Byzantine Stable Matching

Andrei Constantinescu
Marc Dufay
Diana Ghinea
Roger Wattenhofer



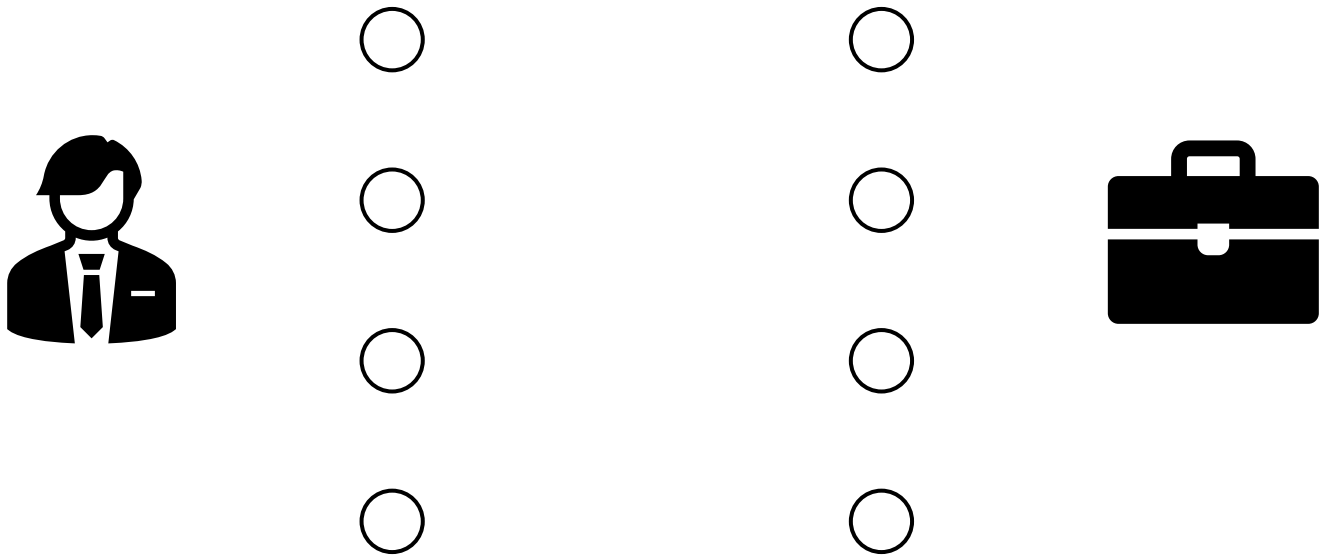

Distributed **Co**mputing Group
ETH zürich

PODC 2025

Matching

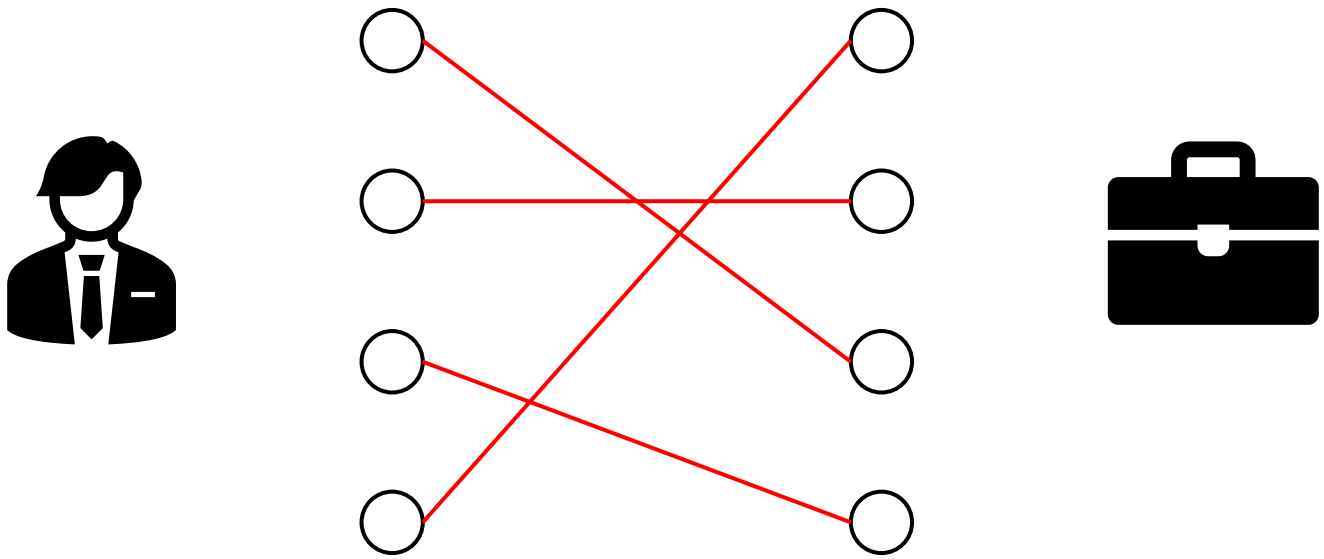
Matching

Matching: Match men and women, job applicants and job positions, kidney donors and receivers…

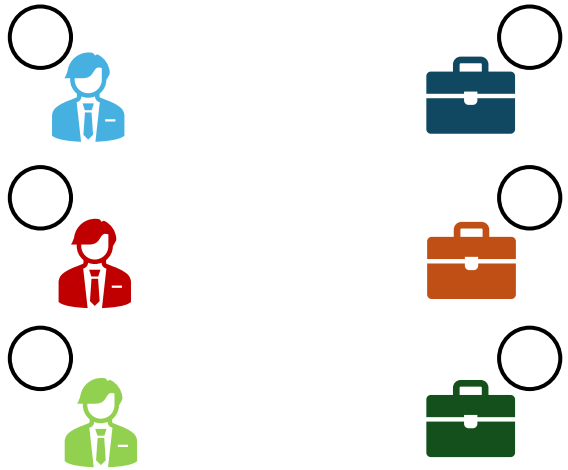


Matching

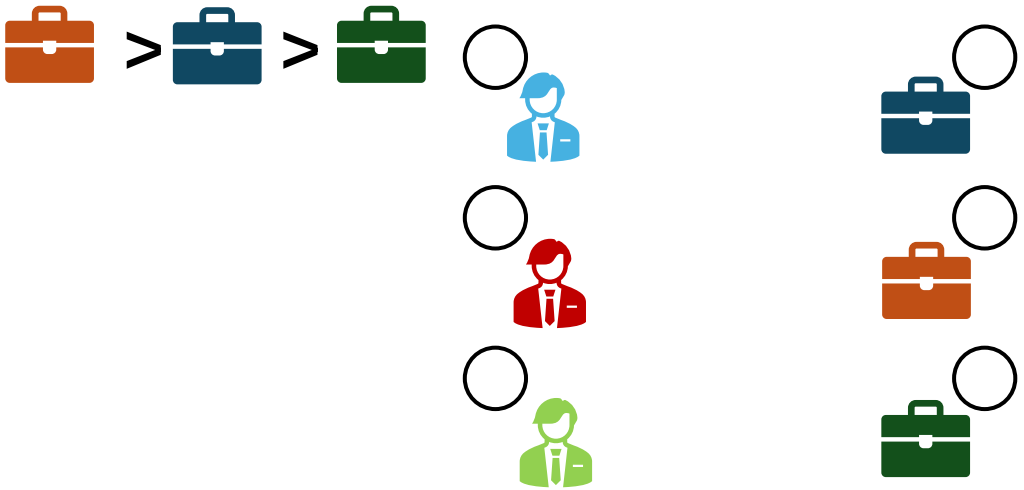
Matching: Match men and women, job applicants and job positions, kidney donors and receivers...



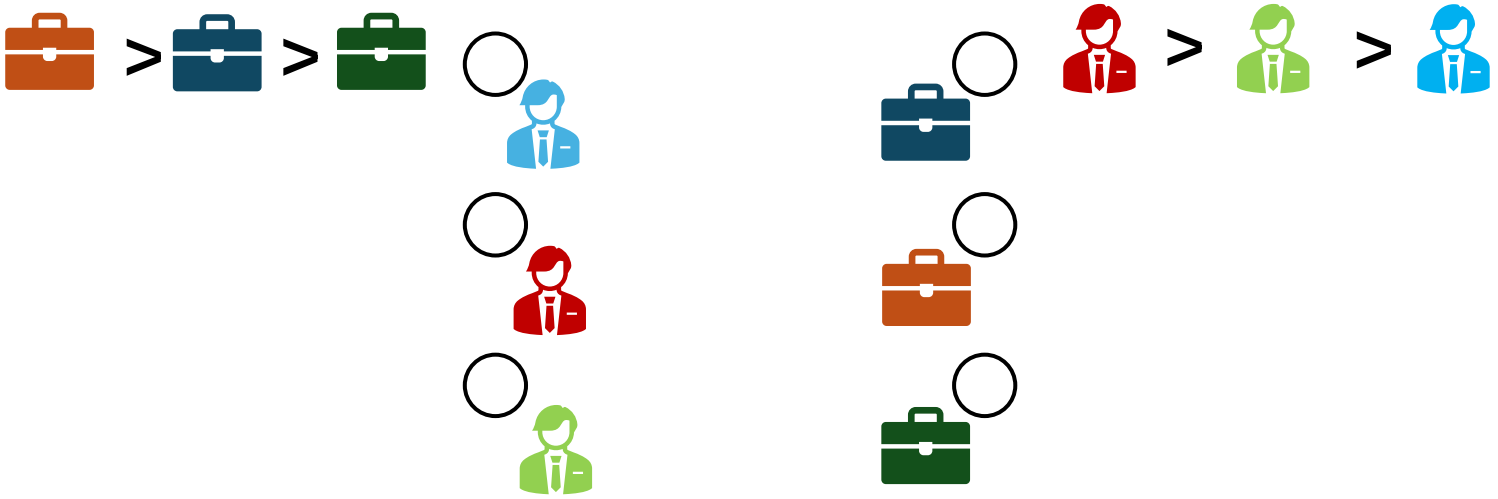
Preference ordering



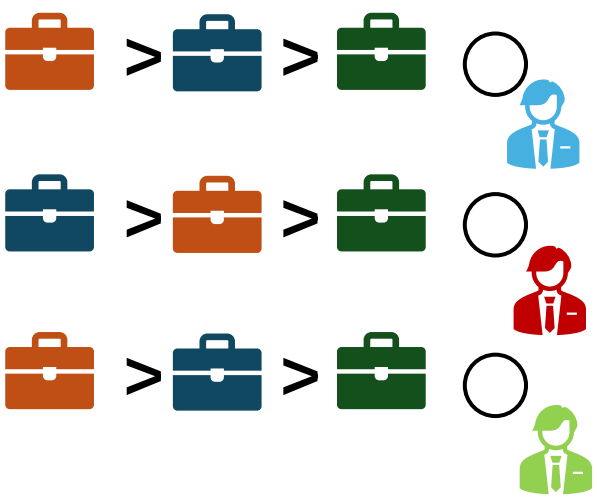
Preference ordering

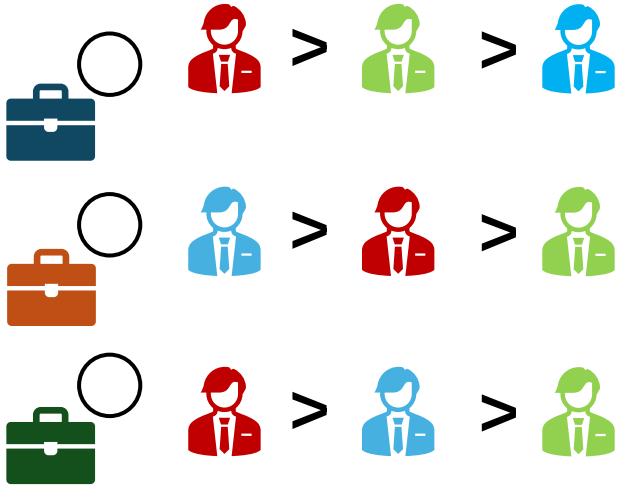


Preference ordering

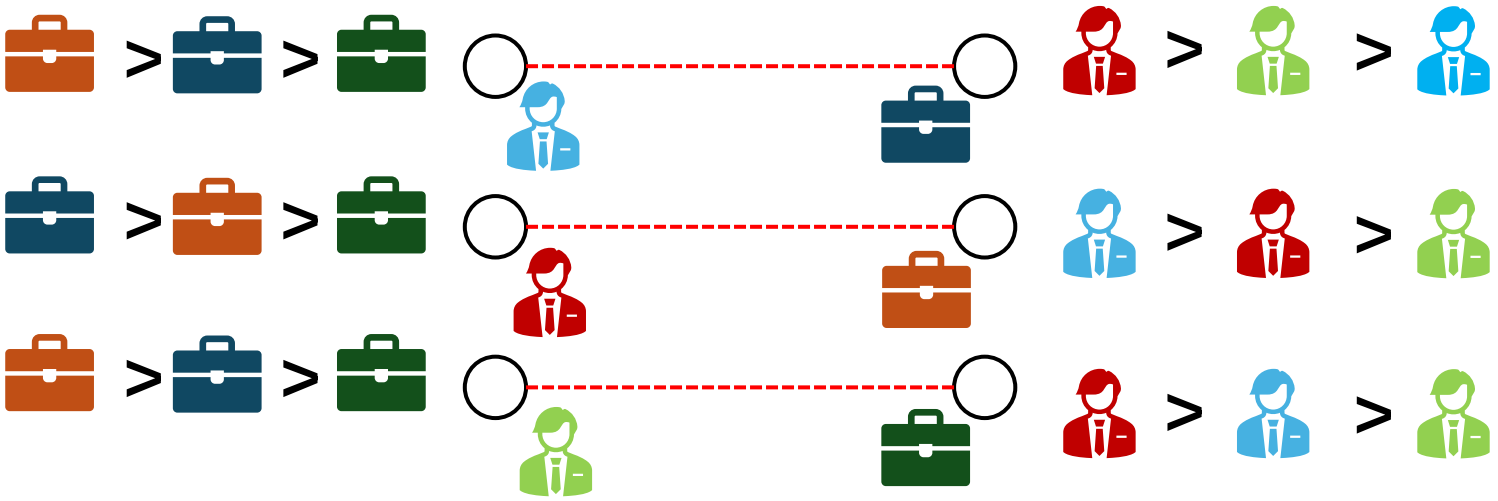


Preference ordering





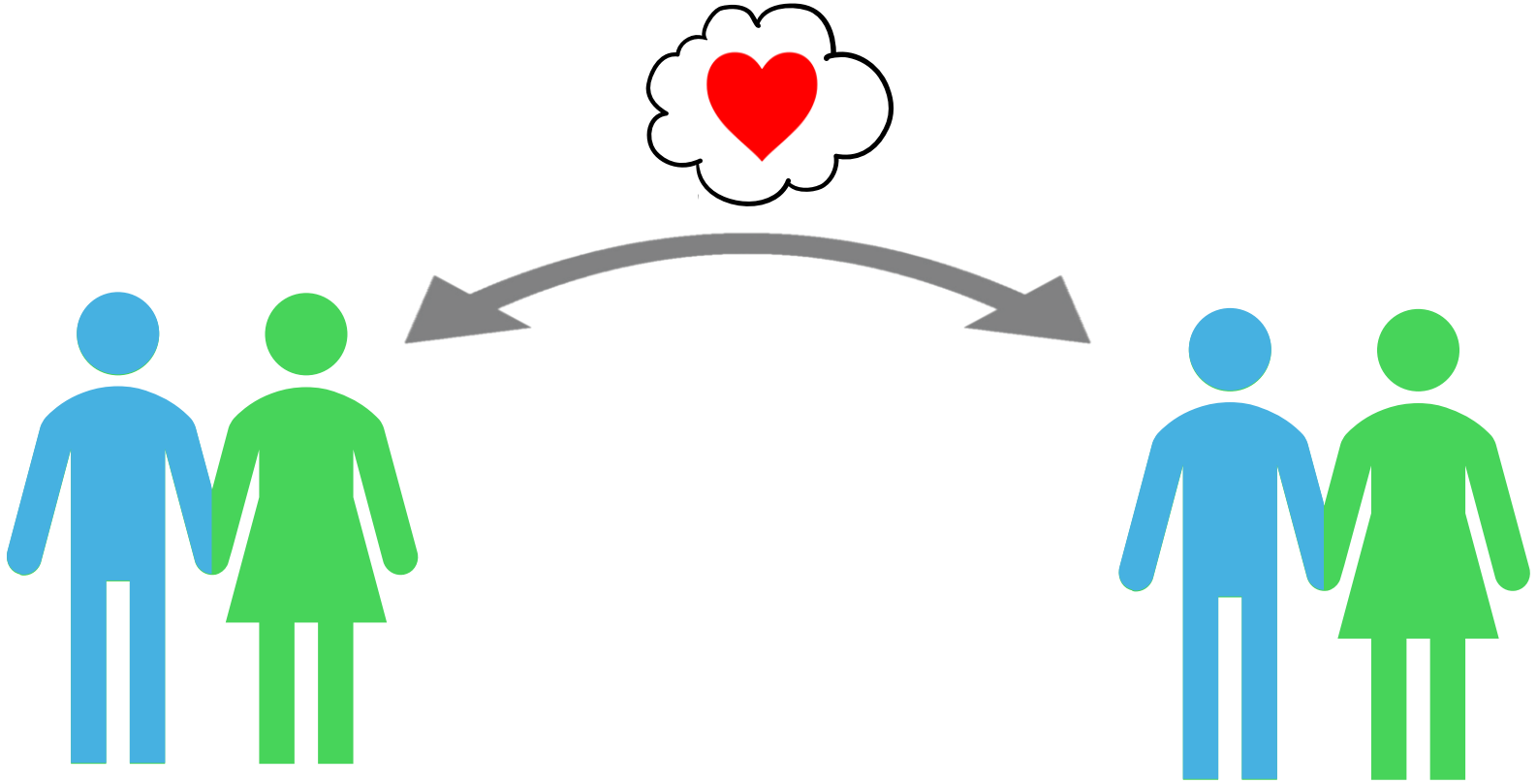
Preference ordering



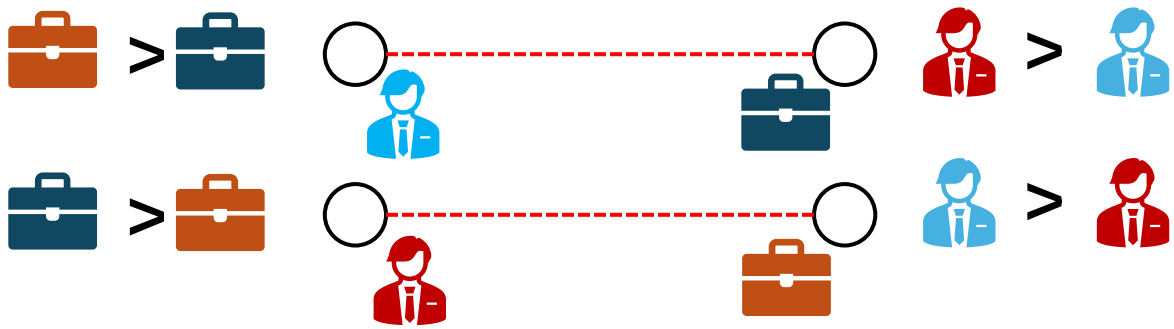
Blocking pair

Blocking pair

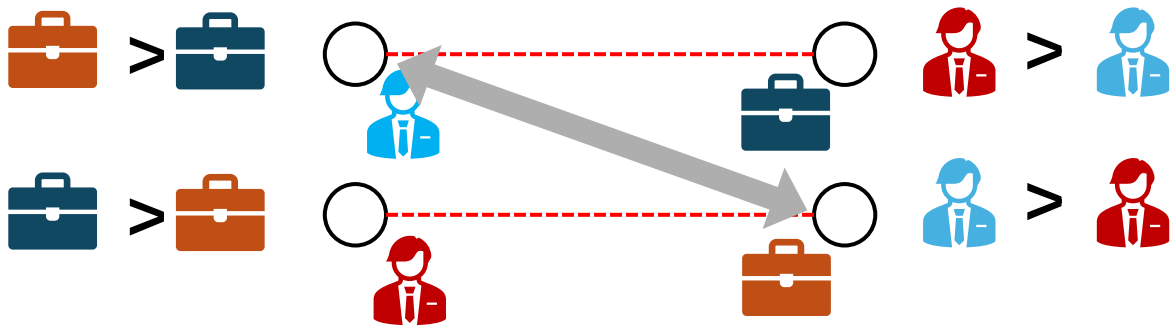
Blocking pair: Two unmatched parties form a blocking pair if they prefer each other compared to their current partner



