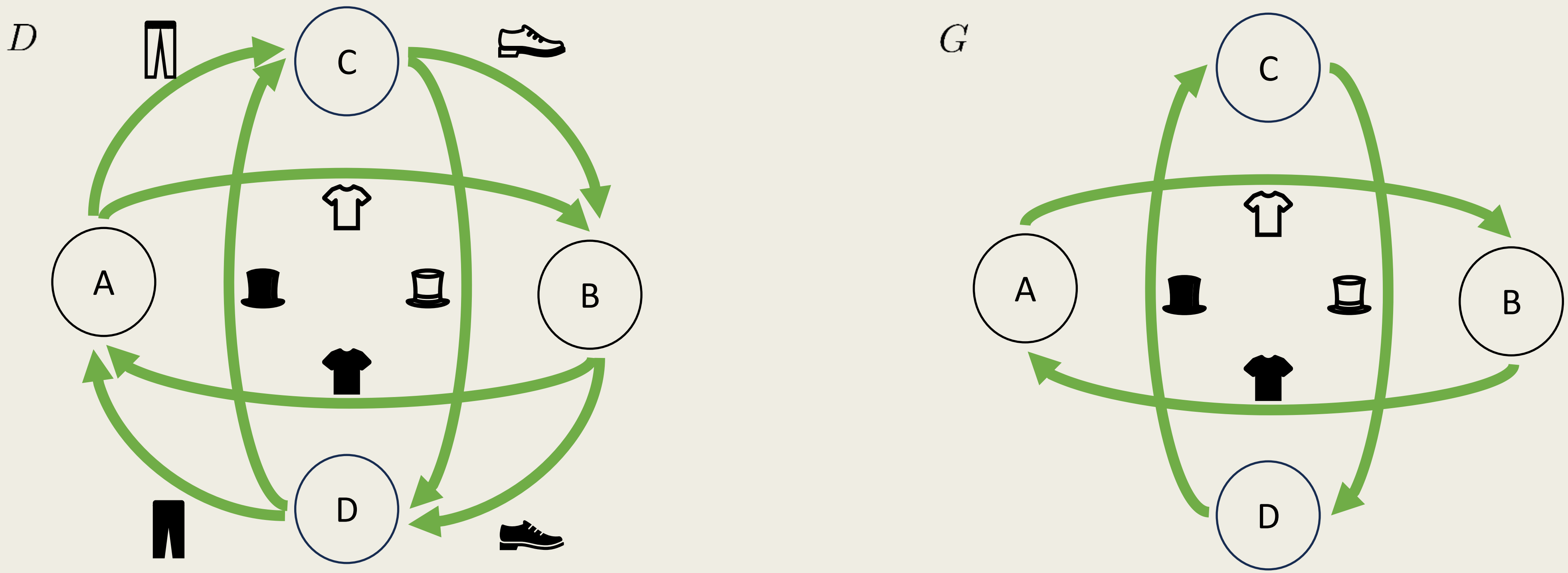


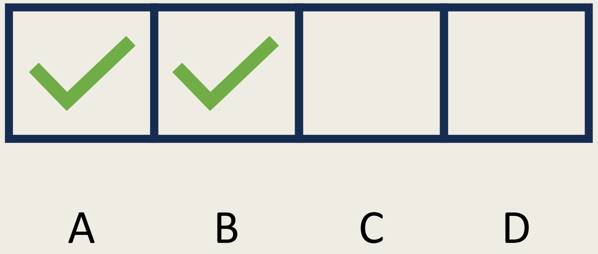
Preference of B:



Condition 2

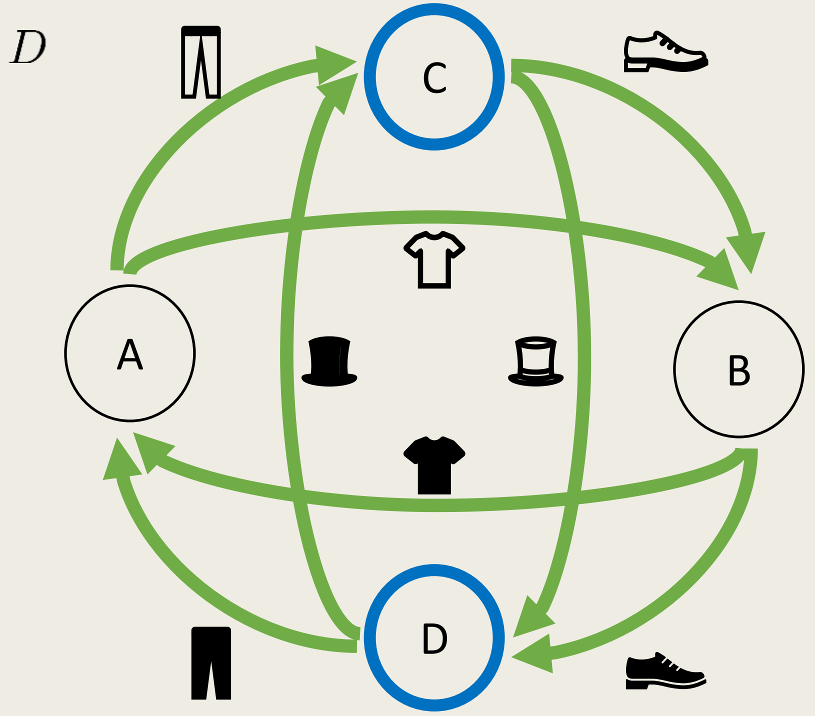
G dominates D: each party in G ends at least as good as they do in D

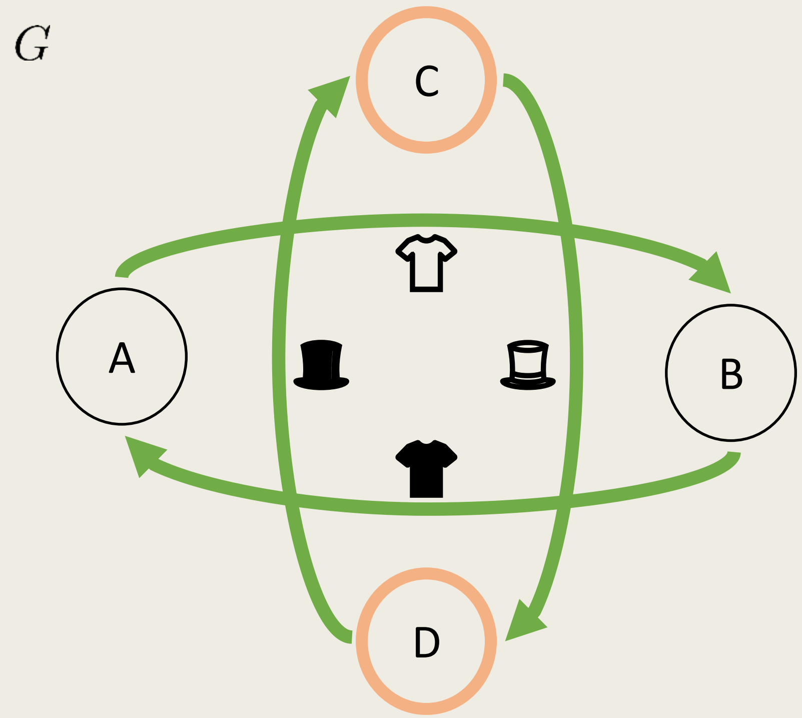


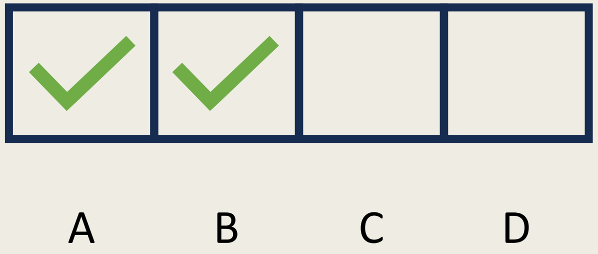


Condition 2

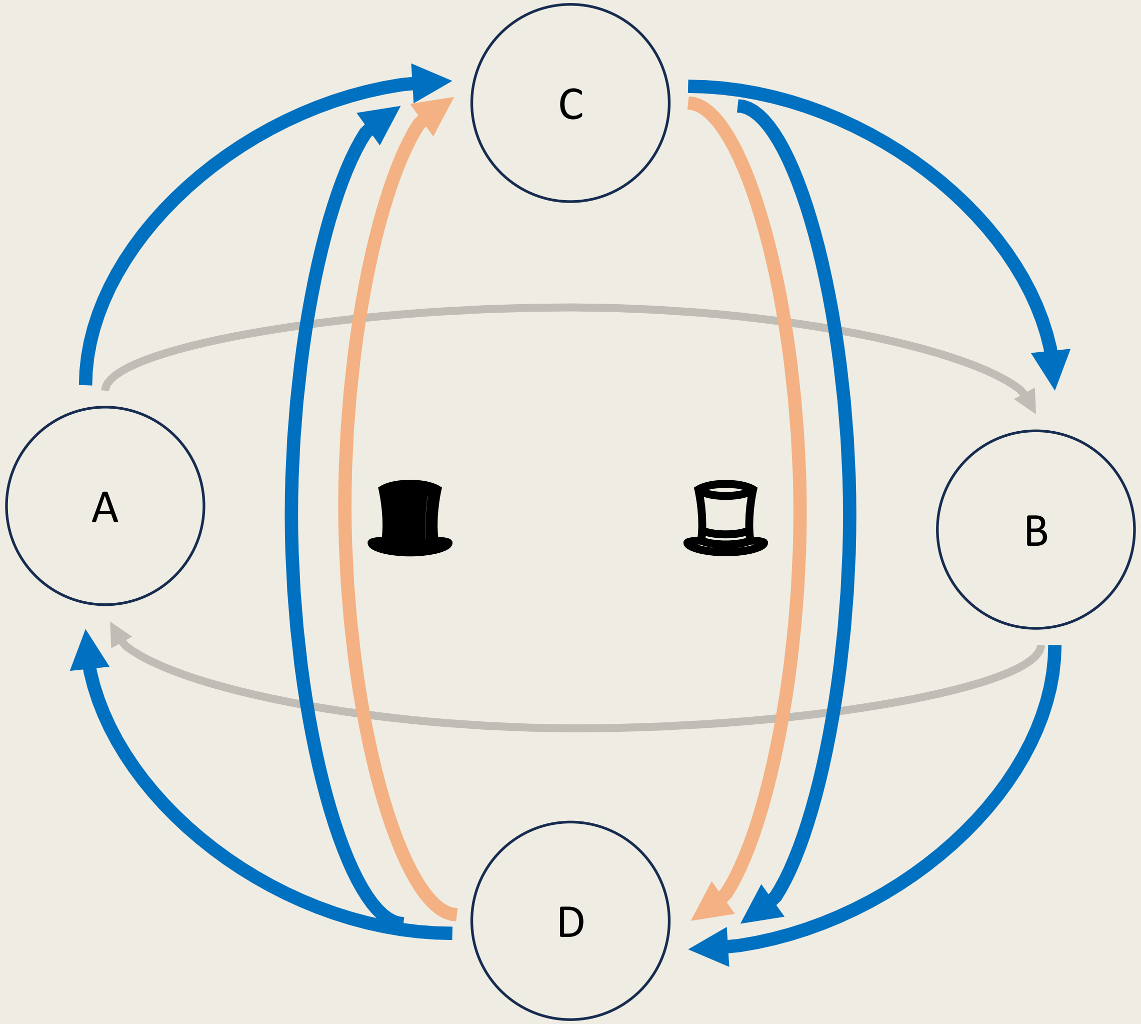
G dominates D: each party in G ends at least as good as they do in D