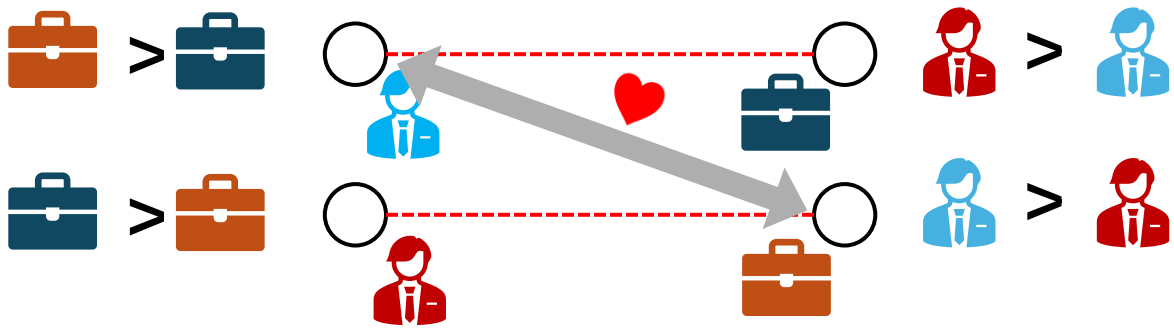
Preference ordering



Preference ordering

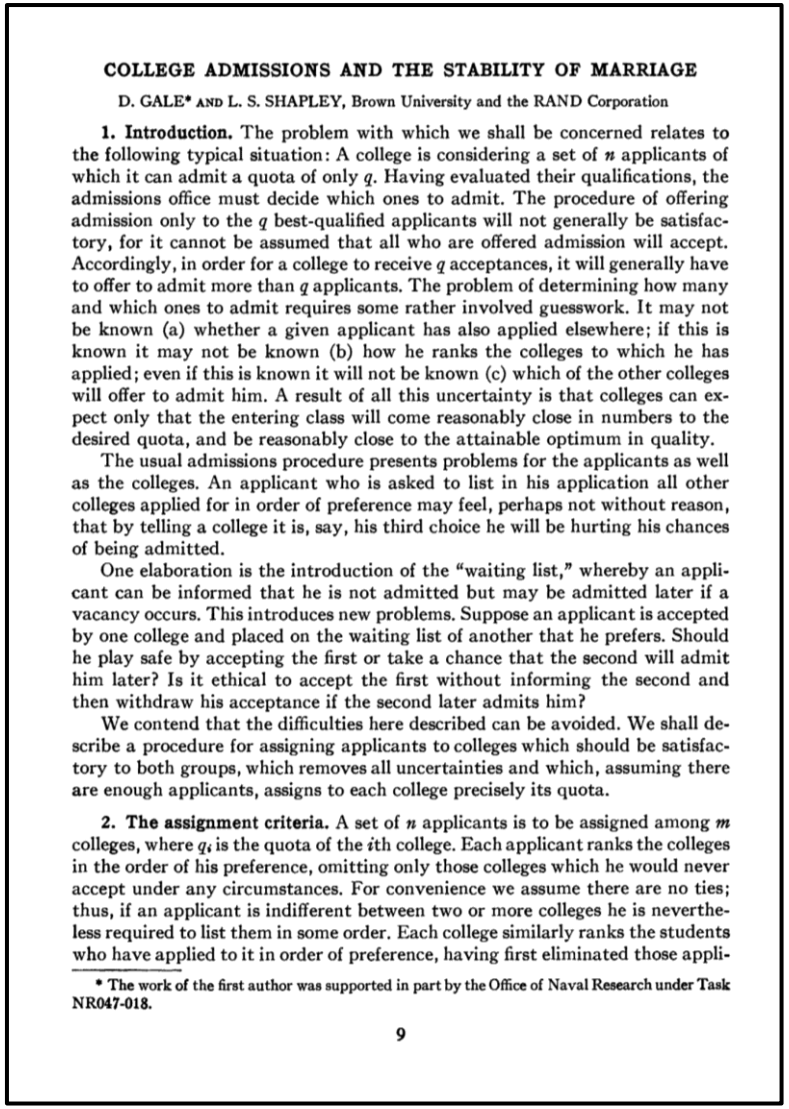


Preference ordering



Stable Matching

Stable Matching



COLLEGE ADMISSIONS AND THE STABILITY OF MARRIAGE

D. GALE* AND L. S. SHAPLEY, Brown University and the RAND Corporation

1. Introduction. The problem with which we shall be concerned relates to the following typical situation: A college is considering a set of n applicants of which it can admit a quota of only q. Having evaluated their qualifications, the admissions office must decide which ones to admit. The procedure of offering admission only to the q best-qualified applicants will not generally be satisfactory, for it cannot be assumed that all who are offered admission will accept. Accordingly, in order for a college to receive q acceptances, it will generally have to offer to admit more than q applicants. The problem of determining how many and which ones to admit requires some rather involved guesswork. It may not be known (a) whether a given applicant has also applied elsewhere; if this is known it may not be known (b) how he ranks the colleges to which he has applied; even if this is known it will not be known (c) which of the other colleges will offer to admit him. A result of all this uncertainty is that colleges can expect only that the entering class will come reasonably close in numbers to the desired quota, and be reasonably close to the attainable optimum in quality.

The usual admissions procedure presents problems for the applicants as well as the colleges. An applicant who is asked to list in his application all other colleges applied for in order of preference may feel, perhaps not without reason, that by telling a college it is, say, his third choice he will be hurting his chances of being admitted.

One elaboration is the introduction of the "waiting list," whereby an applicant can be informed that he is not admitted but may be admitted later if a vacancy occurs. This introduces new problems. Suppose an applicant is accepted by one college and placed on the waiting list of another that he prefers. Should he play safe by accepting the first or take a chance that the second will admit him later? Is it ethical to accept the first without informing the second and then withdraw his acceptance if the second later admits him?

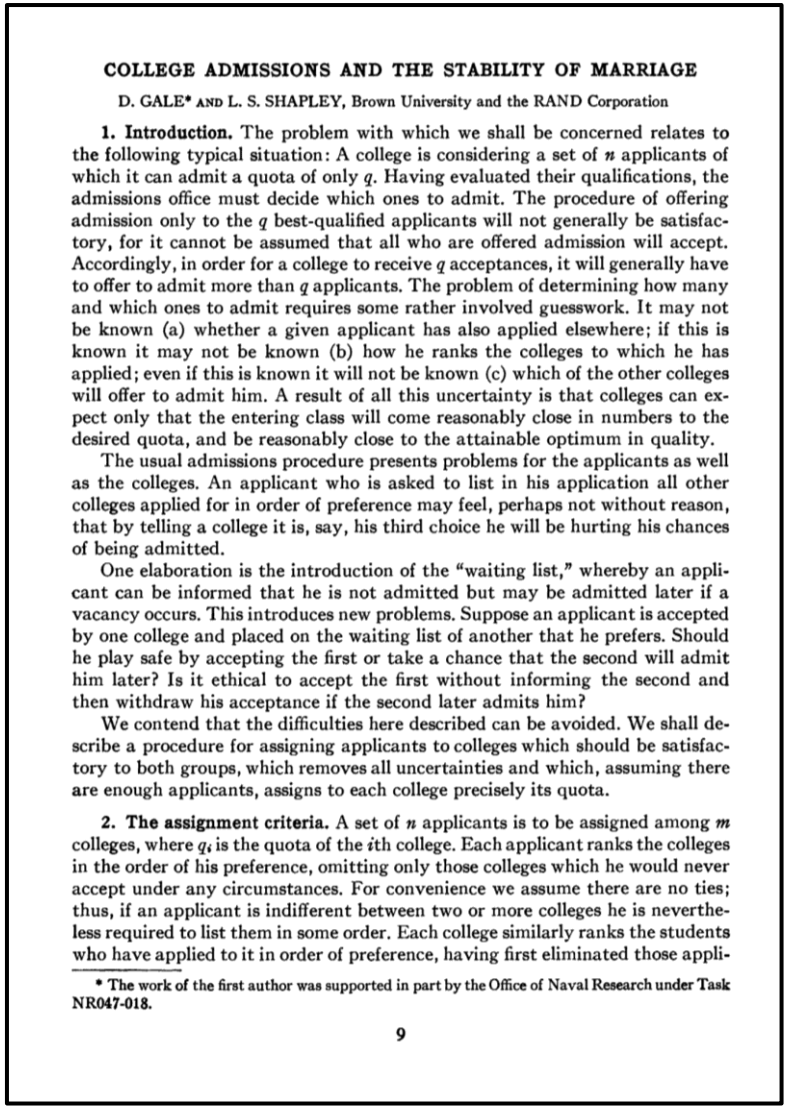
We contend that the difficulties here described can be avoided. We shall describe a procedure for assigning applicants to colleges which should be satisfactory to both groups, which removes all uncertainties and which, assuming there are enough applicants, assigns to each college precisely its quota.

2. The assignment criteria. A set of n applicants is to be assigned among m colleges, where q_i is the quota of the ith college. Each applicant ranks the colleges in the order of his preference, omitting only those colleges which he would never accept under any circumstances. For convenience we assume there are no ties; thus, if an applicant is indifferent between two or more colleges he is nevertheless required to list them in some order. Each college similarly ranks the students who have applied to it in order of preference, having first eliminated those appli-

* The work of the first author was supported in part by the Office of Naval Research under Task NR047-018.

Gale, D., and L. S. Shapley. "College Admissions and the Stability of Marriage." The American Mathematical Monthly, 1962

Stable Matching



COLLEGE ADMISSIONS AND THE STABILITY OF MARRIAGE

D. GALE* AND L. S. SHAPLEY, Brown University and the RAND Corporation

1. Introduction. The problem with which we shall be concerned relates to the following typical situation: A college is considering a set of n applicants of which it can admit a quota of only q. Having evaluated their qualifications, the admissions office must decide which ones to admit. The procedure of offering admission only to the q best-qualified applicants will not generally be satisfactory, for it cannot be assumed that all who are offered admission will accept. Accordingly, in order for a college to receive q acceptances, it will generally have to offer to admit more than q applicants. The problem of determining how many and which ones to admit requires some rather involved guesswork. It may not be known (a) whether a given applicant has also applied elsewhere; if this is known it may not be known (b) how he ranks the colleges to which he has applied; even if this is known it will not be known (c) which of the other colleges will offer to admit him. A result of all this uncertainty is that colleges can expect only that the entering class will come reasonably close in numbers to the desired quota, and be reasonably close to the attainable optimum in quality.

The usual admissions procedure presents problems for the applicants as well as the colleges. An applicant who is asked to list in his application all other colleges applied for in order of preference may feel, perhaps not without reason, that by telling a college it is, say, his third choice he will be hurting his chances of being admitted.

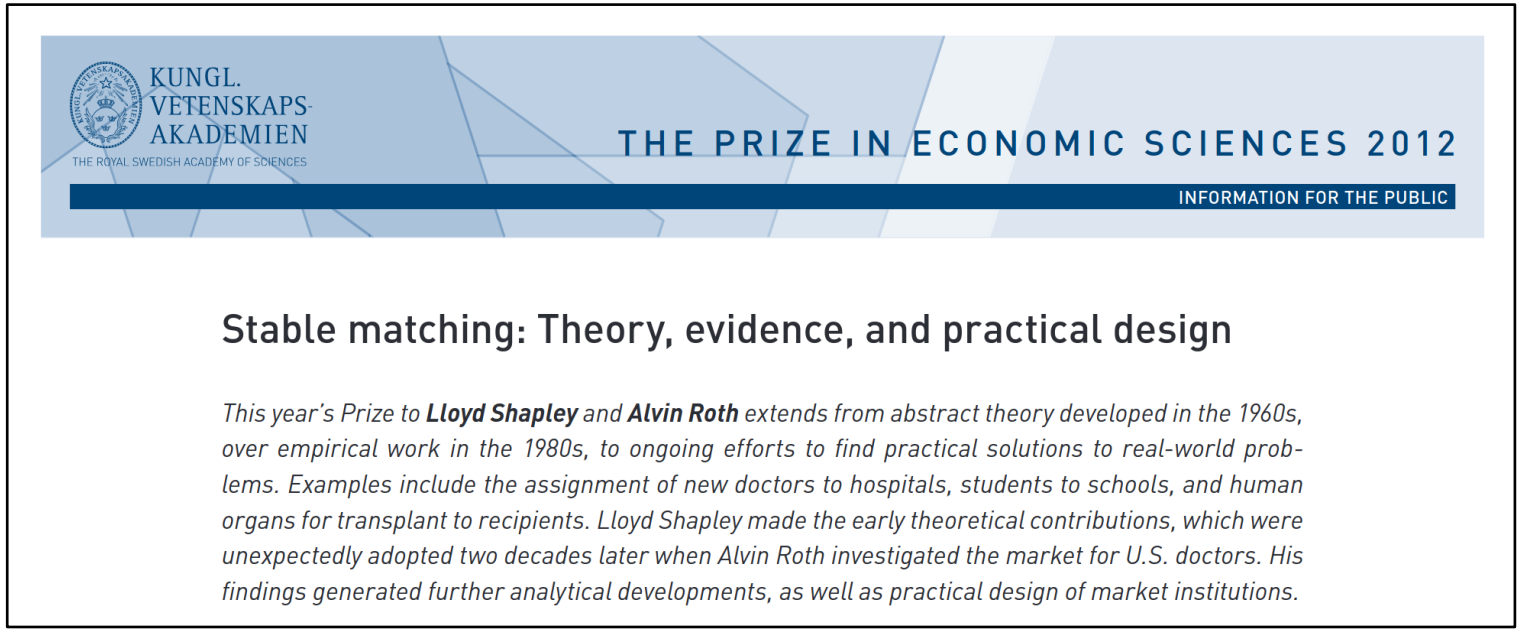
One elaboration is the introduction of the "waiting list," whereby an applicant can be informed that he is not admitted but may be admitted later if a vacancy occurs. This introduces new problems. Suppose an applicant is accepted by one college and placed on the waiting list of another that he prefers. Should he play safe by accepting the first or take a chance that the second will admit him later? Is it ethical to accept the first without informing the second and then withdraw his acceptance if the second later admits him?

We contend that the difficulties here described can be avoided. We shall describe a procedure for assigning applicants to colleges which should be satisfactory to both groups, which removes all uncertainties and which, assuming there are enough applicants, assigns to each college precisely its quota.

2. The assignment criteria. A set of n applicants is to be assigned among m colleges, where q_i is the quota of the ith college. Each applicant ranks the colleges in the order of his preference, omitting only those colleges which he would never accept under any circumstances. For convenience we assume there are no ties; thus, if an applicant is indifferent between two or more colleges he is nevertheless required to list them in some order. Each college similarly ranks the students who have applied to it in order of preference, having first eliminated those appli-

* The work of the first author was supported in part by the Office of Naval Research under Task NR047-018.