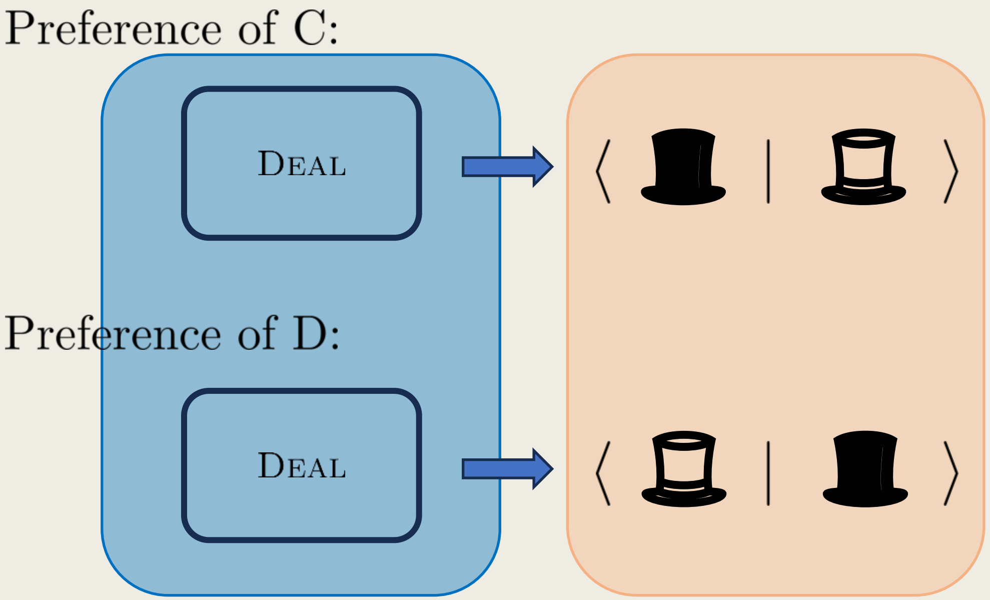






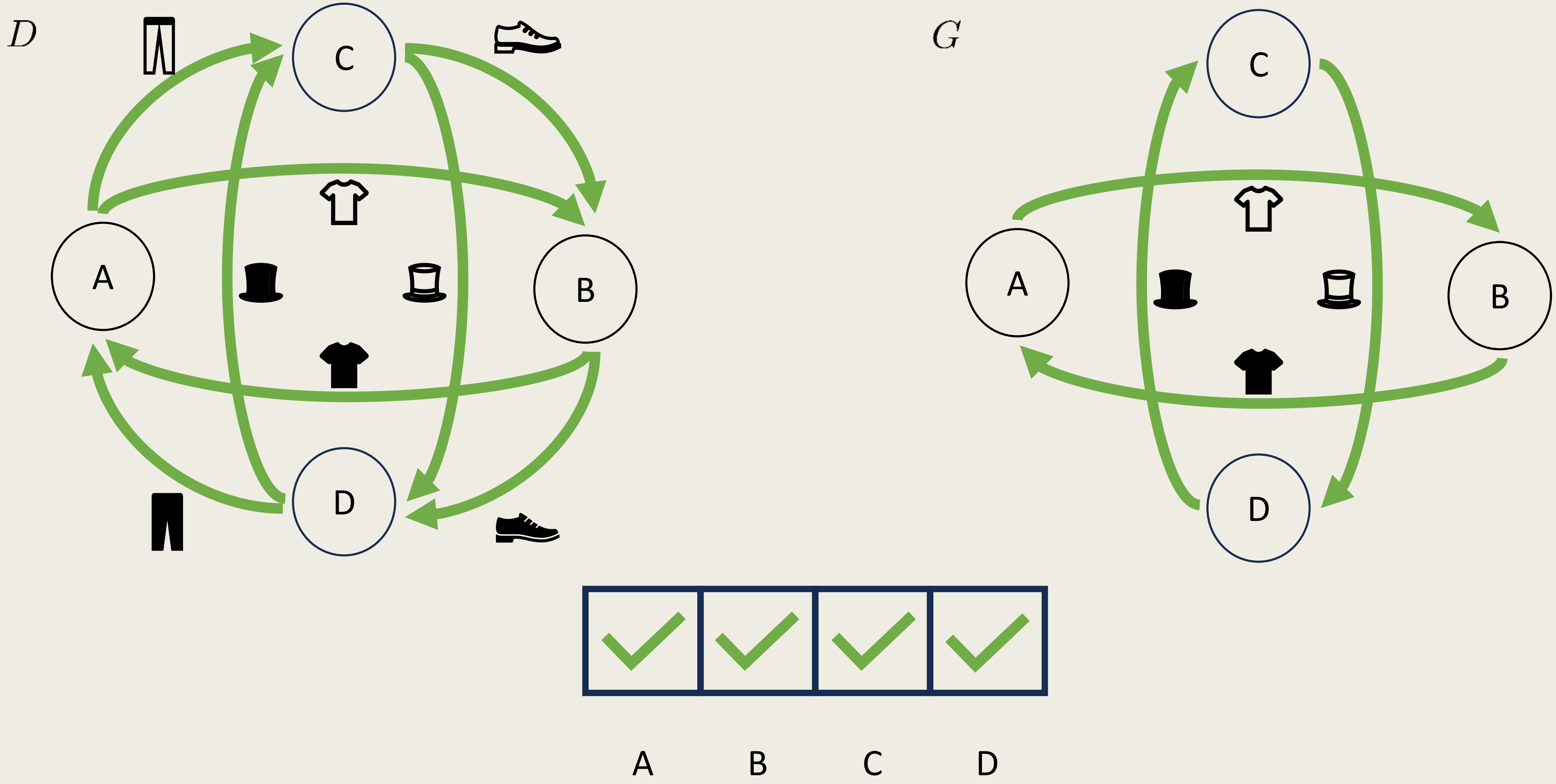
Condition 2





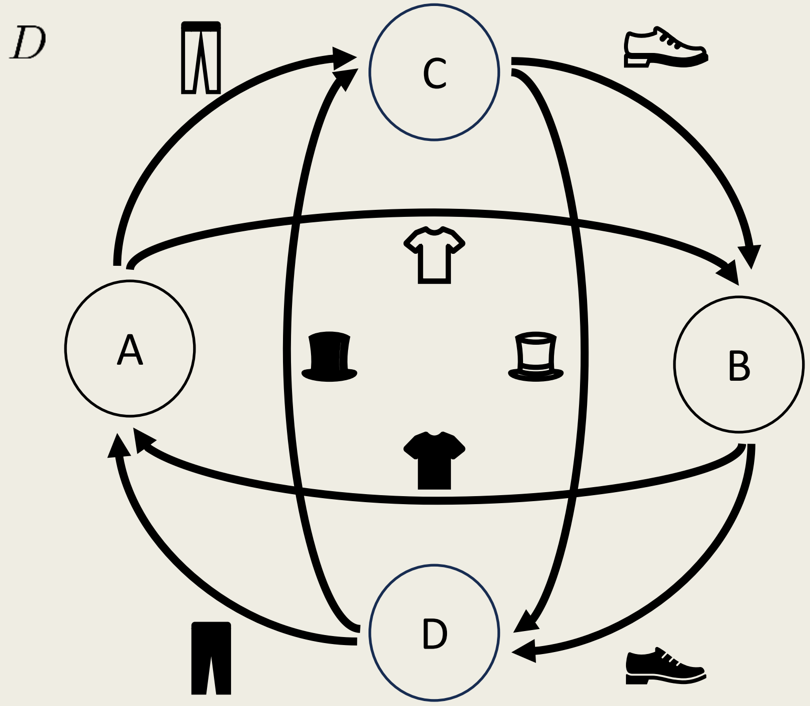
Condition 2

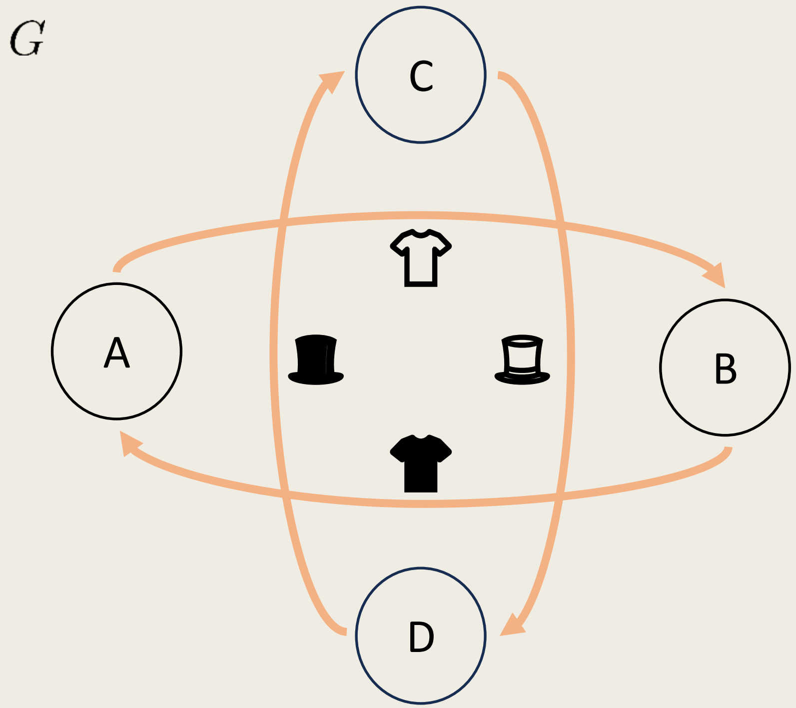
G dominates D: each party in G ends at least as good as they do in D



Condition 3

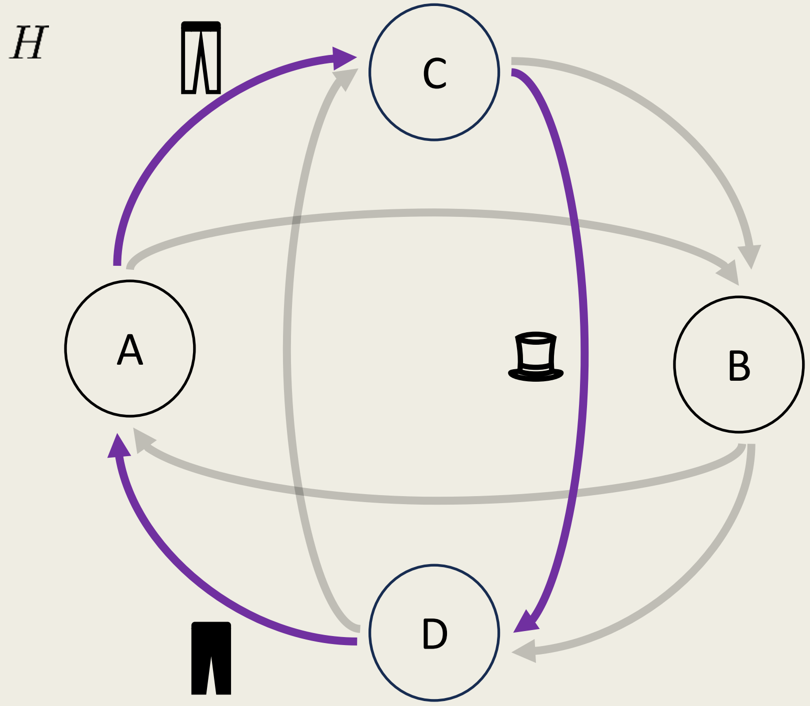
no subgraph H of D strictly dominates G

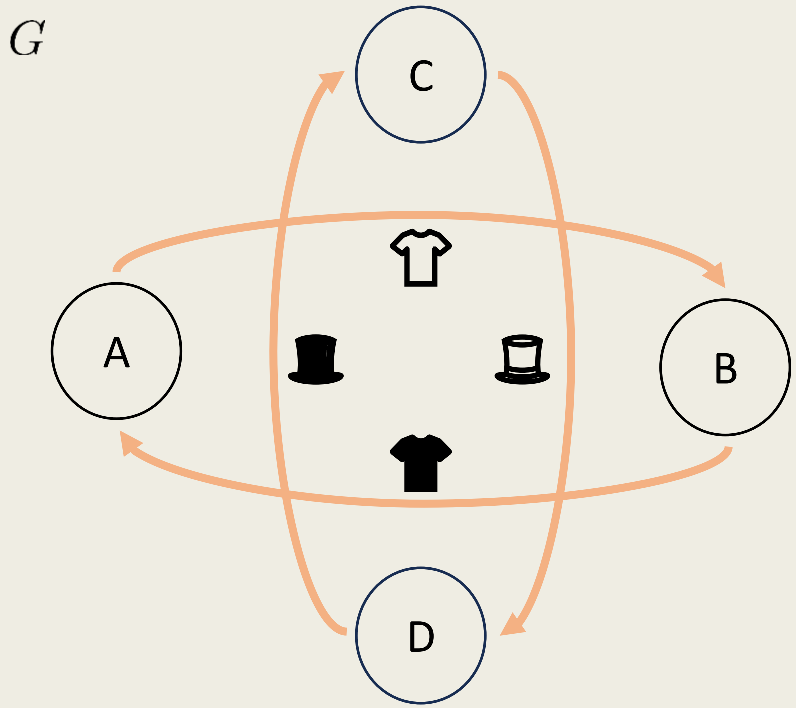




Condition 3

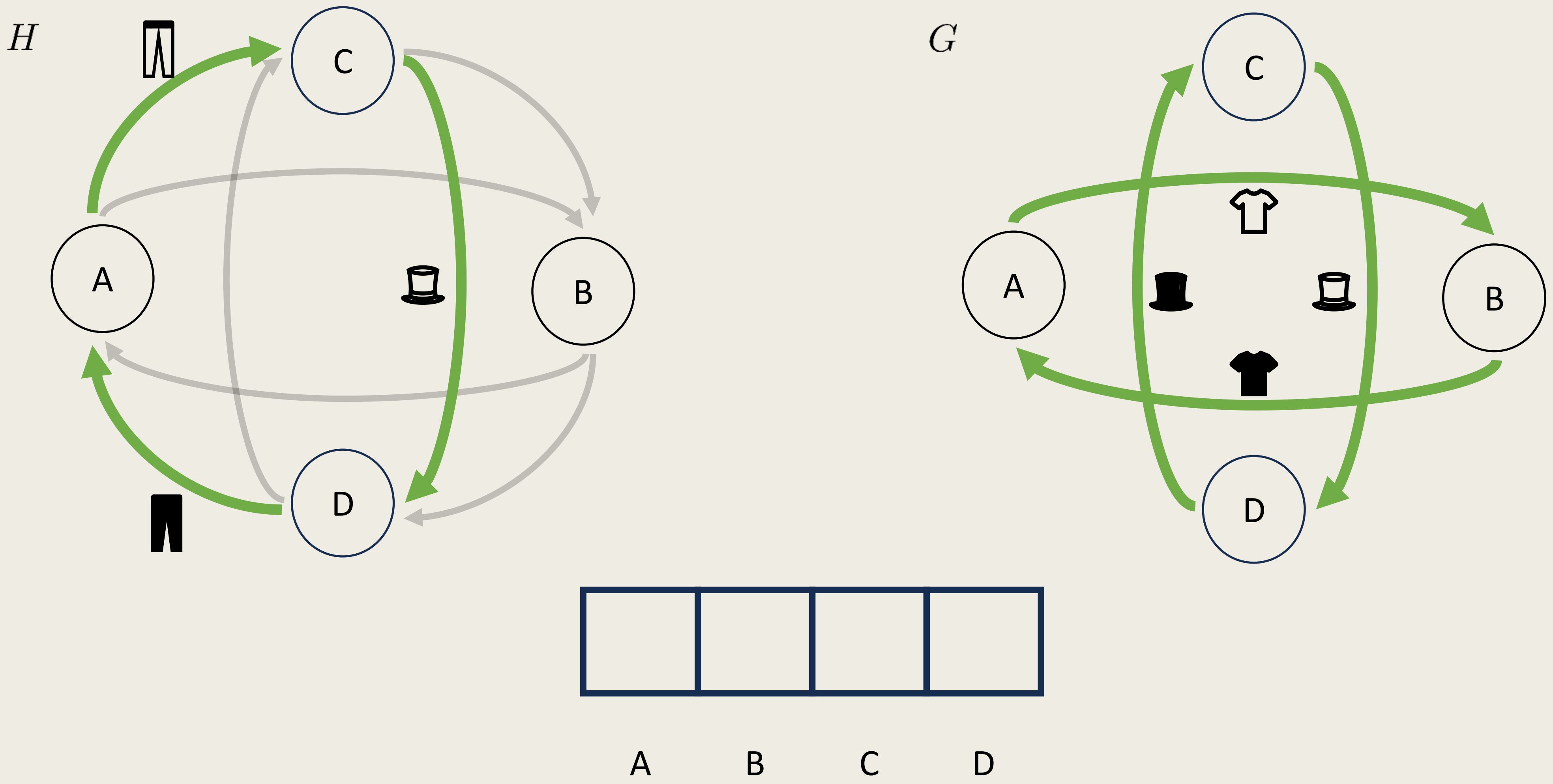
no subgraph H of D strictly dominates G