Gale, D., and L. S. Shapley. "College Admissions and the Stability of Marriage." The American Mathematical Monthly, 1962



KUNGL. VETENSKAPS-AKADEMIEN
THE ROYAL SWEDISH ACADEMY OF SCIENCES

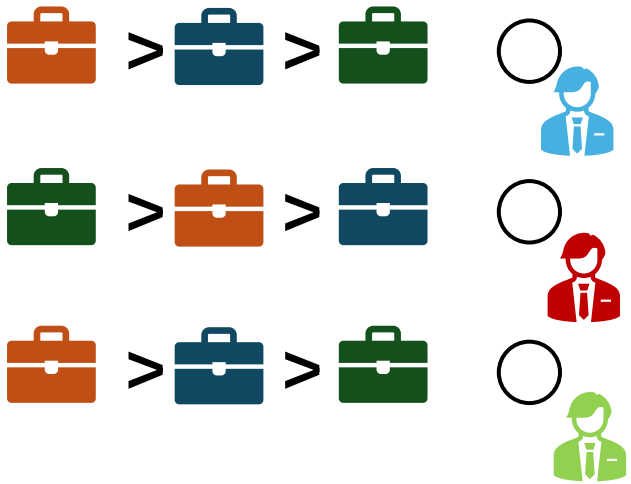
THE PRIZE IN ECONOMIC SCIENCES 2012

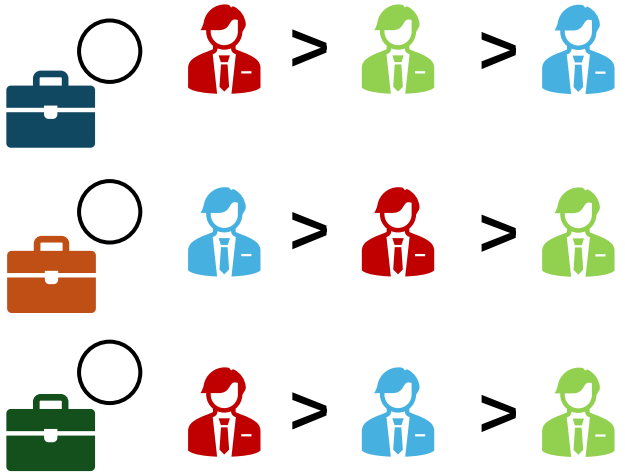
INFORMATION FOR THE PUBLIC

Stable matching: Theory, evidence, and practical design

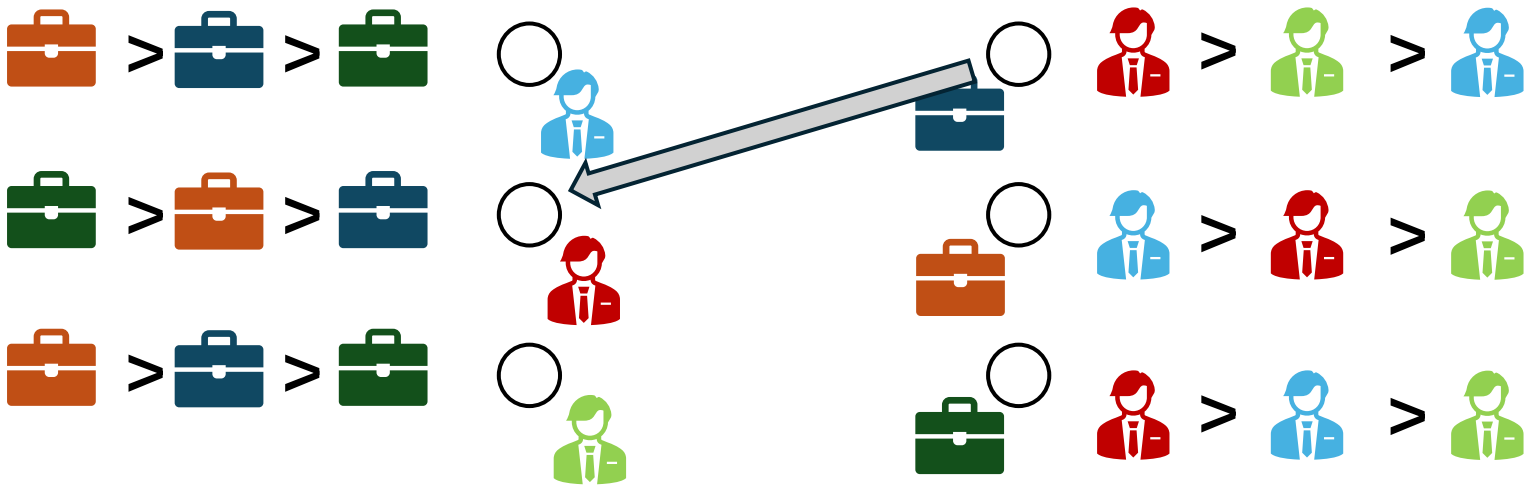
*This year's Prize to **Lloyd Shapley** and **Alvin Roth** extends from abstract theory developed in the 1960s, over empirical work in the 1980s, to ongoing efforts to find practical solutions to real-world problems. Examples include the assignment of new doctors to hospitals, students to schools, and human organs for transplant to recipients. Lloyd Shapley made the early theoretical contributions, which were unexpectedly adopted two decades later when Alvin Roth investigated the market for U.S. doctors. His findings generated further analytical developments, as well as practical design of market institutions.*

Gale-Shapley Algorithm



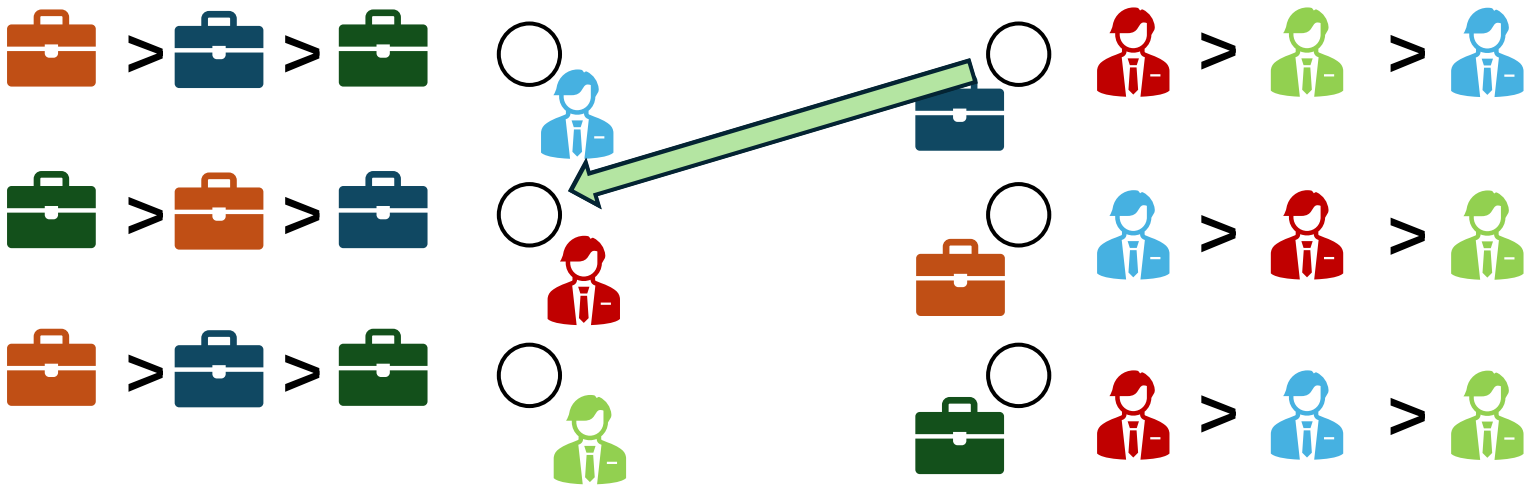


Gale-Shapley Algorithm



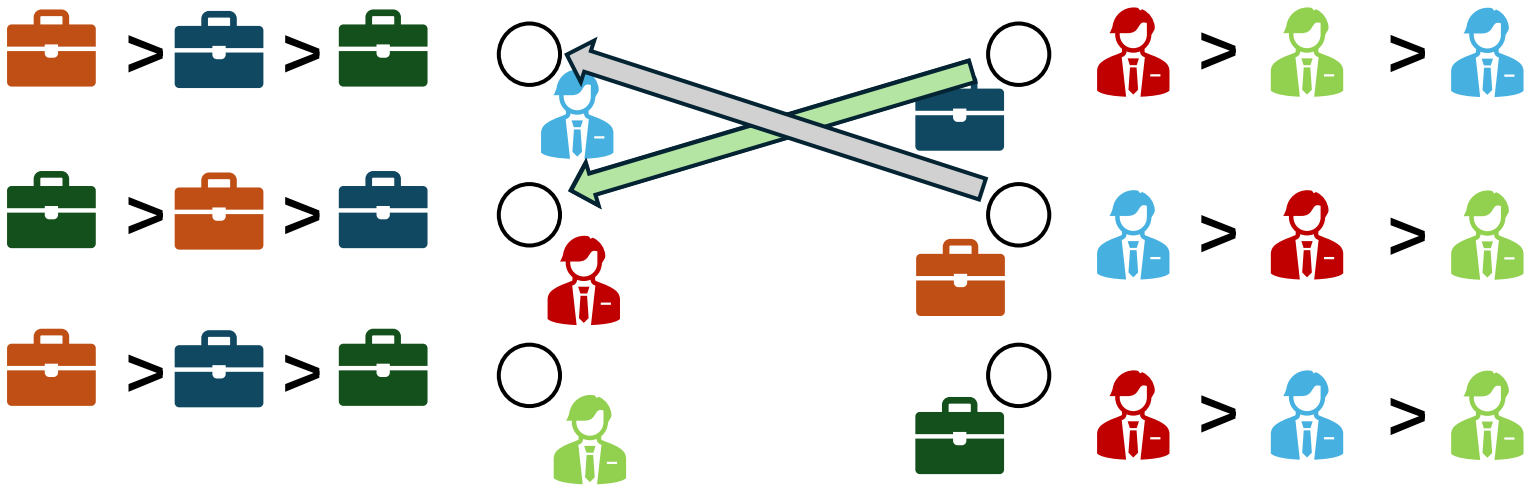
Proposition

Gale-Shapley Algorithm



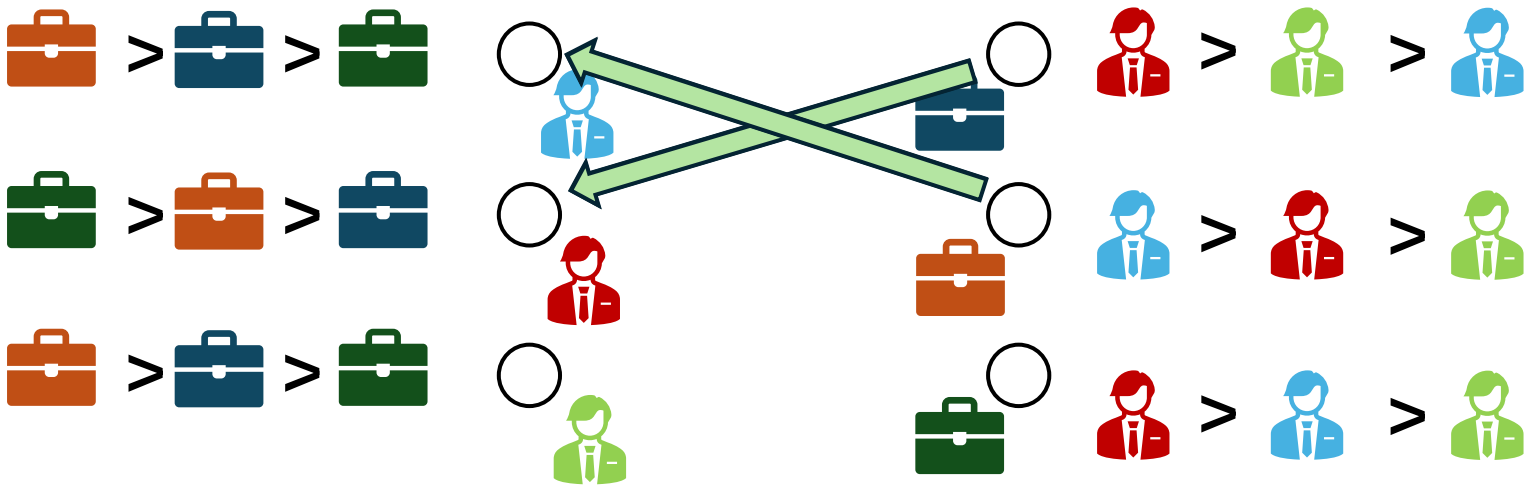
Proposition

Gale-Shapley Algorithm



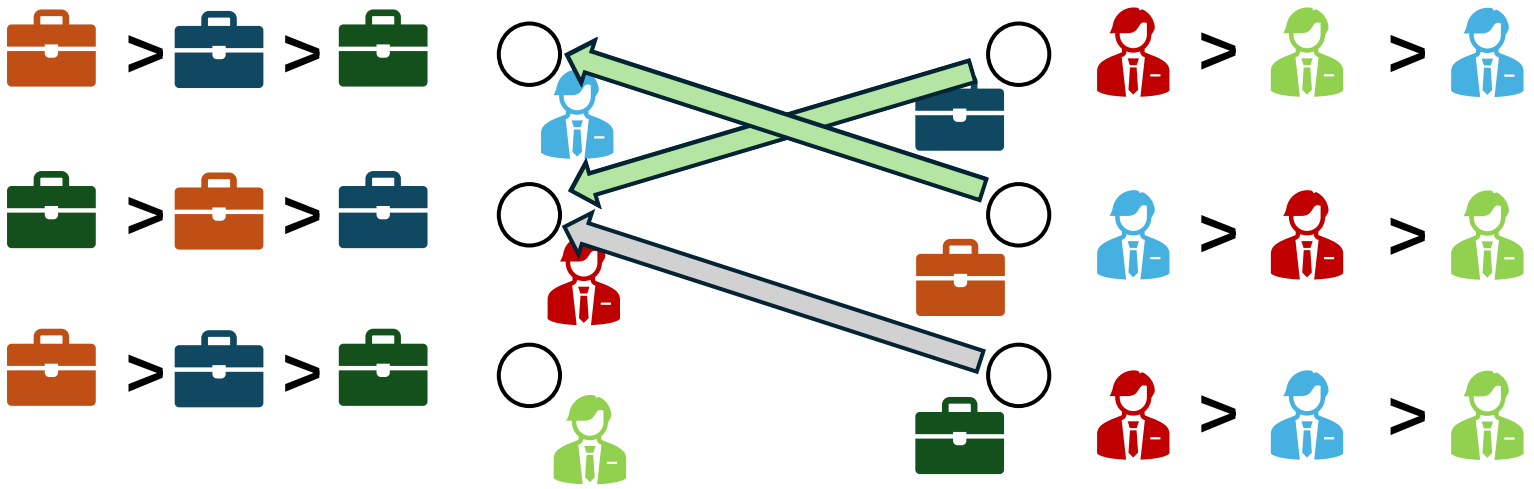
Proposition

Gale-Shapley Algorithm



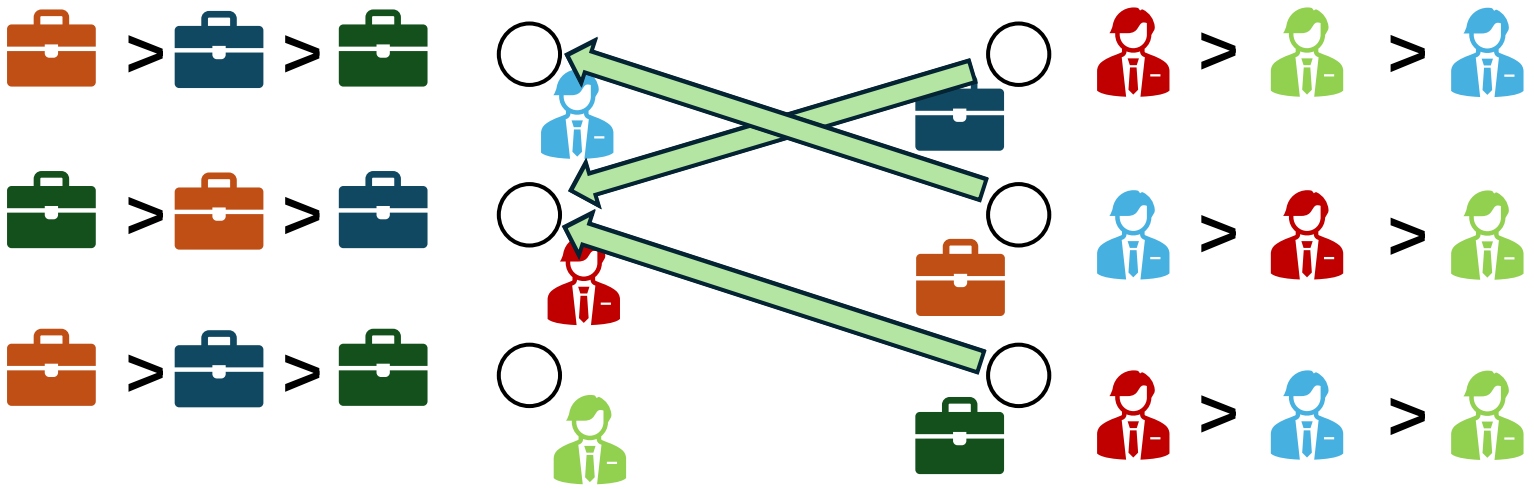
Proposition

Gale-Shapley Algorithm



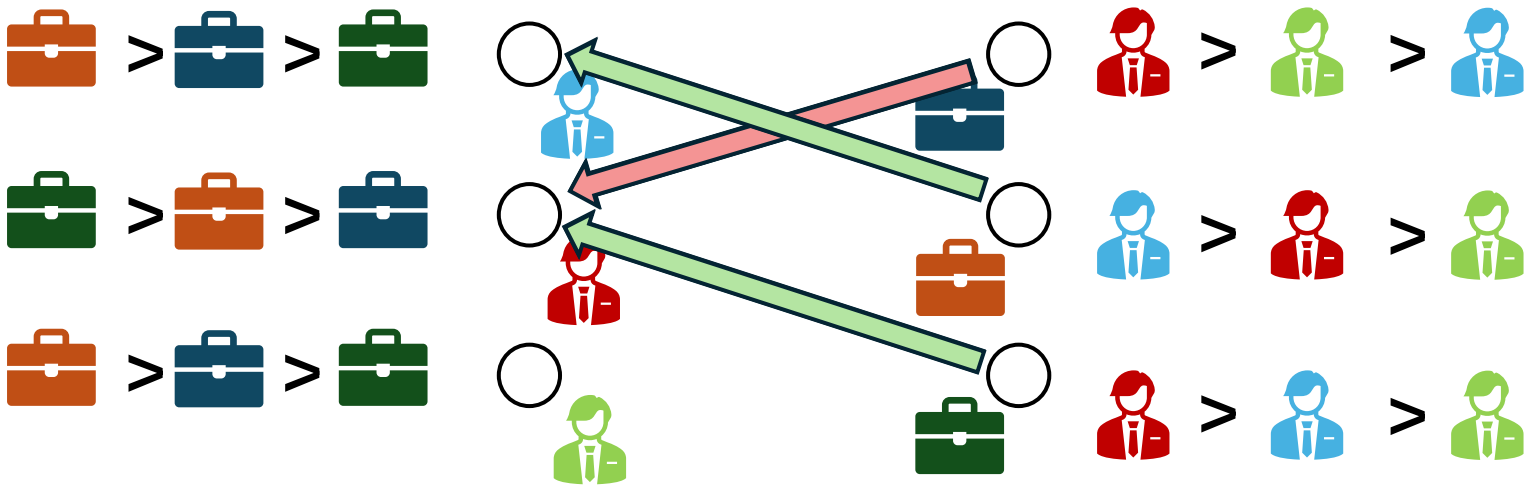
Proposition

Gale-Shapley Algorithm



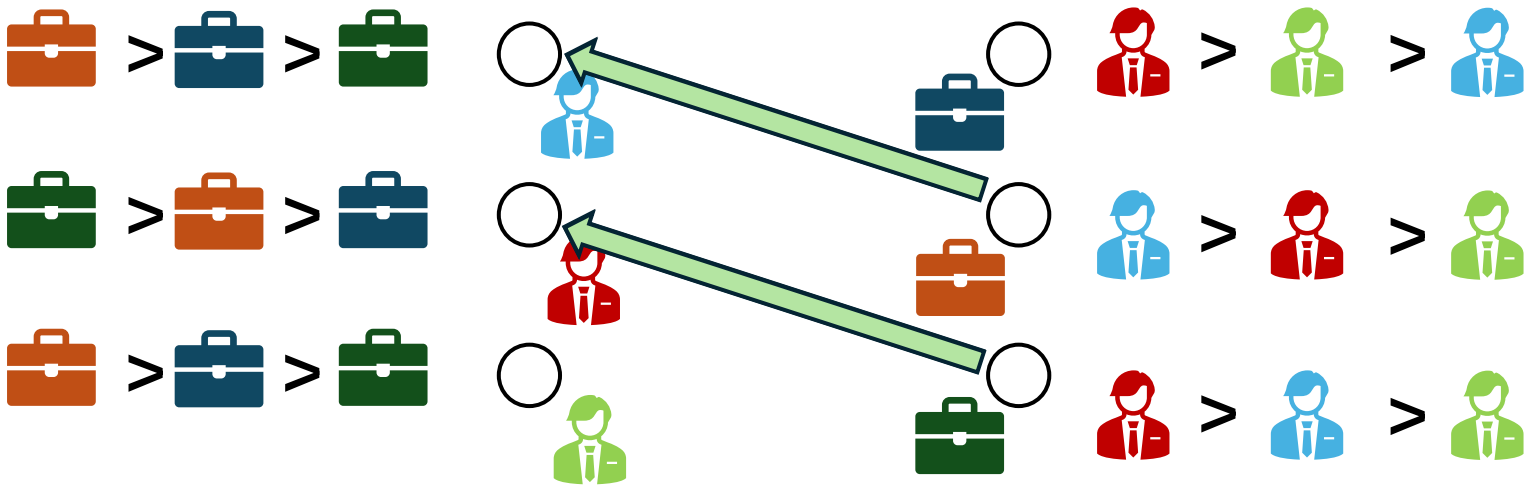
Proposition

Gale-Shapley Algorithm



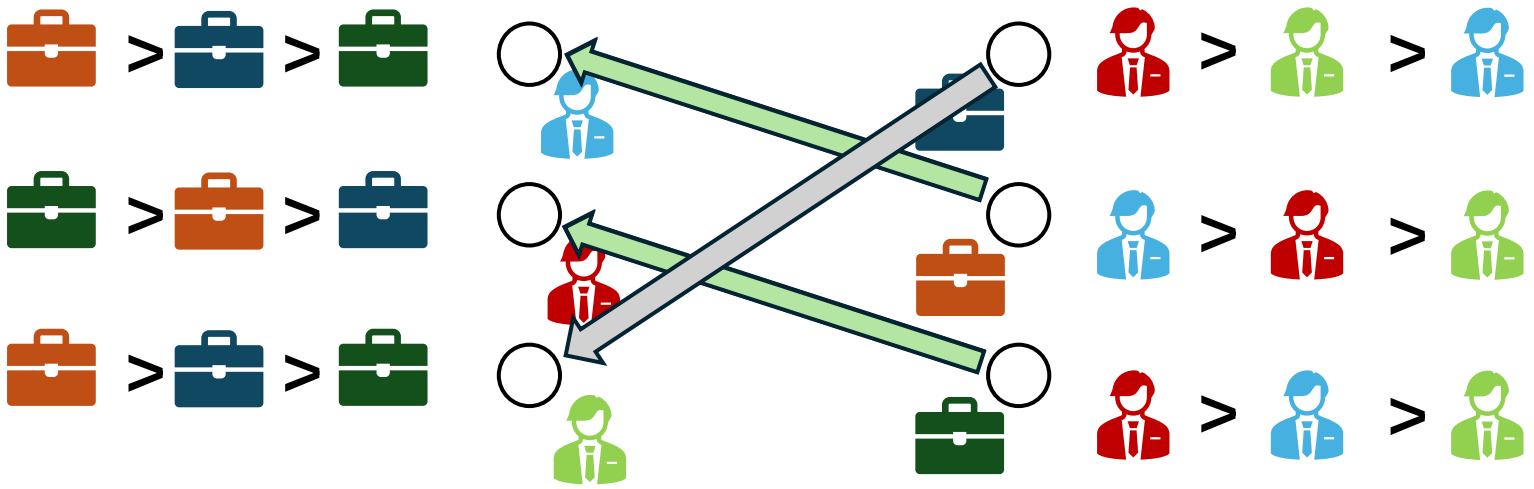
Proposition

Gale-Shapley Algorithm



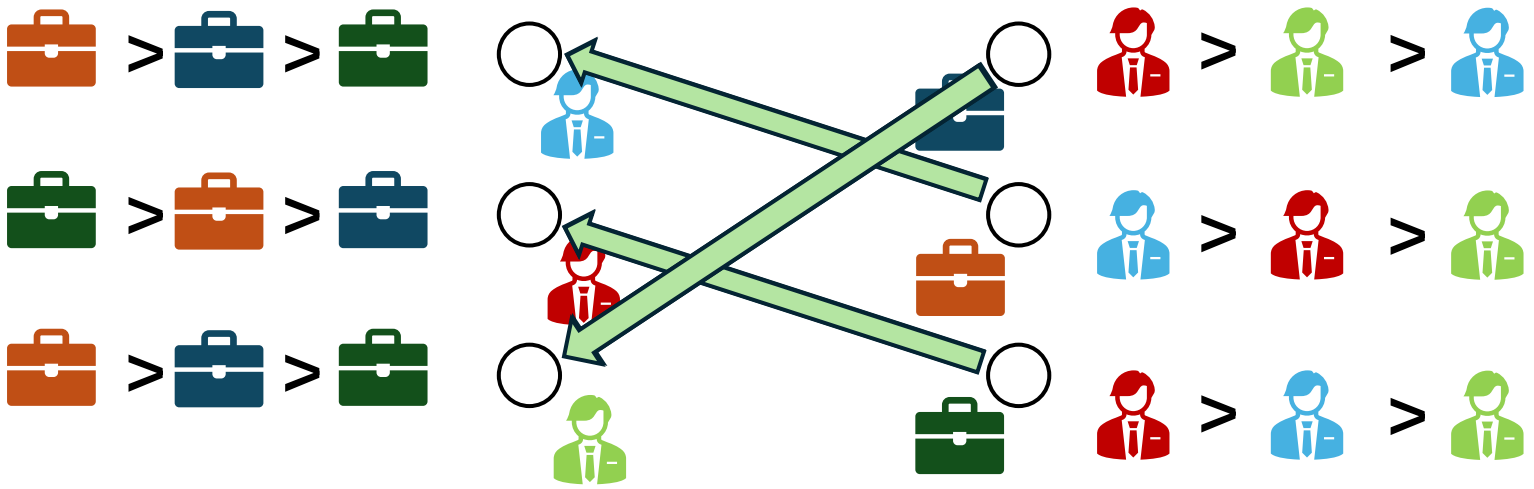
Proposition

Gale-Shapley Algorithm



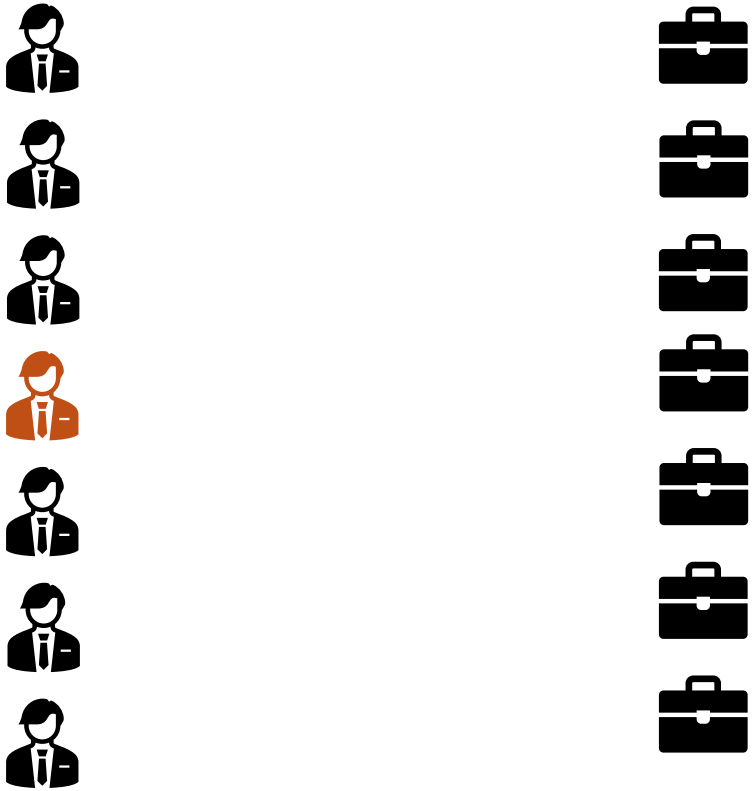
Proposition

Gale-Shapley Algorithm

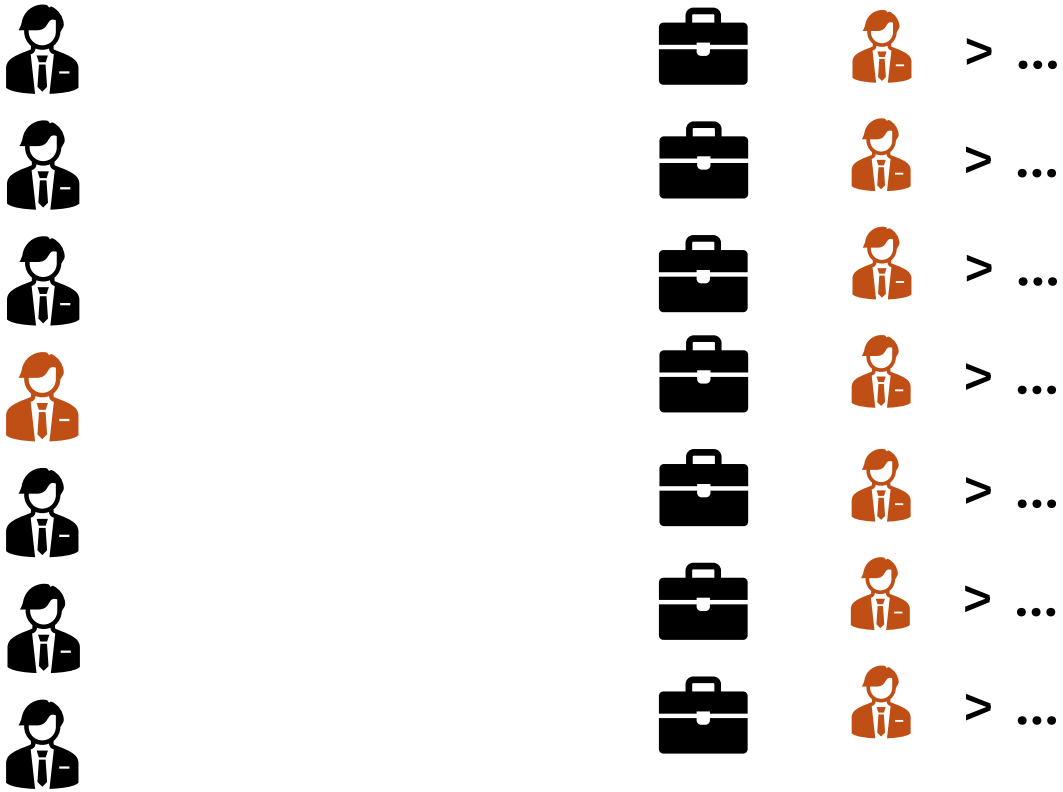


Proposition

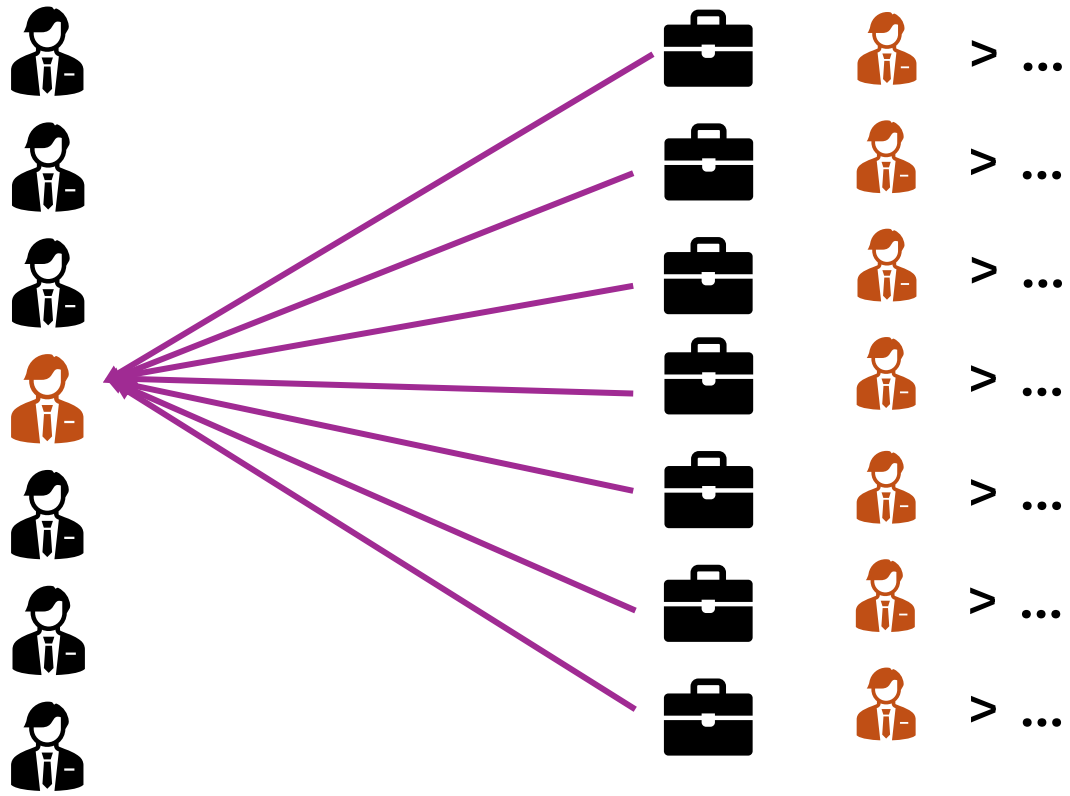