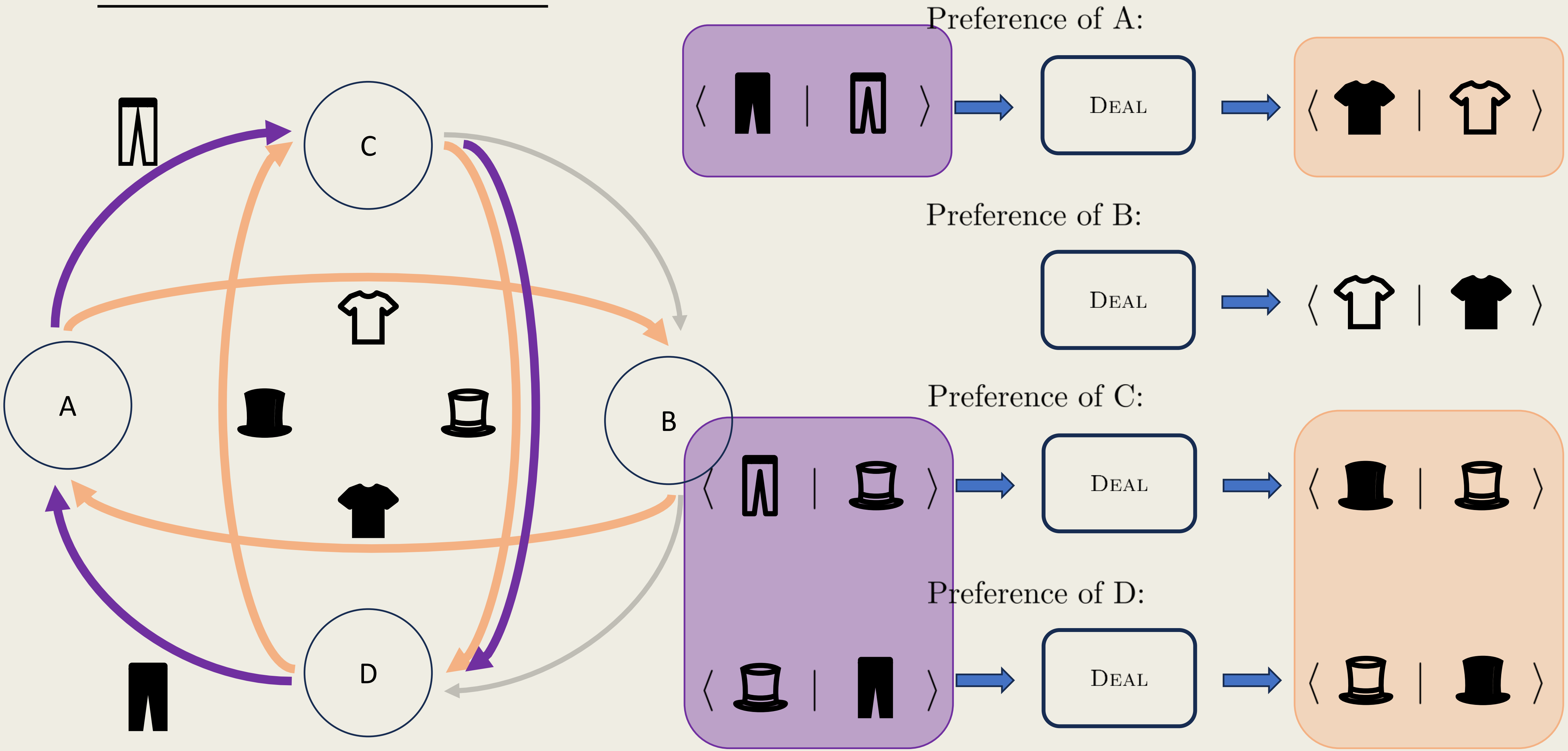


Condition 3

no subgraph H of D strictly dominates G

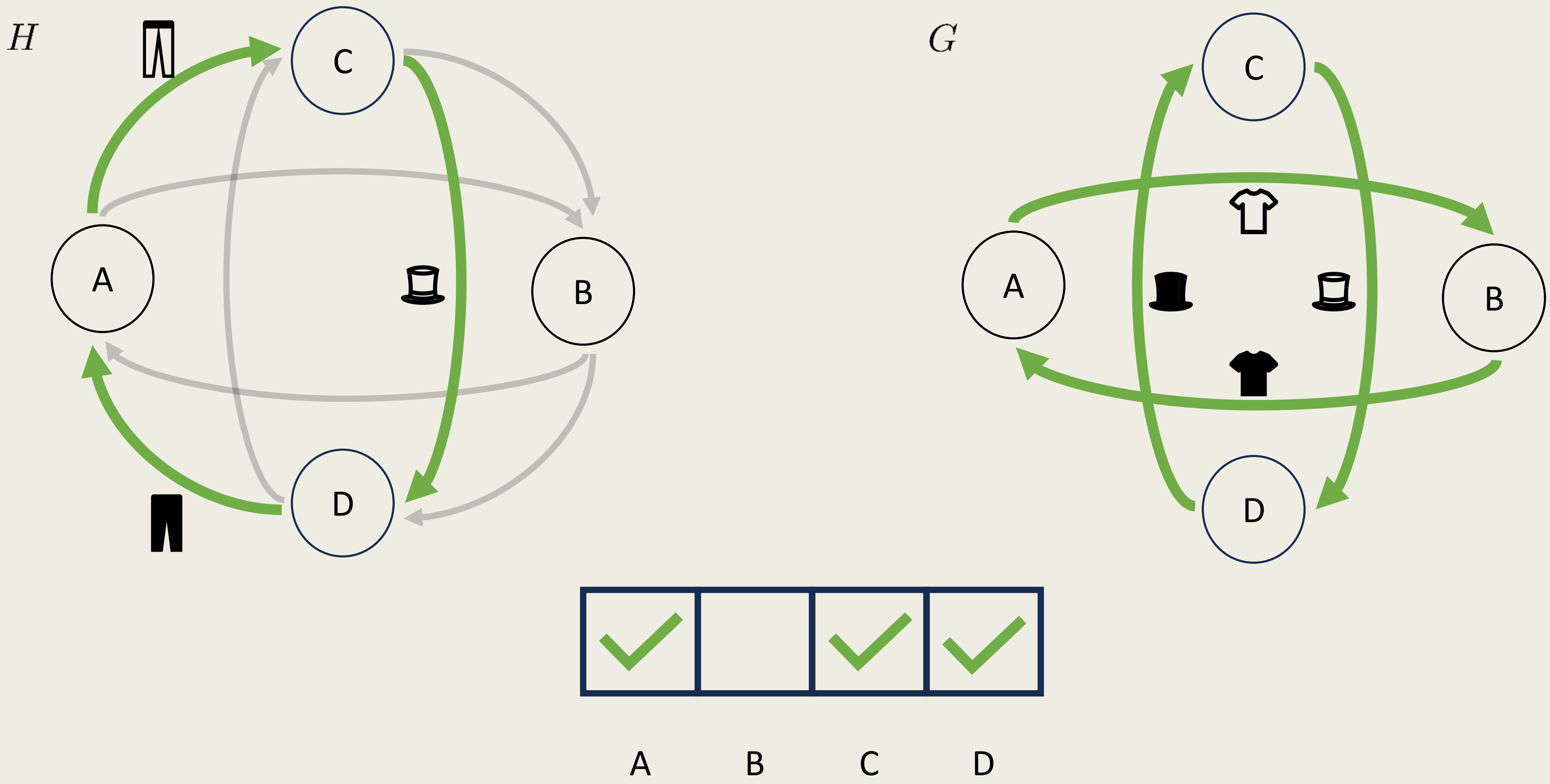


Condition 3


C
A
B
D
Preference of A:
DEAL
Preference of B:
DEAL
Preference of C:
DEAL
Preference of D:
DEAL