Breaking Gale-Shapley



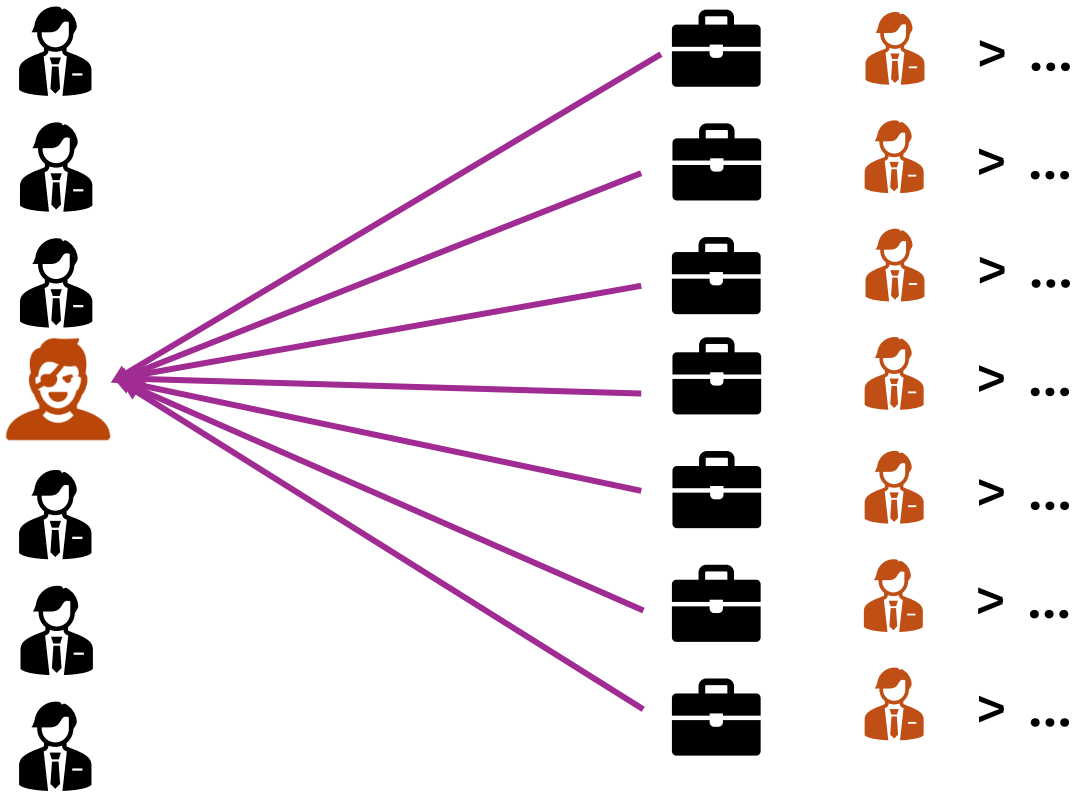
Breaking Gale-Shapley



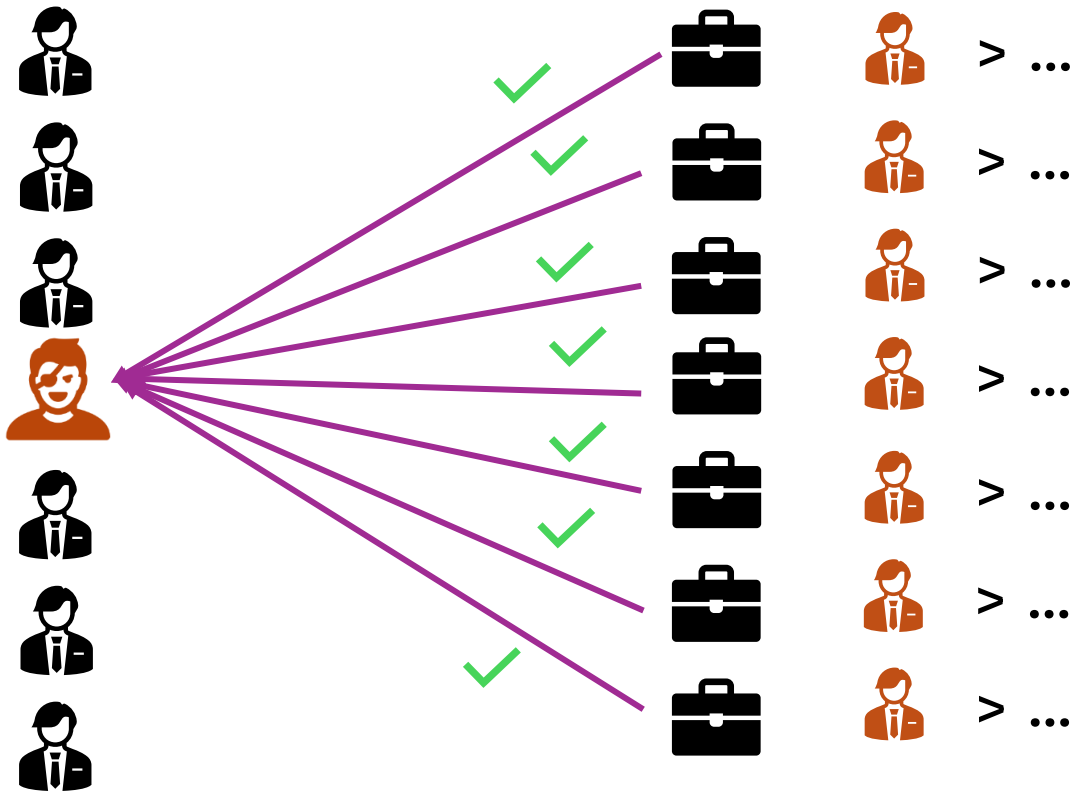
Breaking Gale-Shapley



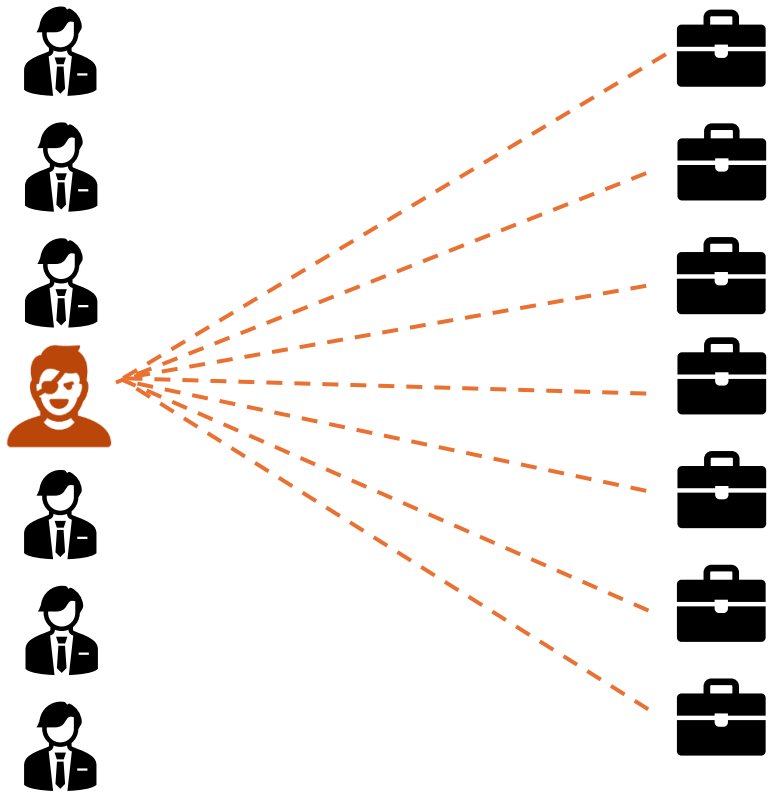
Breaking Gale-Shapley



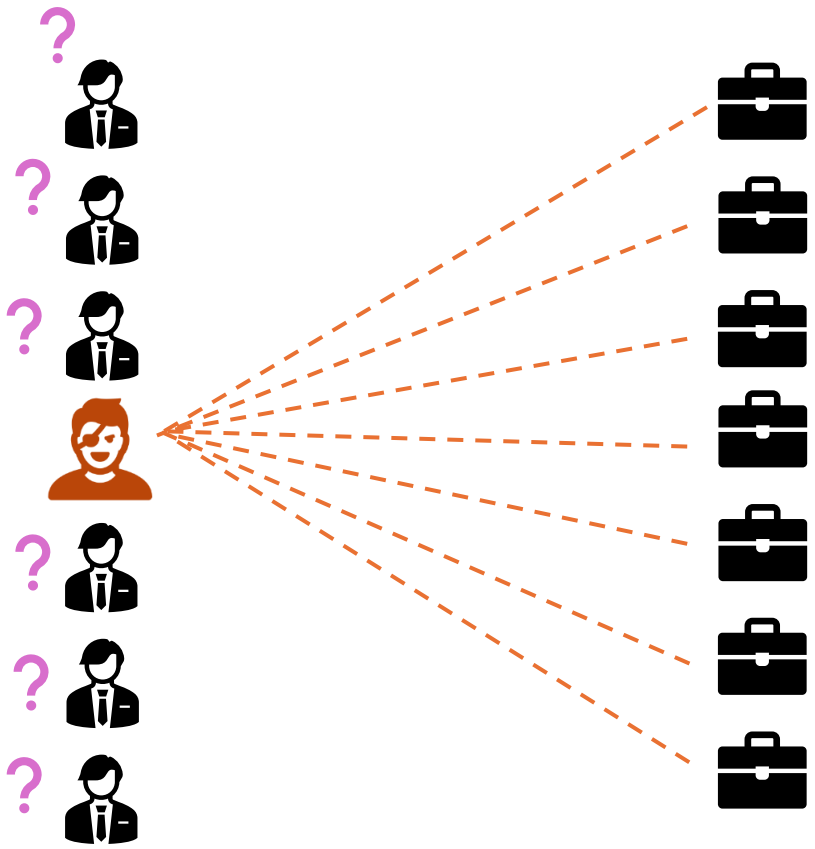
Breaking Gale-Shapley



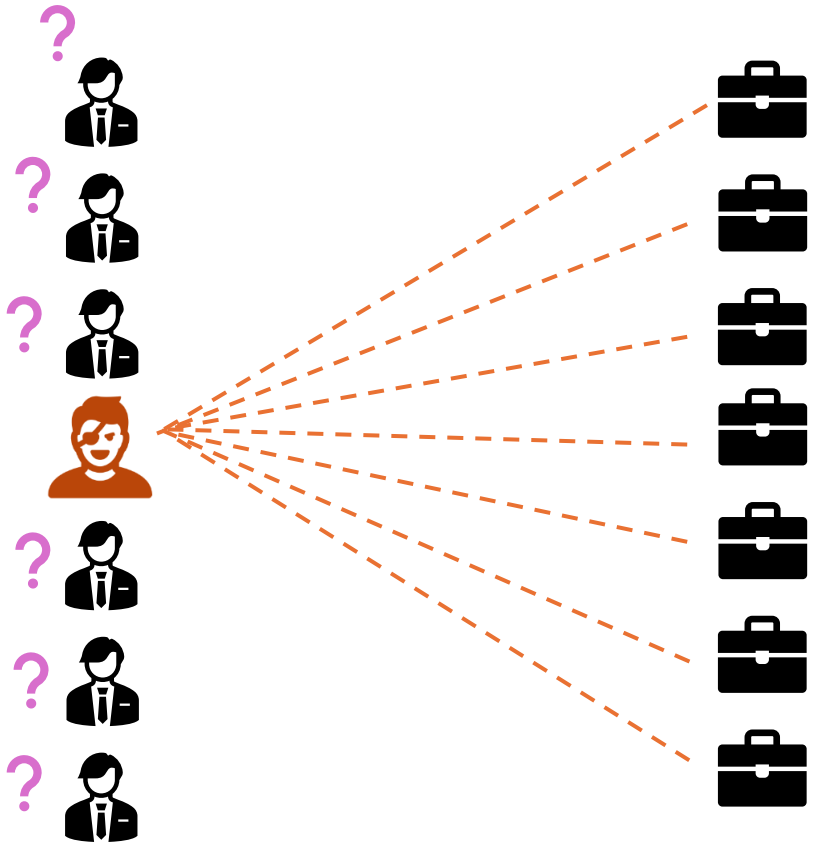
Breaking Gale-Shapley



Breaking Gale-Shapley

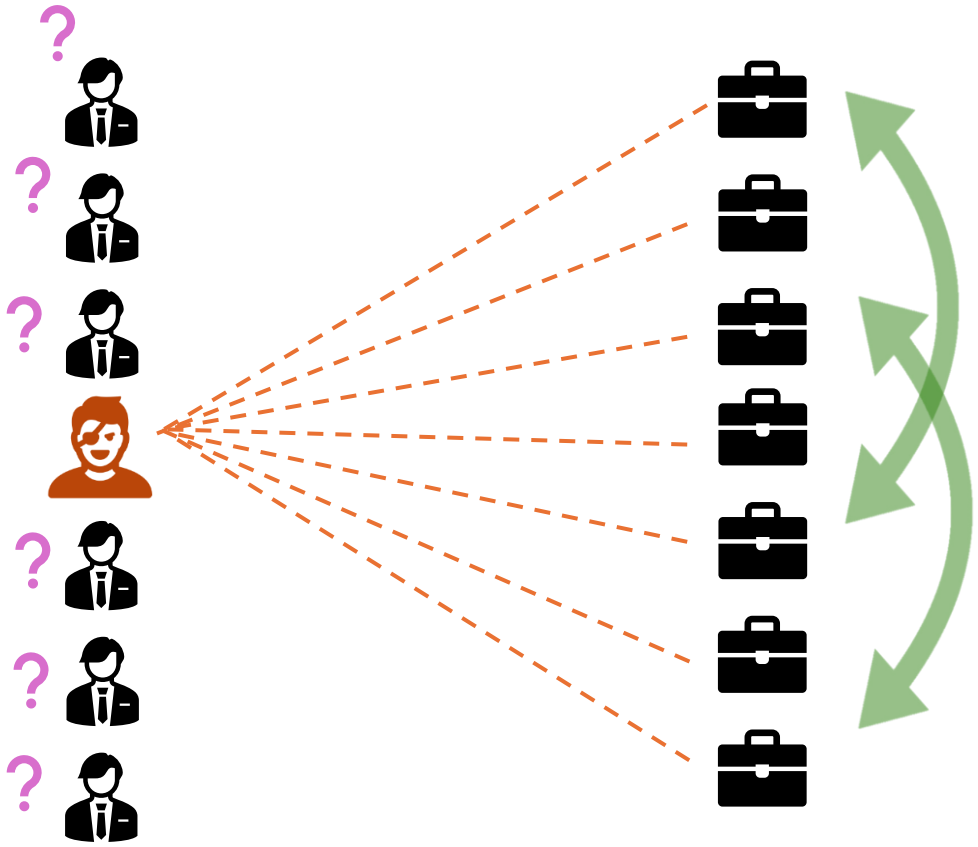


Breaking Gale-Shapley



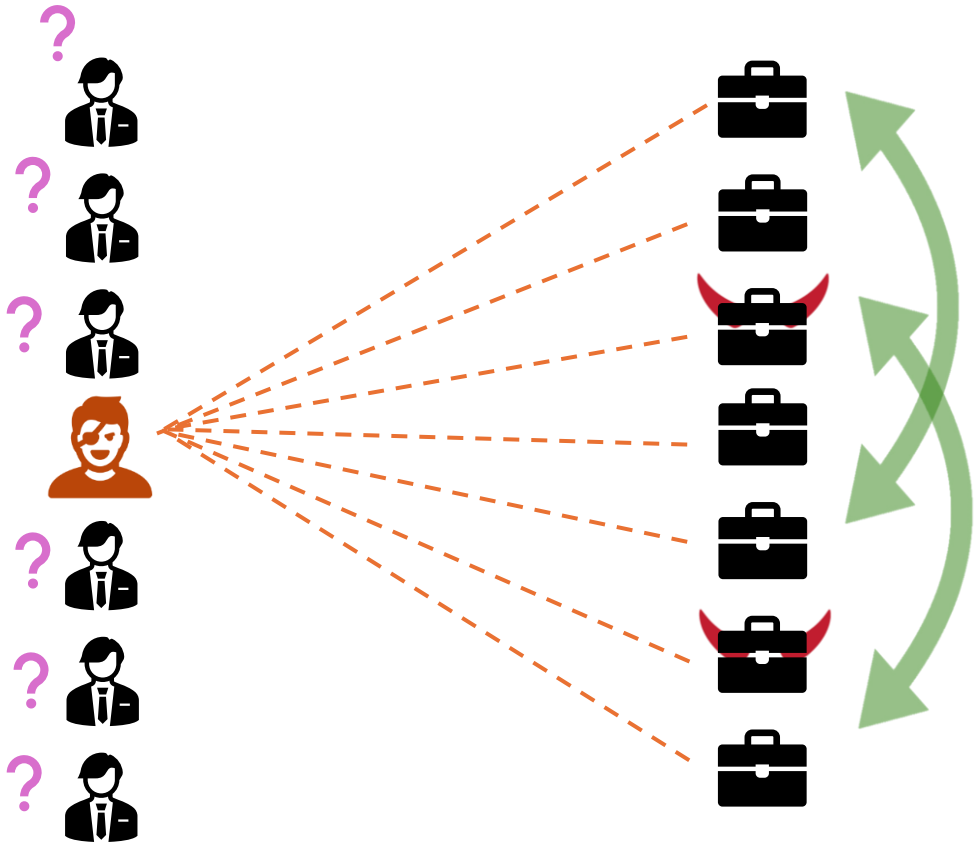
The Gale-Shapley algorithm is not resilient against even one byzantine party!

Breaking Gale-Shapley



The Gale-Shapley algorithm is not resilient against even one byzantine party!

Breaking Gale-Shapley

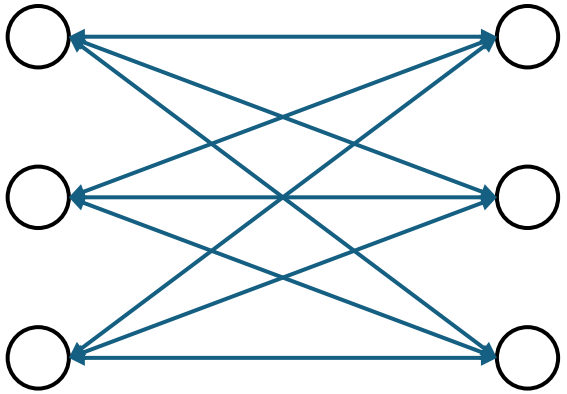


The Gale-Shapley algorithm is not resilient against even one byzantine party!

How many byzantine parties can a protocol solving stable matching support?

Formal definition

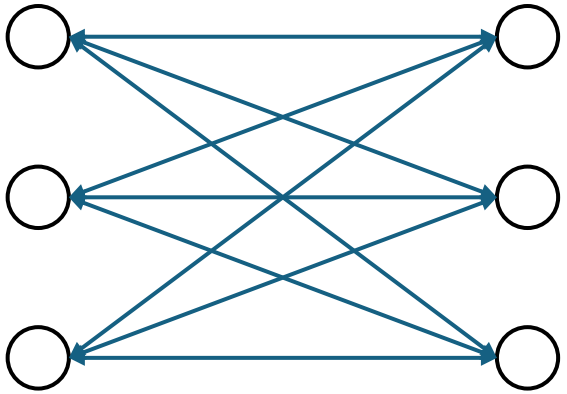
Matching setting:



$n = 2k$ parties

Formal definition

Matching setting:

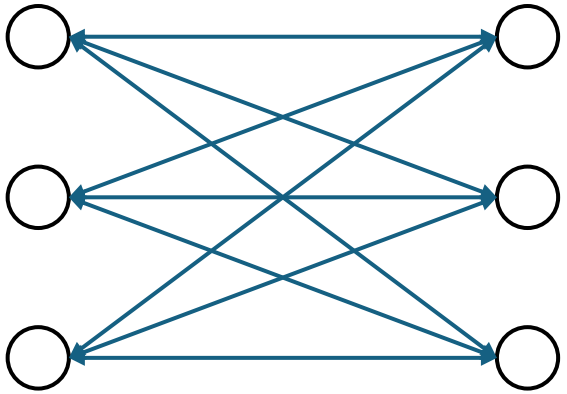


$n = 2k$ parties

Distributed protocol:

Formal definition

Matching setting:



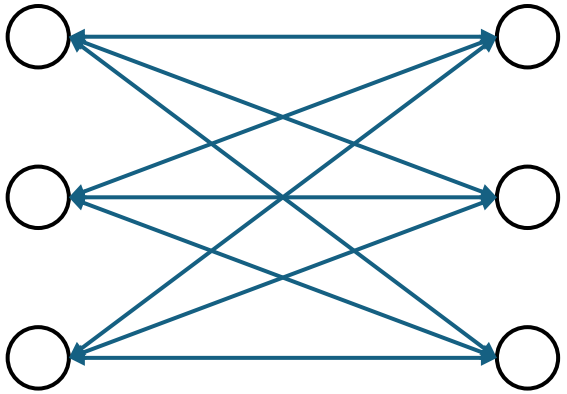
$n = 2k$ parties

Distributed protocol:

Party u

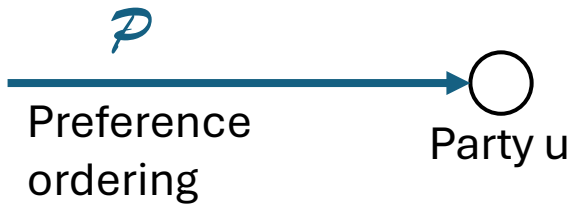
Formal definition

Matching setting:



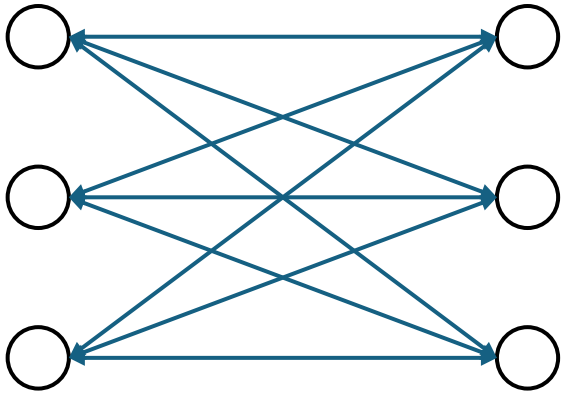
$n = 2k$ parties

Distributed protocol:



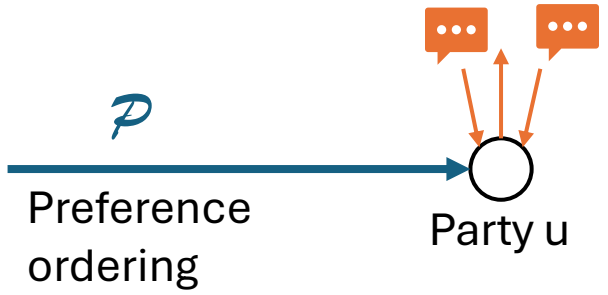
Formal definition

Matching setting:



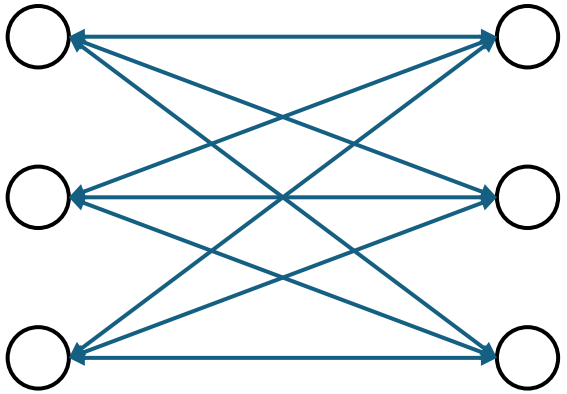
$n = 2k$ parties

Distributed protocol:



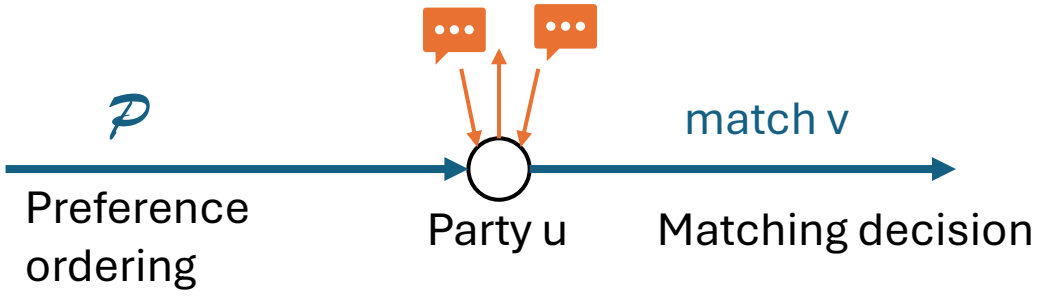
Formal definition

Matching setting:



$n = 2k$ parties

Distributed protocol:



Formal definition

Formal definition

- **Termination**: Every party decides someone to match with.

Formal definition

- **Termination**: Every party decides someone to match with.

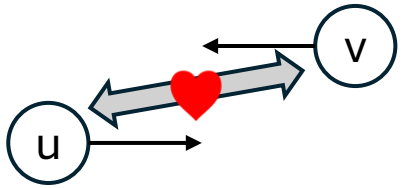
- **Symmetry**: If party u decides to match with v, then v must decide to match with u.

Formal definition

- **Termination**: Every party decides someone to match with.

- **Symmetry**: If party u decides to match with v, then v must decide to match with u.

- **Stability**: There is no blocking pair.

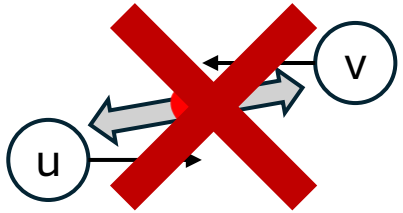


Formal definition

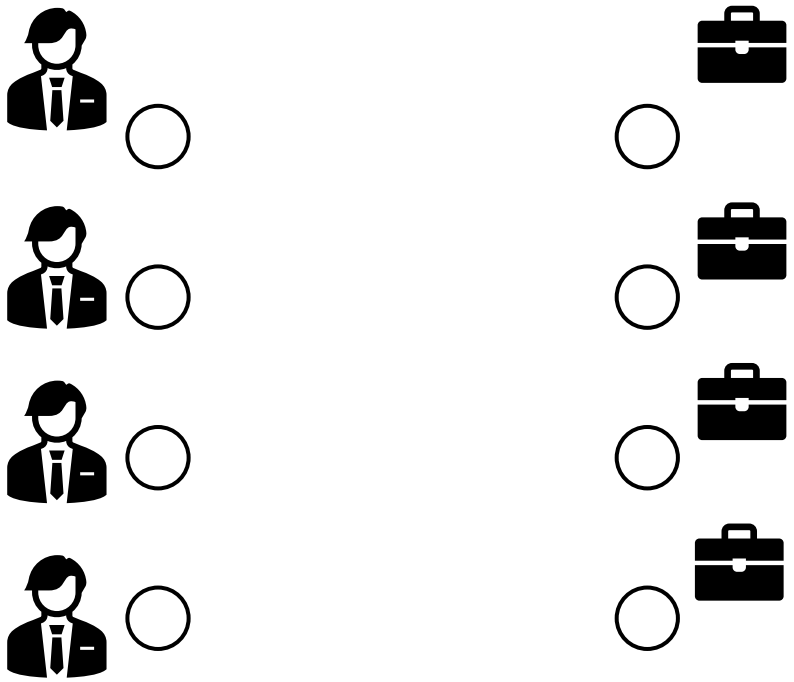
- **Termination**: Every party decides someone to match with.

- **Symmetry**: If party u decides to match with v, then v must decide to match with u.

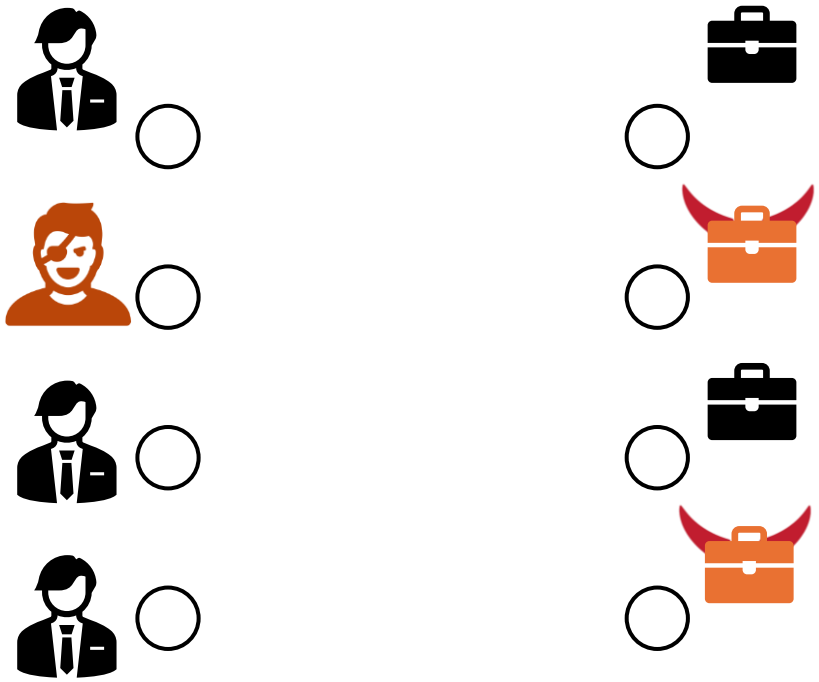
- **Stability**: There is no blocking pair.



Byzantine setting

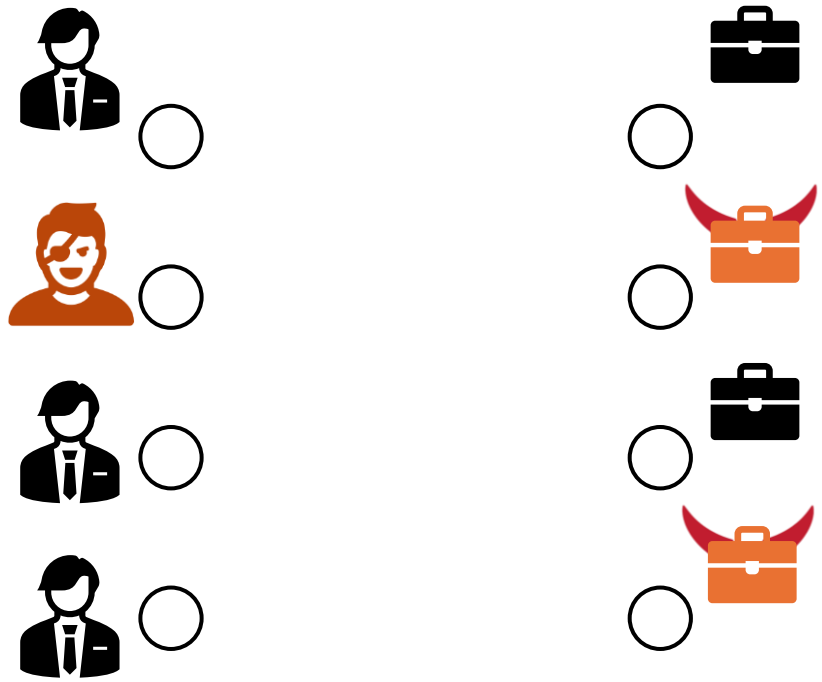


Byzantine setting



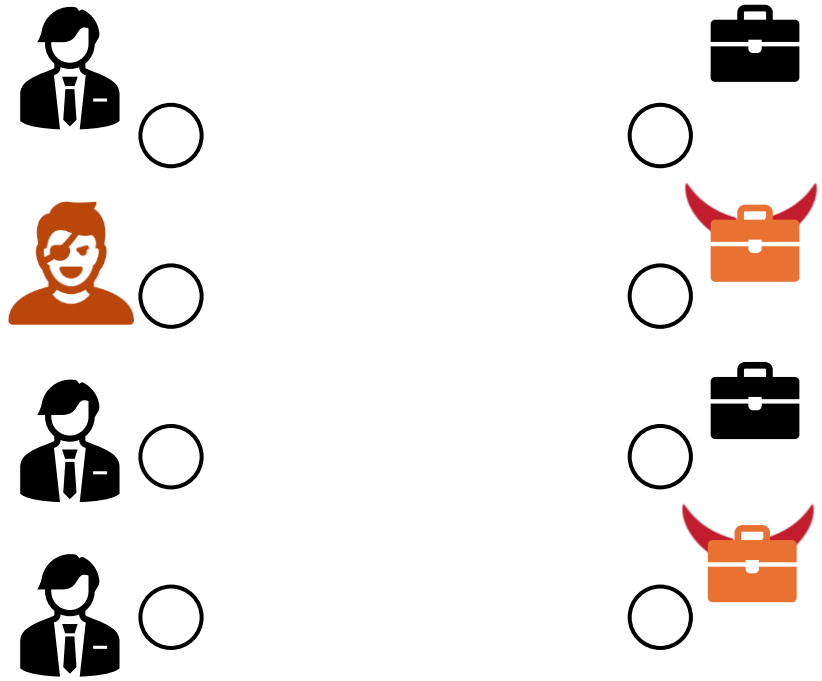
Byzantine setting

At most t_L byzantine parties on the left



Byzantine setting

At most t_L byzantine parties on the left



At most t_R byzantine parties on the right

Formal definition

Formal definition

- **Symmetry**: If an **honest** party u decides to match with v **and v is honest**, then v must match with u.

Formal definition

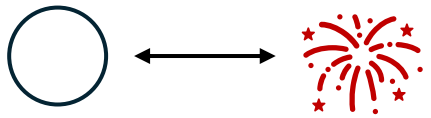
- **Symmetry**: If an **honest** party u decides to match with v **and v is honest**, then v must match with u.

- **Stability**: There is no blocking **pair made of 2 honest parties.**

Formal definition

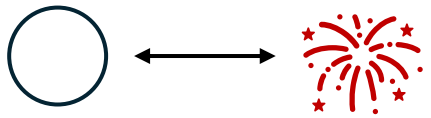
- **Symmetry**: If an **honest** party u decides to match with v **and v is honest**, then v must match with u.

- **Stability**: There is no blocking **pair made of 2 honest parties.**

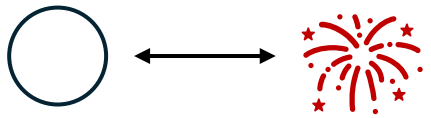


Formal definition

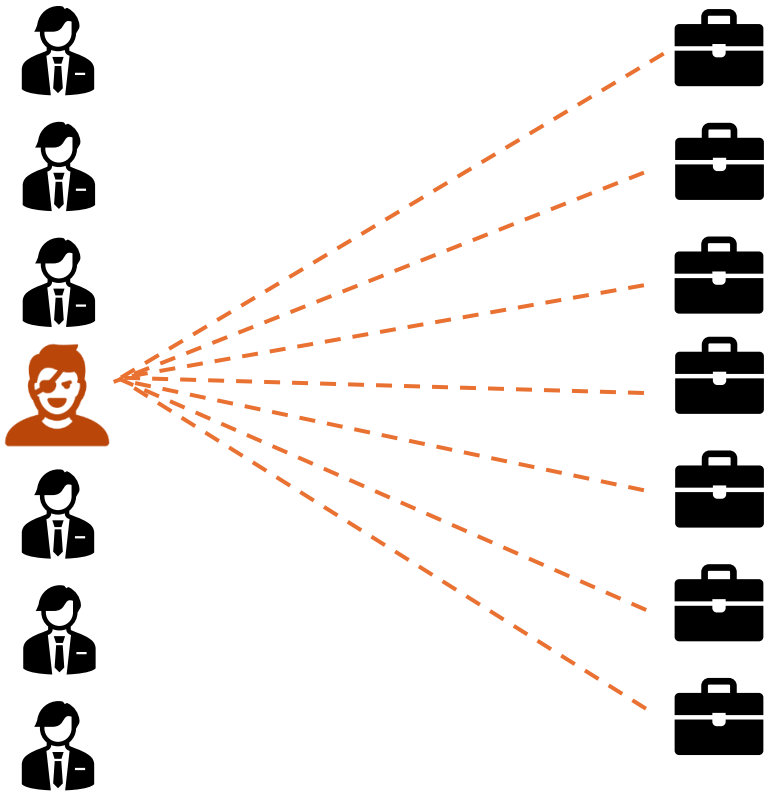
- **Symmetry**: If an **honest** party u decides to match with v **and v is honest**, then v must match with u.
- **Stability**: There is no blocking **pair made of 2 honest parties.**
- An honest party can decide to match with nobody.



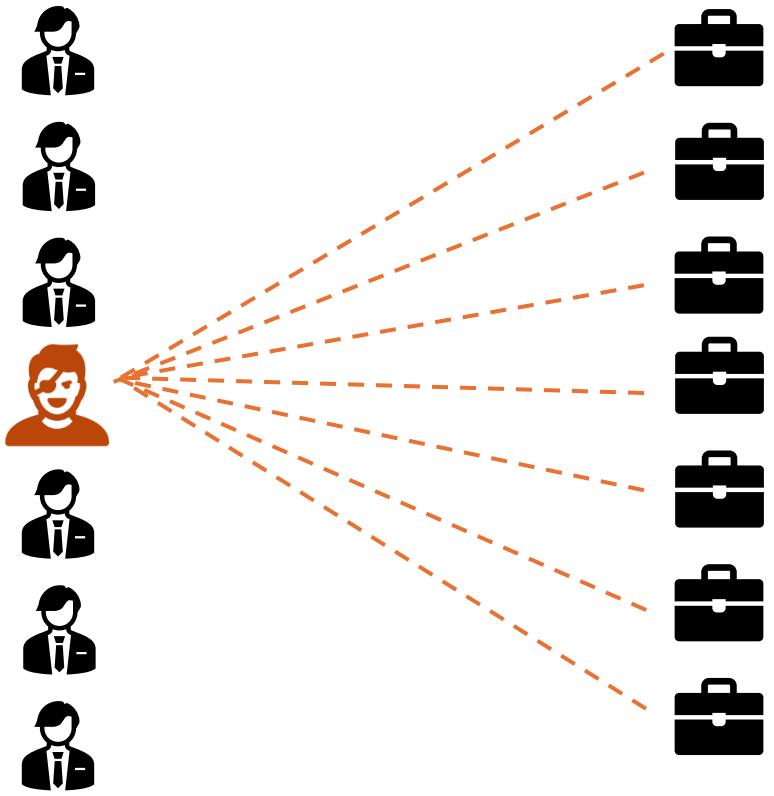
Formal definition

- **Symmetry**: If an **honest** party u decides to match with v **and v is honest**, then v must match with u.
- **Stability**: There is no blocking **pair made of 2 honest parties.**
- An honest party can decide to match with nobody. 
- **Termination**: Every **honest** party decide to match with someone **or nobody**.