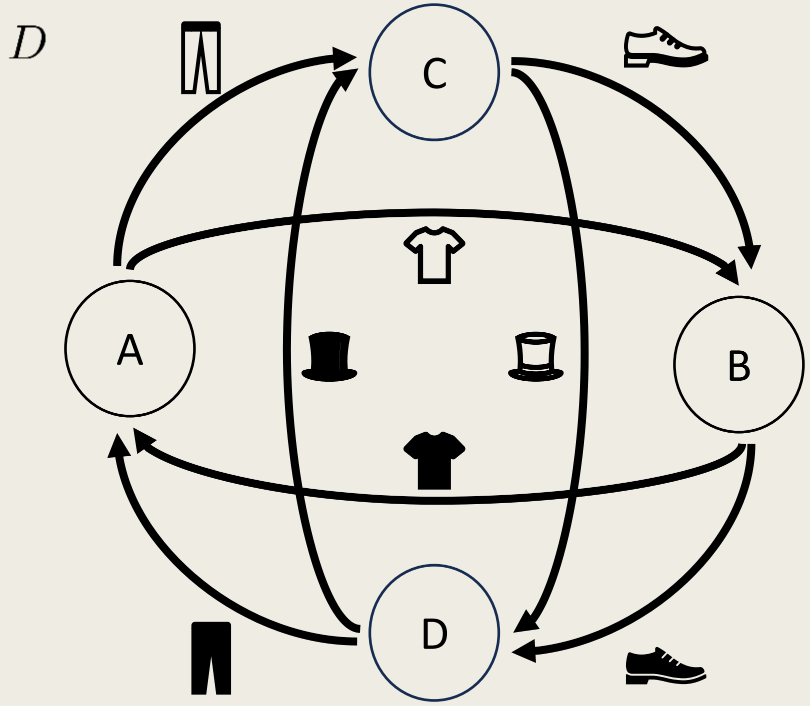
Condition 3

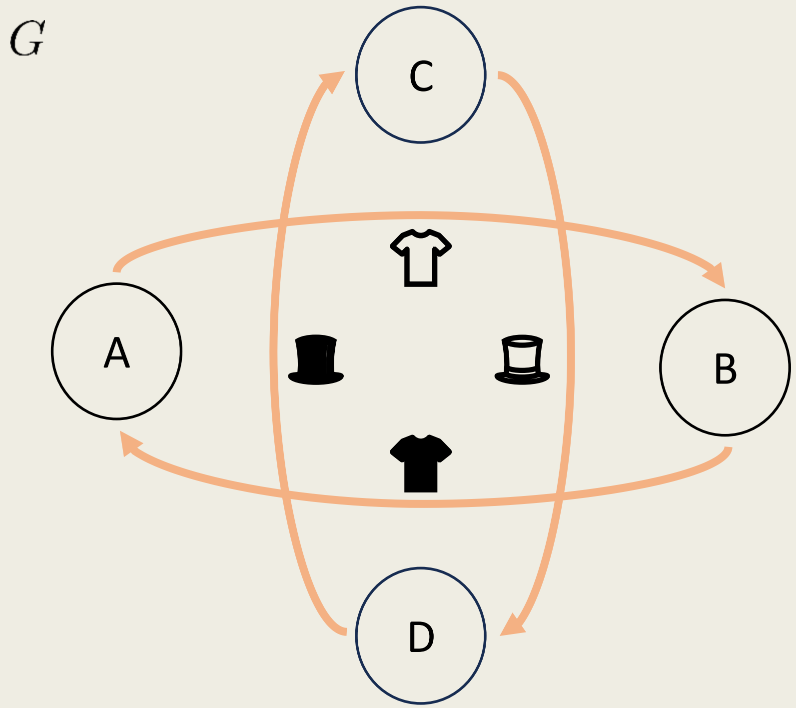
no subgraph H of D strictly dominates G



Condition 3

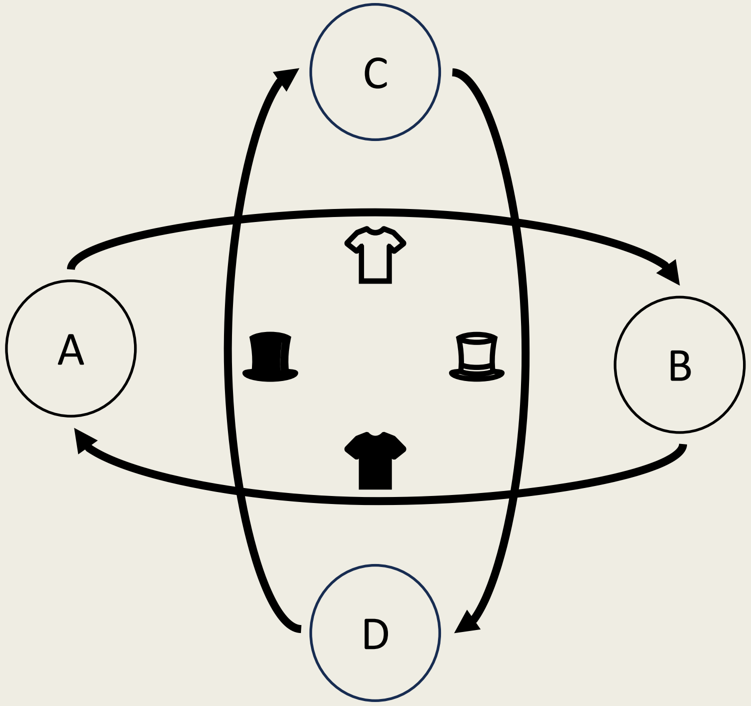
no subgraph H of D strictly dominates G



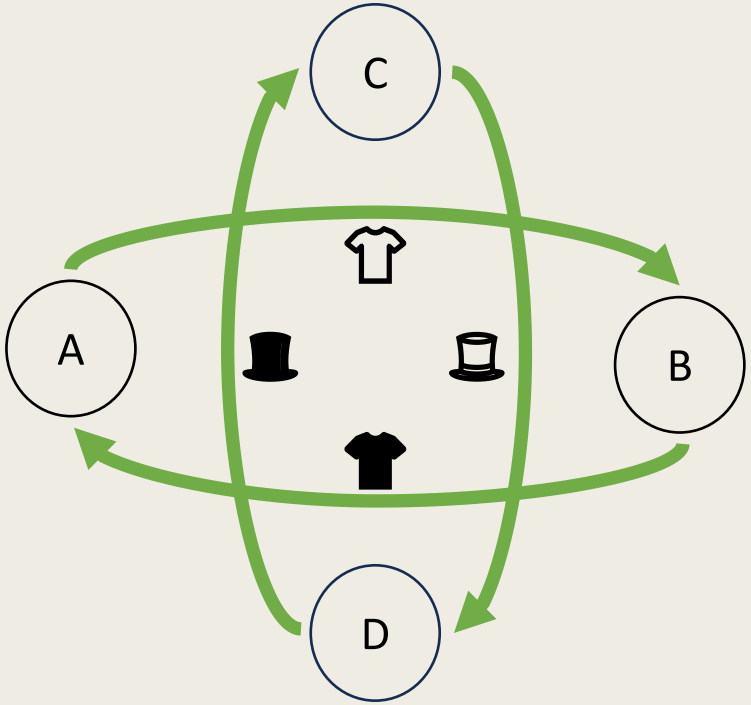


Protocol

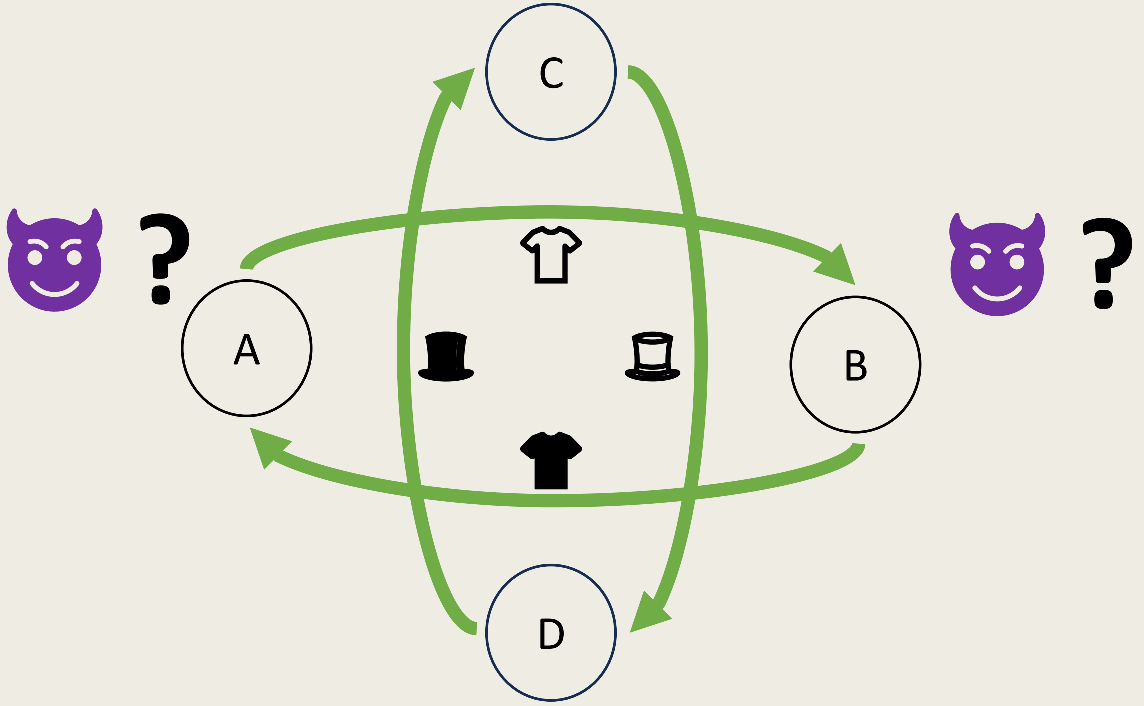
Applying Herlihy's Protocol



Applying Herlihy's Protocol

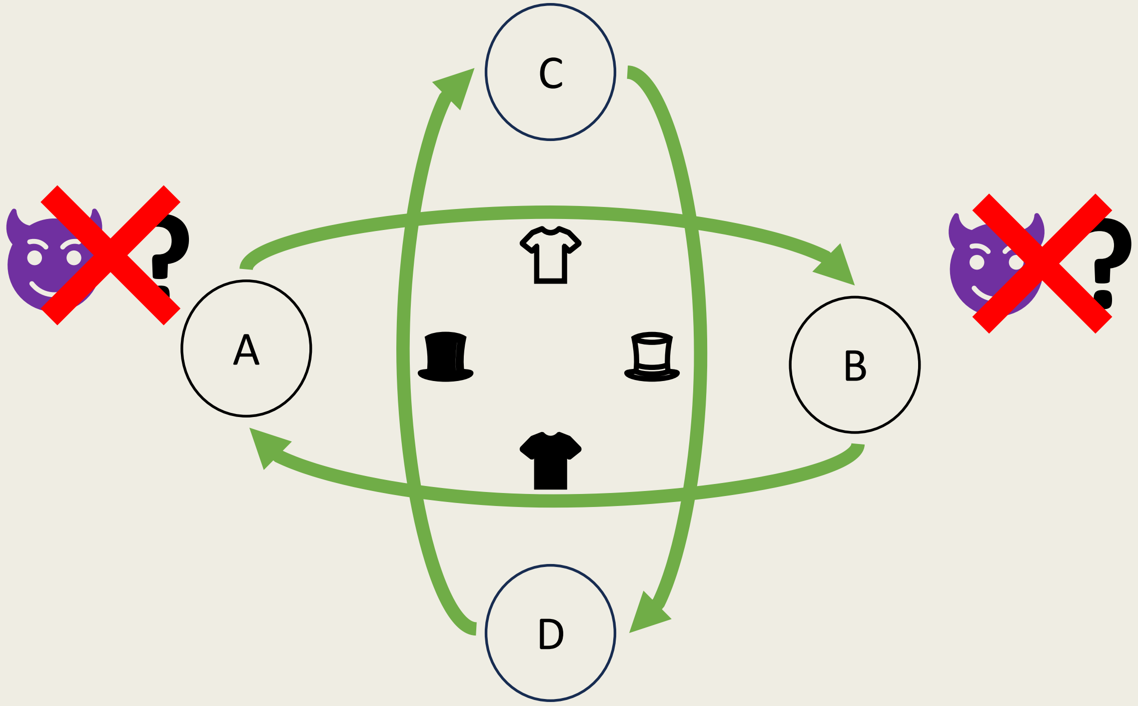


Applying Herlihy’s Protocol



Applying Herlihy's Protocol

Condition 3: no subgraph H of D strictly dominates G



Complexity

SwapAtomic

SwapAtomic:

- **input**: swap system $S = (D, P)$
- **output**: YES if S has an atomic swap protocol, otherwise NO

SwapAtomic

SwapAtomic:

- **input**: swap system $S = (D, P)$
- **output**: YES if S has an atomic swap protocol, otherwise NO

Theorem. SwapAtomic is Σ_2^{P}-complete.

Σ_2^{P}-completeness

Theorem. $S = (D, P)$ has an atomic protocol **iff** there exists a spanning subgraph G of D such that:

- G is piece-wise strongly connected and has no isolated vertices
- G dominates D
- no subgraph H of D strictly dominates G

$$\exists G. \neg \exists H. \pi(G, H)$$

Σ_2^{P}-completeness

Theorem. $S = (D, P)$ has an atomic protocol **iff** there exists a spanning subgraph G of D such that:

- G is piece-wise strongly connected and has no isolated vertices
- G dominates D
- no subgraph H of D strictly dominates G

$$\exists G . \neg \exists H . \pi(G, H)$$

Σ_2^{P}-completeness

Theorem. $S = (D, P)$ has an atomic protocol **iff** there exists a spanning subgraph G of D such that:

- G is piece-wise strongly connected and has no isolated vertices
- G dominates D
- no subgraph H of D strictly dominates G

$$\exists G . \neg \exists H . \pi(G, H)$$

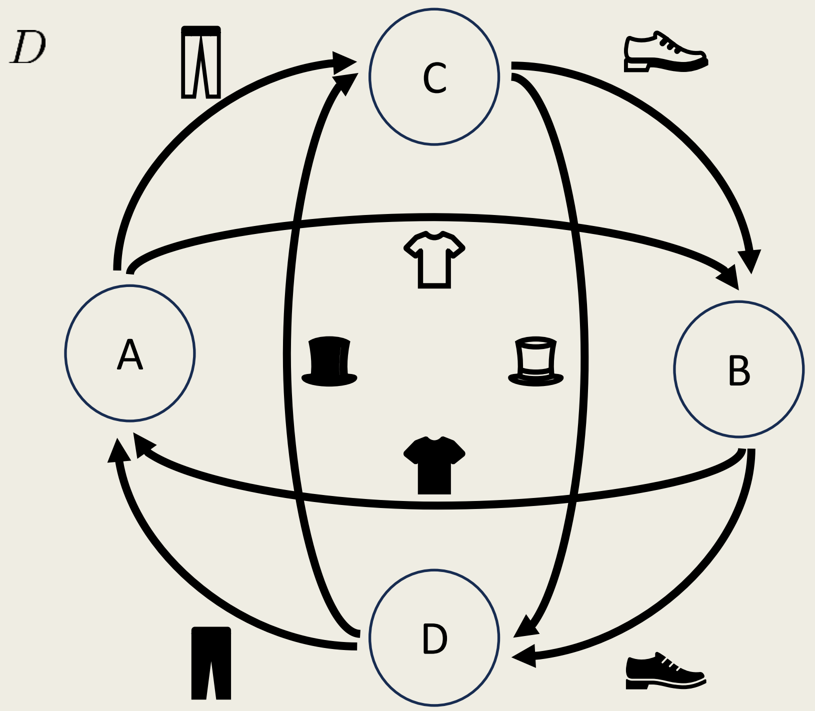
Σ_2^{P}-completeness

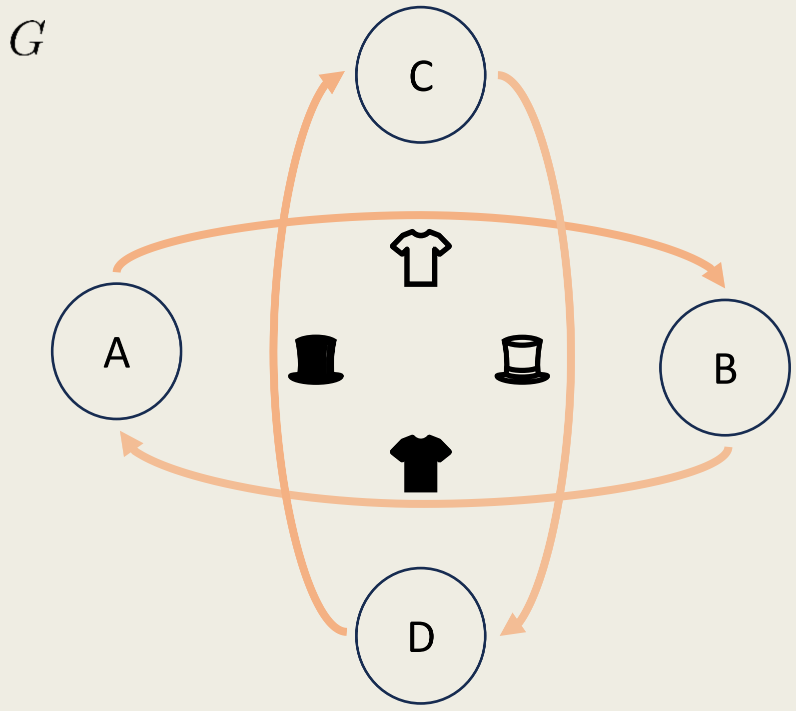
Theorem. $S = (D, P)$ has an atomic protocol **iff** there exists a spanning subgraph G of D such that:

- G is piece-wise strongly connected and has no isolated vertices
- G dominates D
- no subgraph H of D strictly dominates G

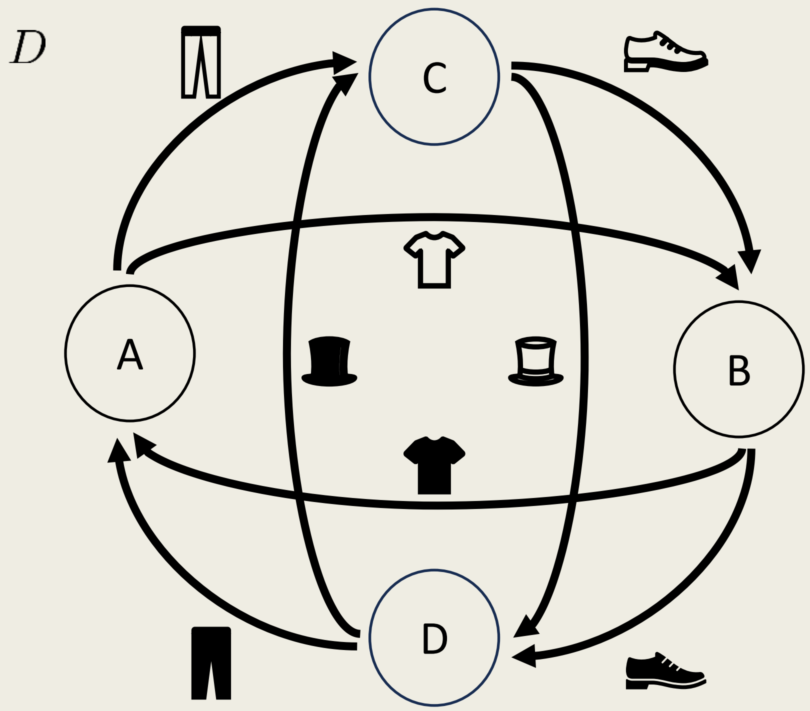
$$\exists G. \neg \exists H. \pi(G, H)$$

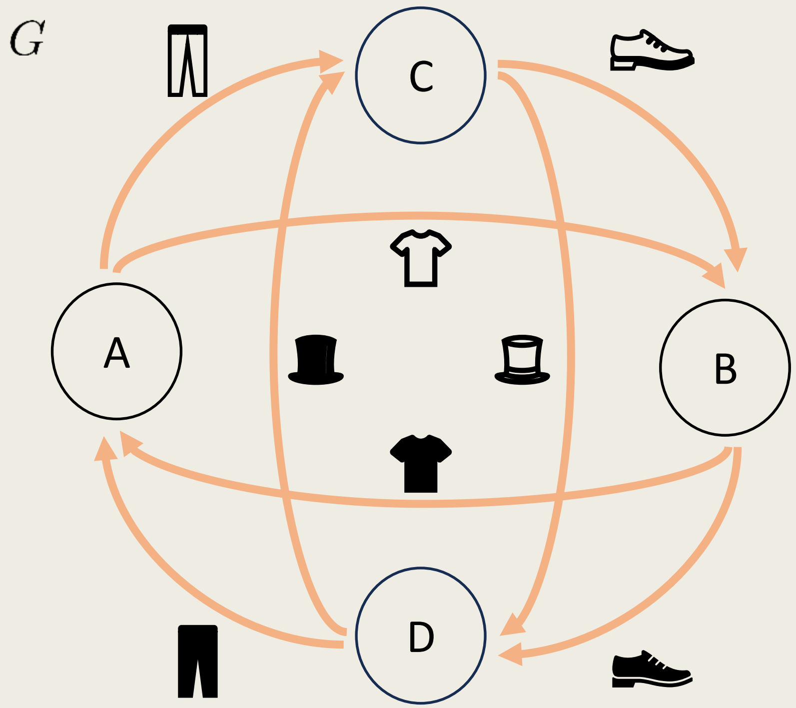
Example



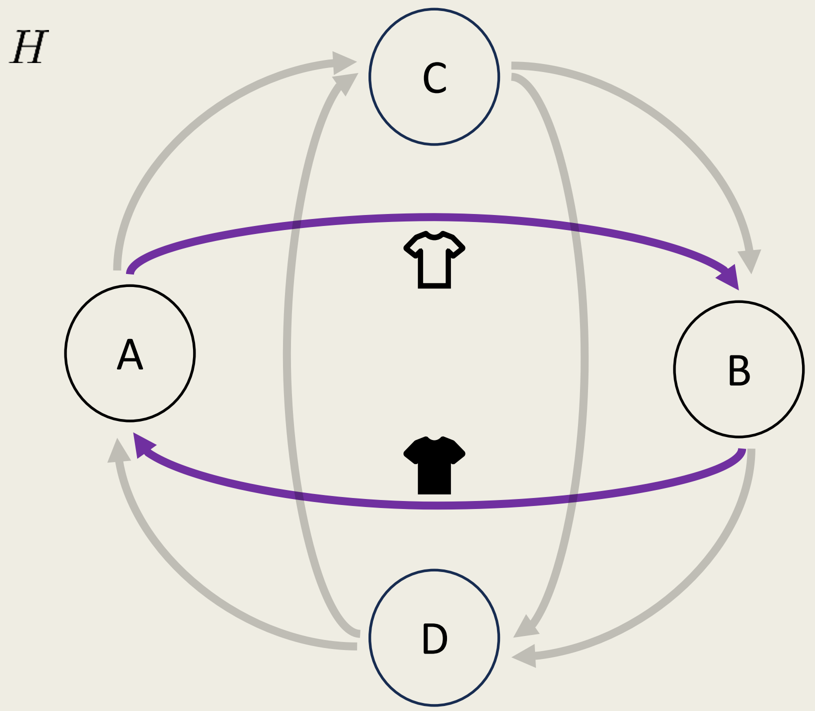


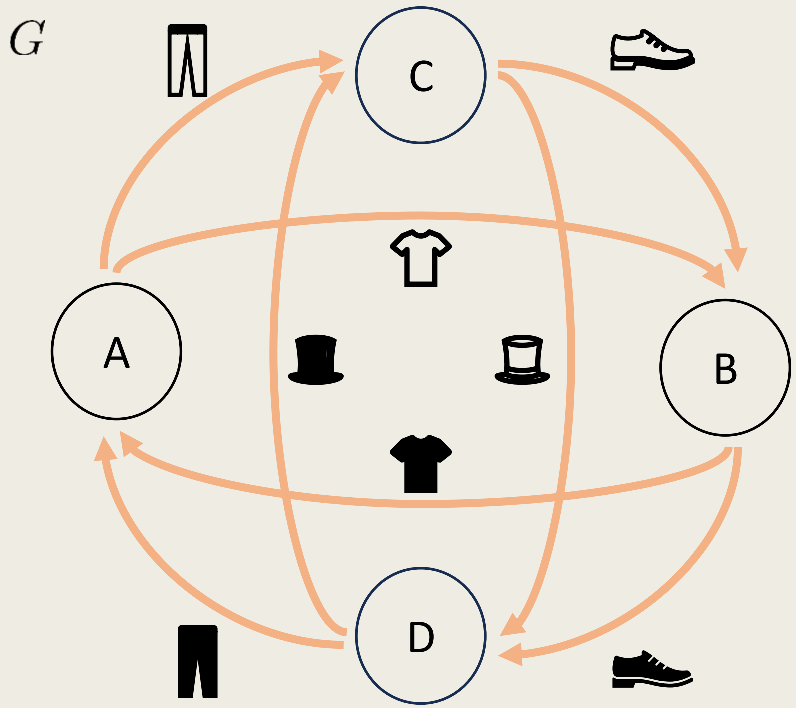
Example





Example





Summary

- Relax structure of preference posets
- Characterize when swap systems have an atomic protocol
- If there is an atomic protocol, we give one
- Complexity of deciding whether a swap system has an atomic protocol

Thank You