Byzantine setting

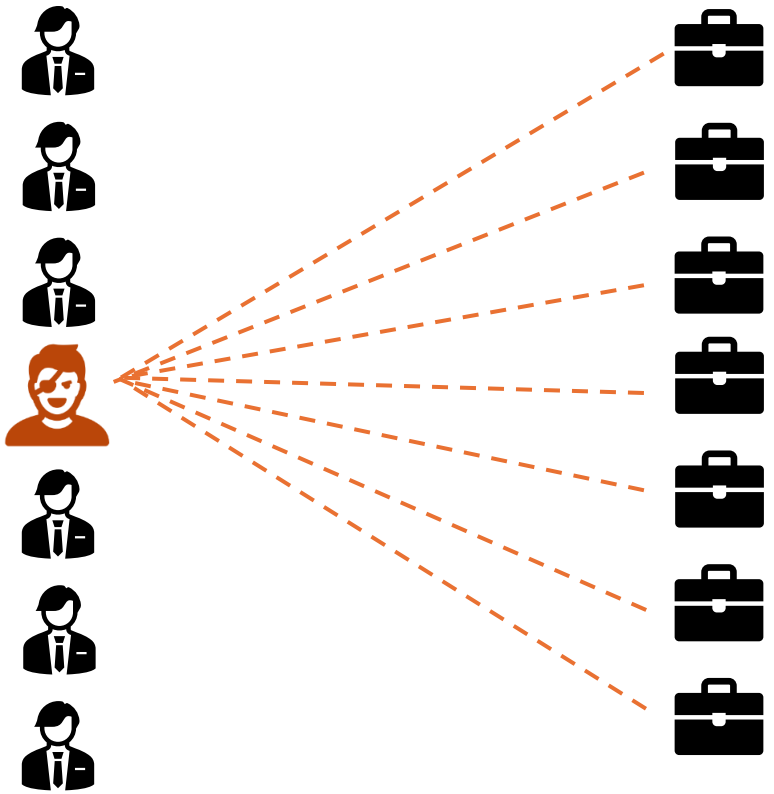


Byzantine setting



Non-competition: 2 honest parties cannot decide to match with the same individual.

Byzantine setting

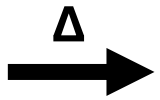


(monogamy)

Non-competition: 2 honest parties cannot decide to match with the same individual.

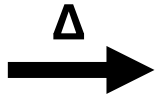
Distributed setting

Distributed setting



Synchronous setting

Distributed setting

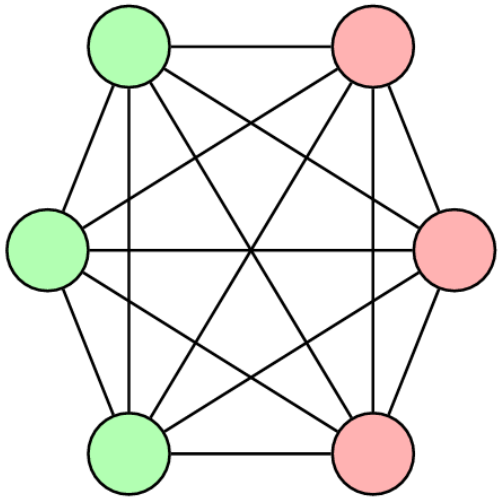


Synchronous setting

PKI (Public Key Infrastructure): Our approach accounts for settings both with and without PKI availability

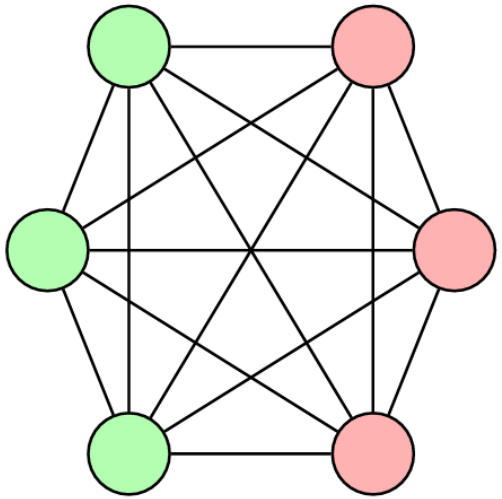
Communication setting

Communication setting

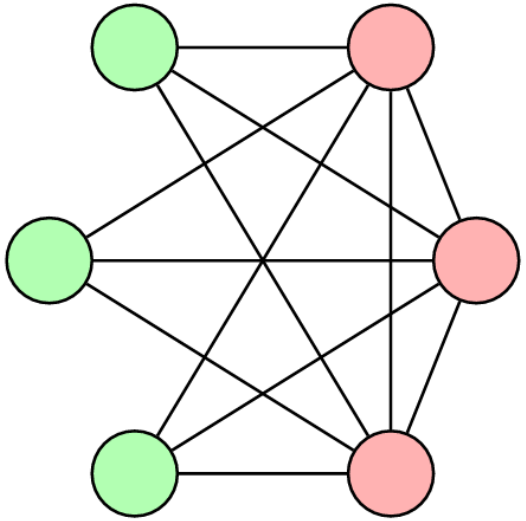


Complete

Communication setting

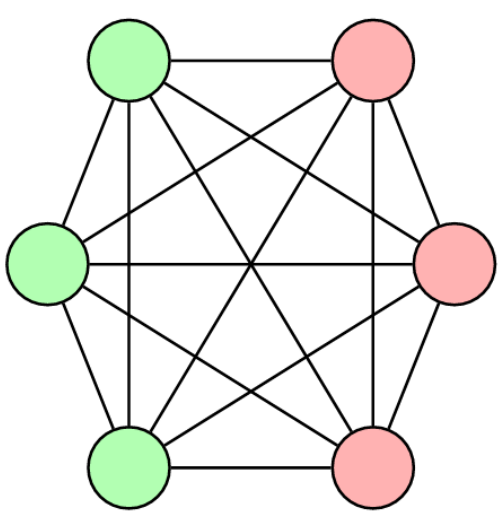


Complete

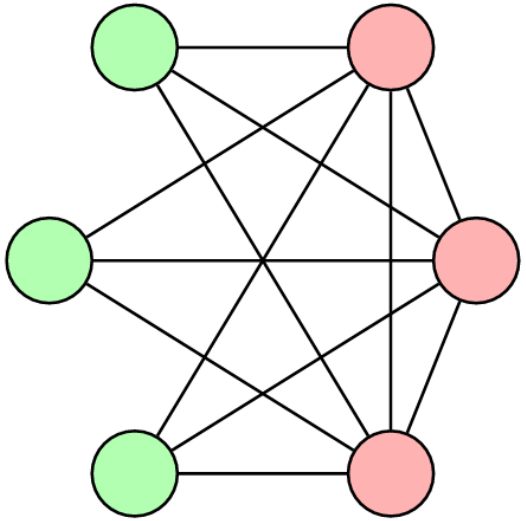


One-sided

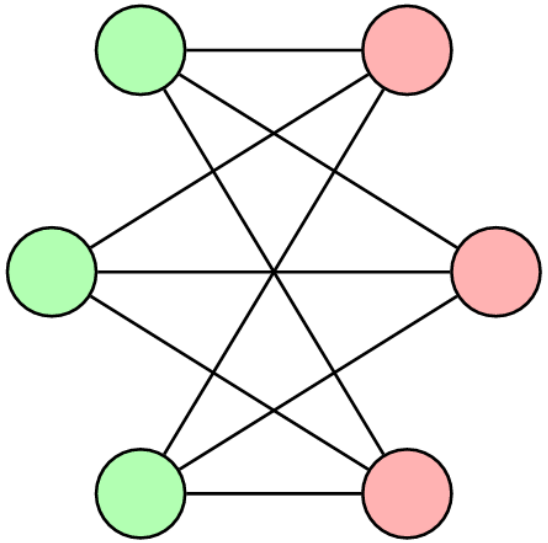
Communication setting



Complete



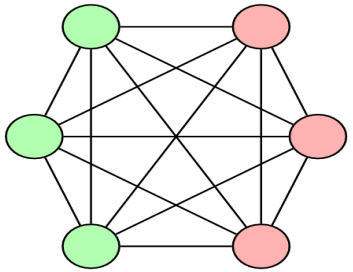
One-sided



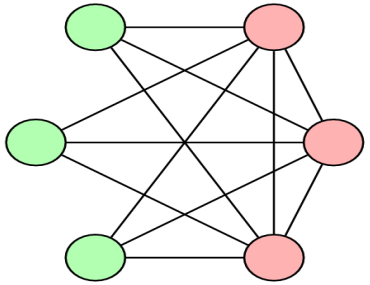
Bipartite

Our results

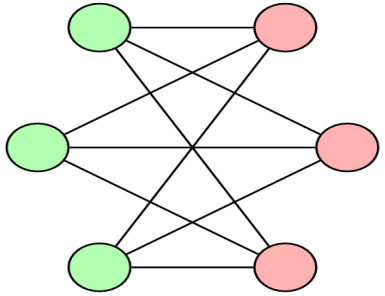
Our results



Complete

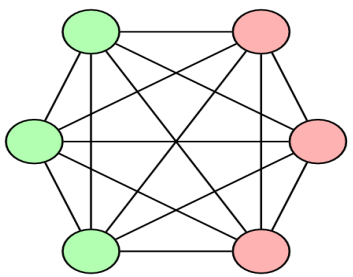


One-sided

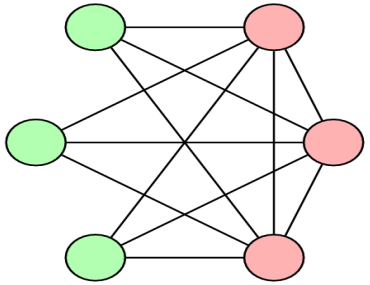


Bipartite

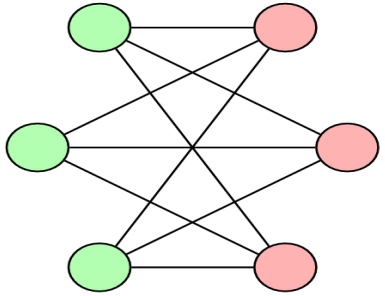
Our results



Complete



One-sided

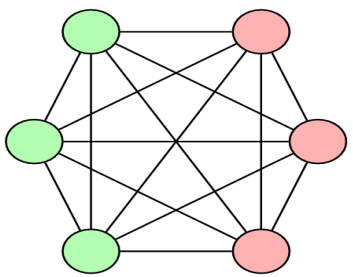


Bipartite

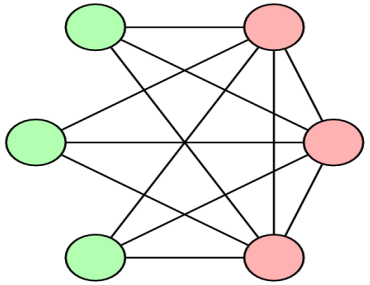
PKI

No PKI

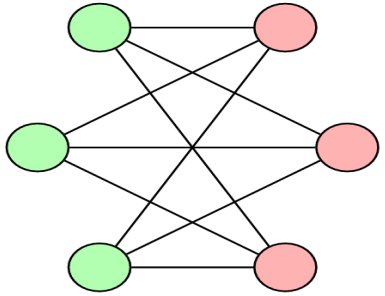
Our results



Complete



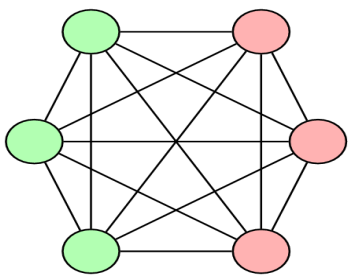
One-sided



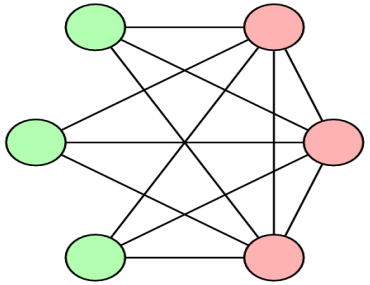
Bipartite

	PKI	No PKI
	Lower bound	Upper bound

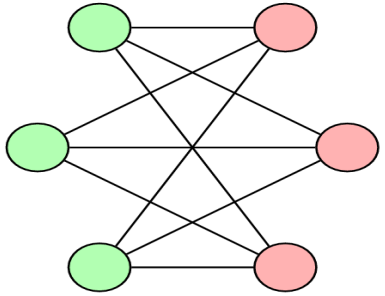
Our results



Complete



One-sided



Bipartite

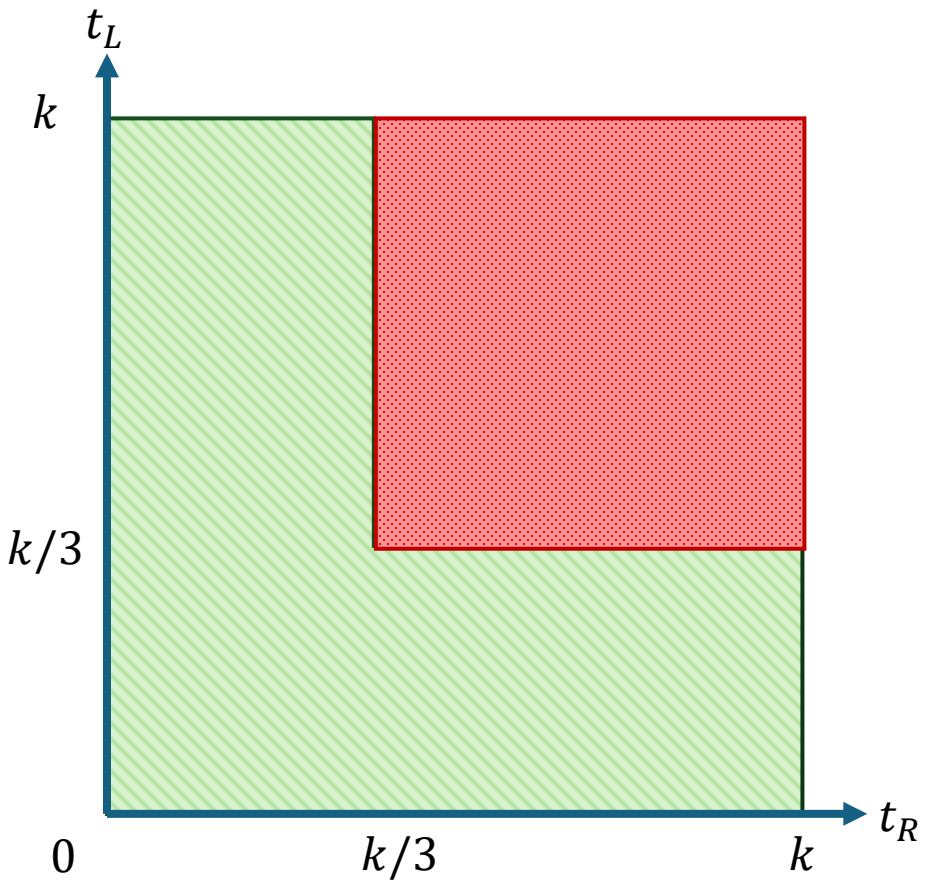
	PKI	No PKI
	Lower bound	Upper bound

We provide tight bounds for all of these cases!

Results: Without PKI

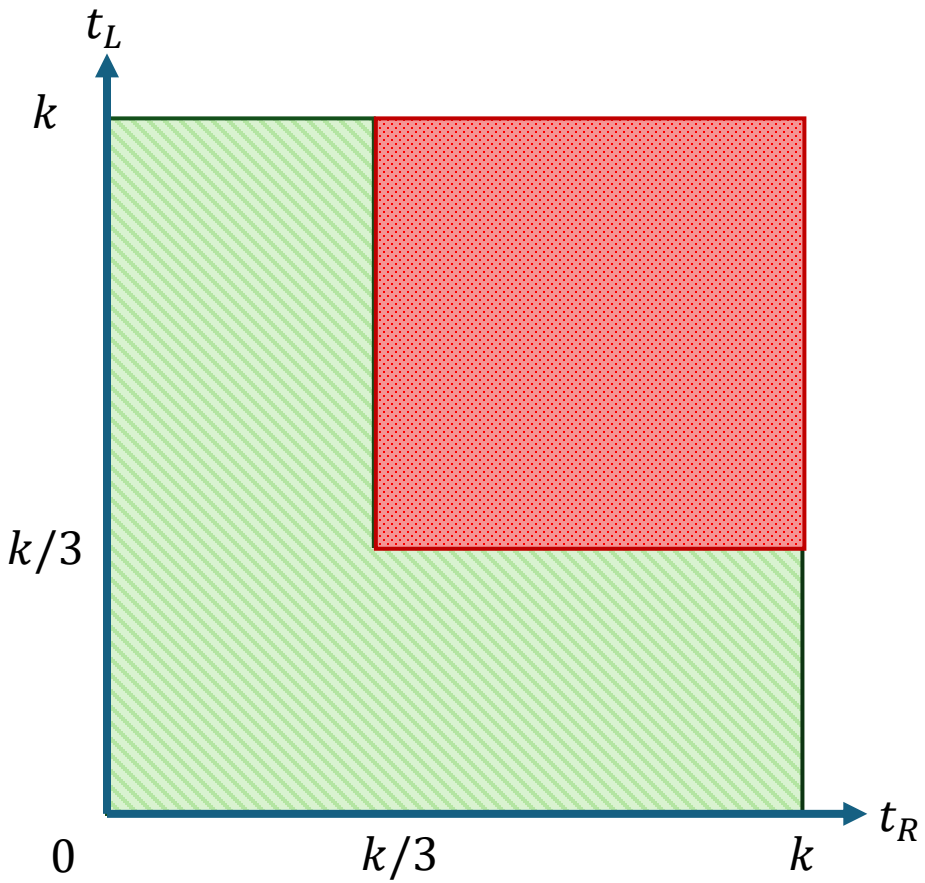
Results: Without PKI

Complete communications:

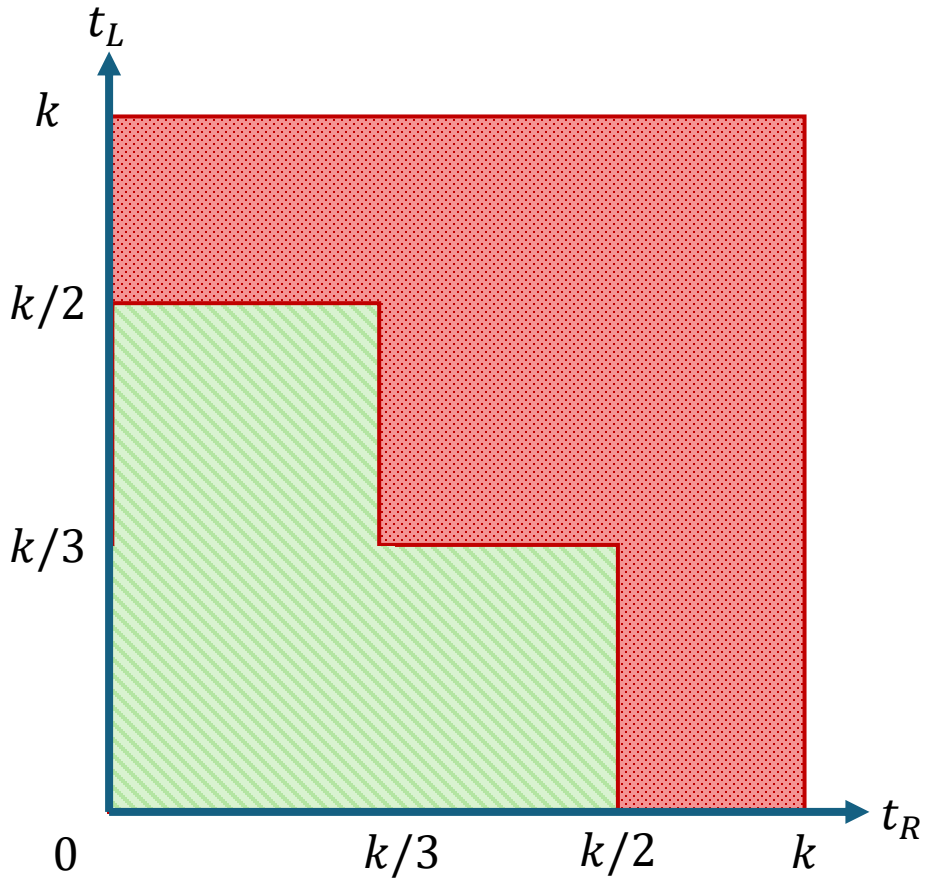


Results: Without PKI

Complete communications:

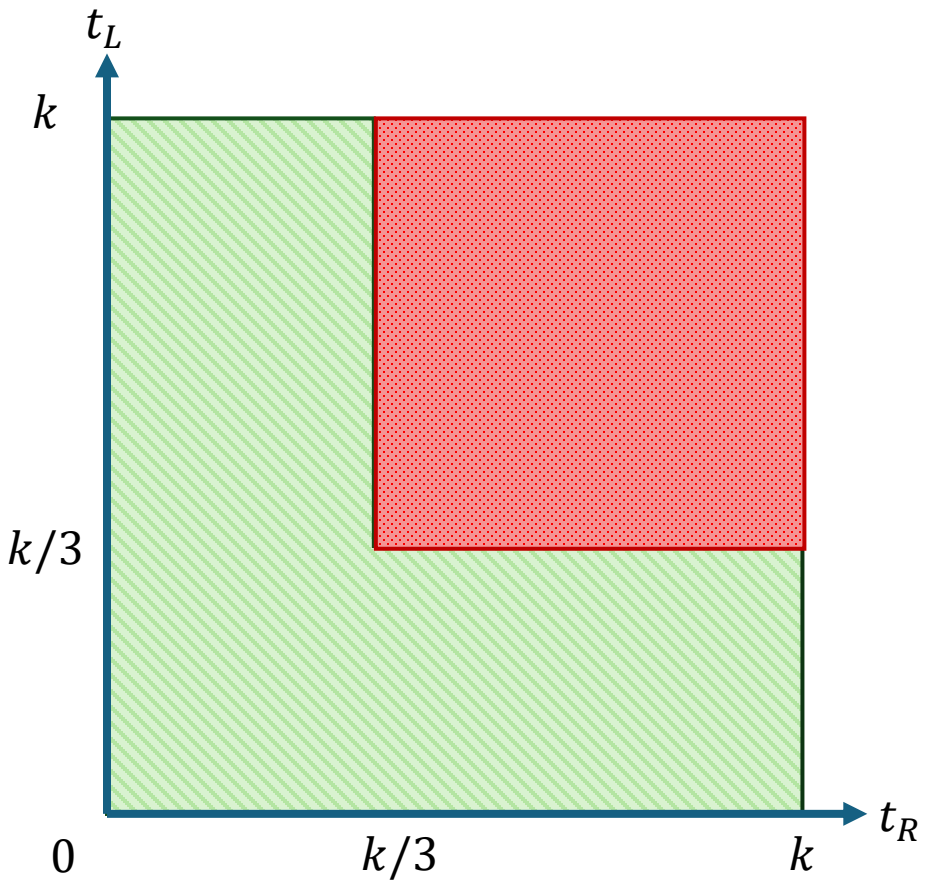


Bipartite communications:

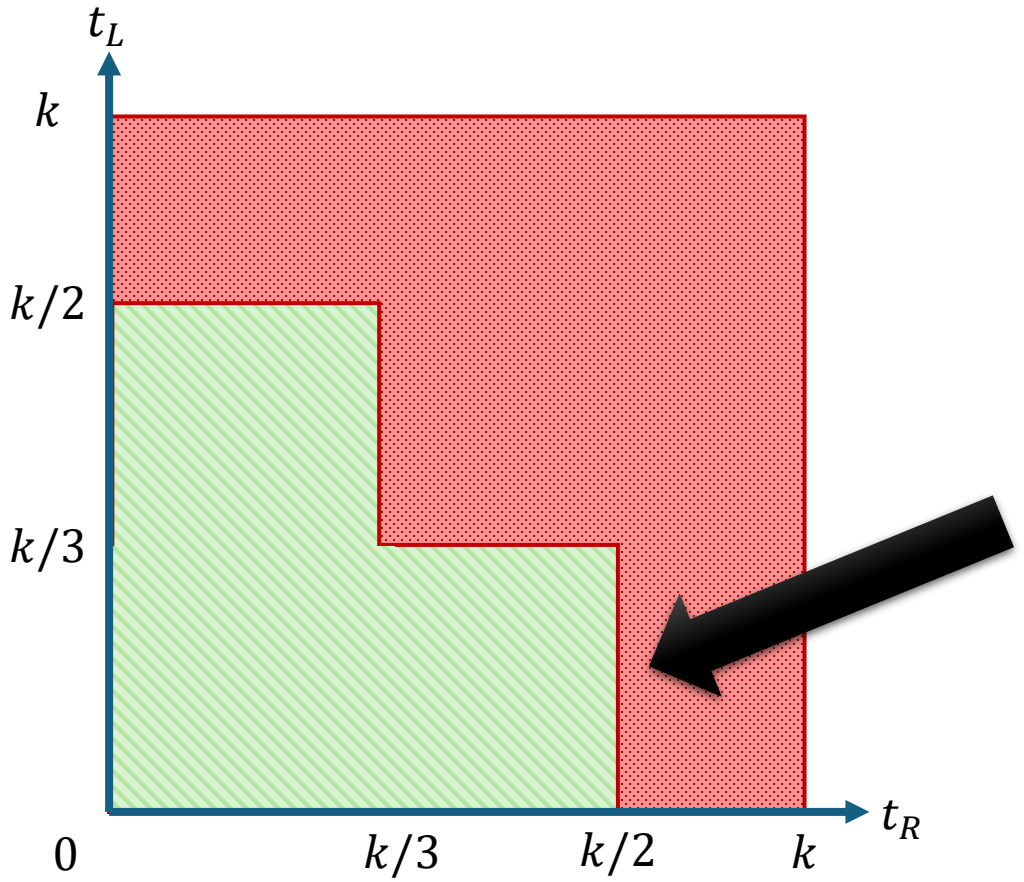


Results: Without PKI

Complete communications:



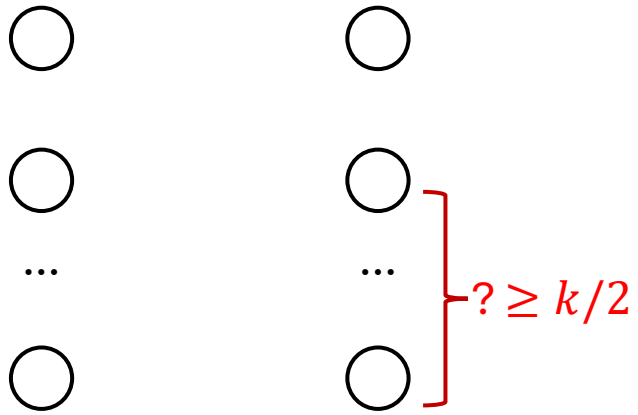
Bipartite communications:



Lower bound

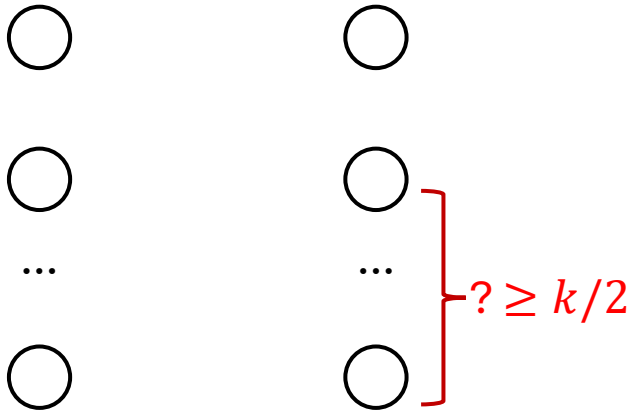
Lower bound

- Without PKI, with bipartite communications, if $t_L = 0$ and $t_R \geq k/2$, then stable matching is not solvable.

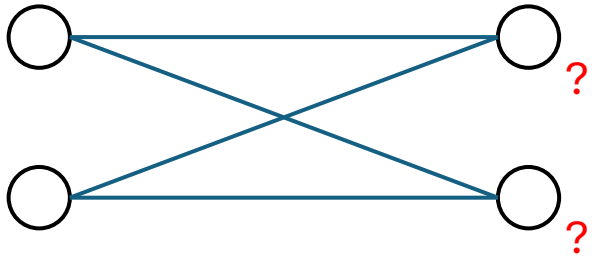


Lower bound

- Without PKI, with bipartite communications, if $t_L = 0$ and $t_R \geq k/2$, then stable matching is not solvable.

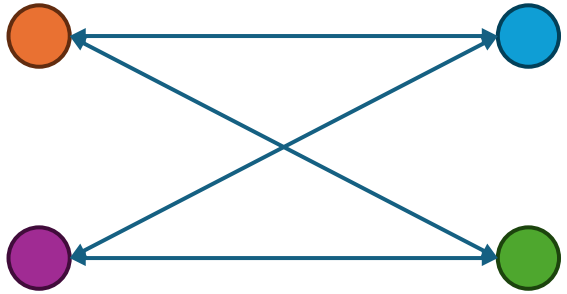


- Without PKI, with bipartite communications and $n = 4$, if $t_L = 0$ and $t_R = 1$, then stable matching is not solvable.

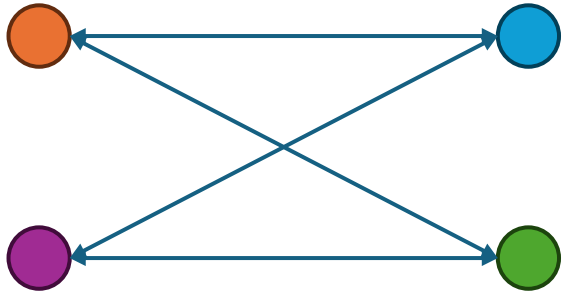


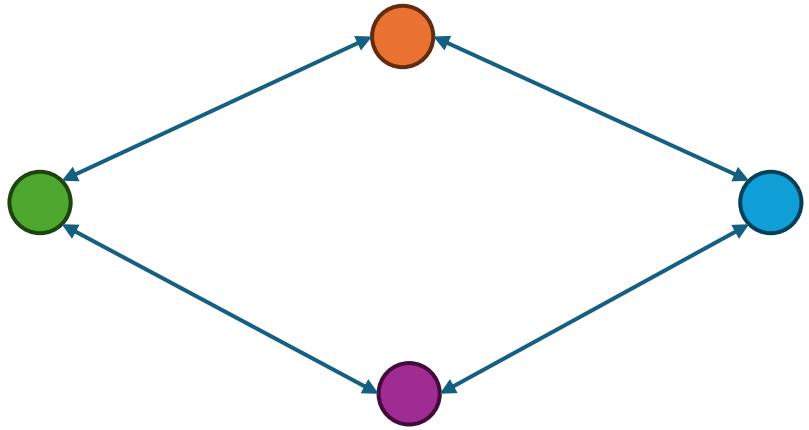
Assume by contradiction a protocol A solves stable matching in this setting

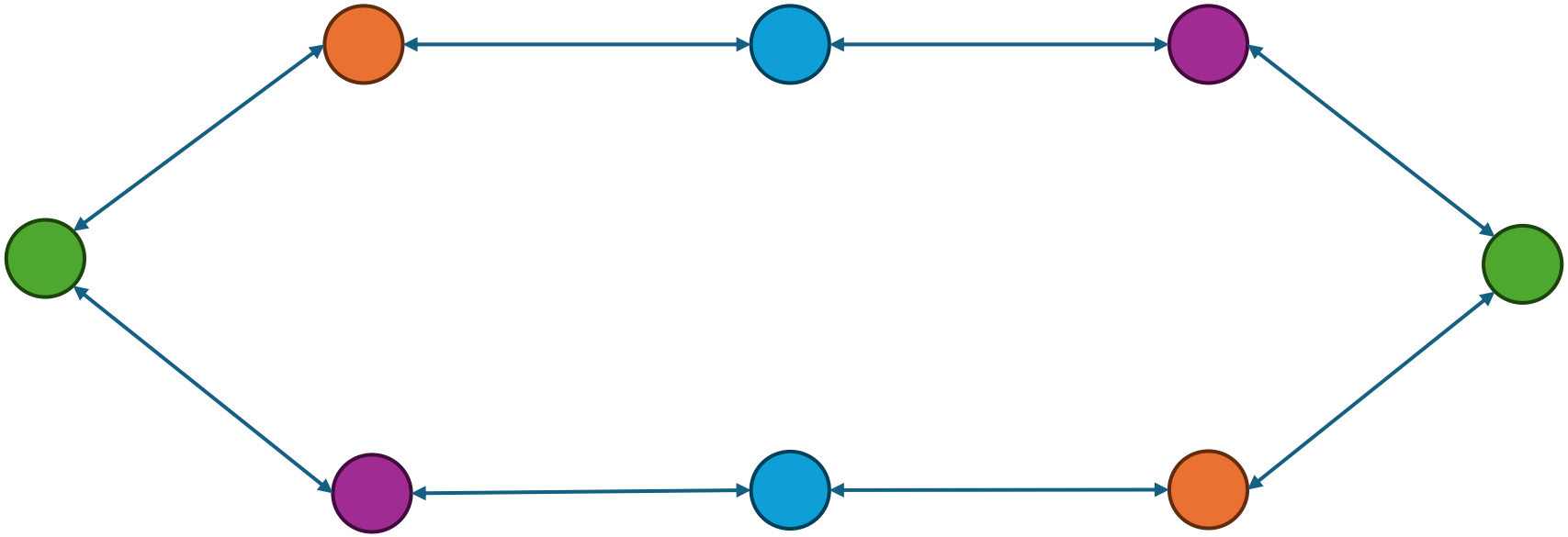
Assume by contradiction a protocol A solves stable matching in this setting

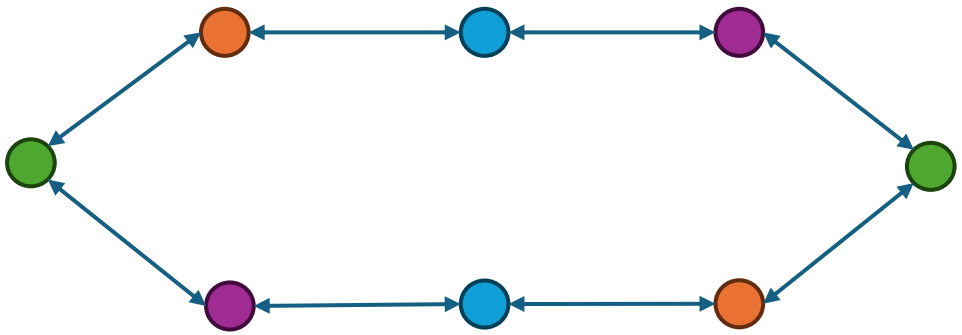


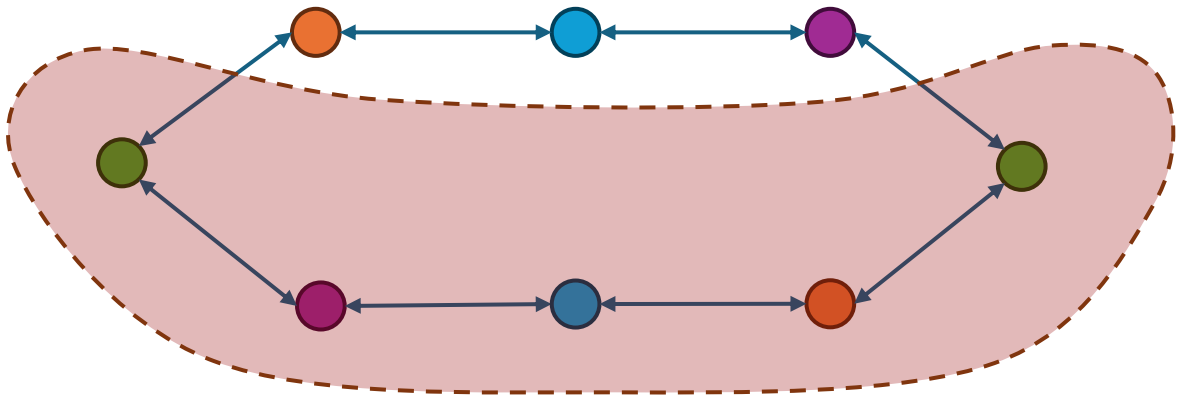
Assume by contradiction a protocol A solves stable matching in this setting

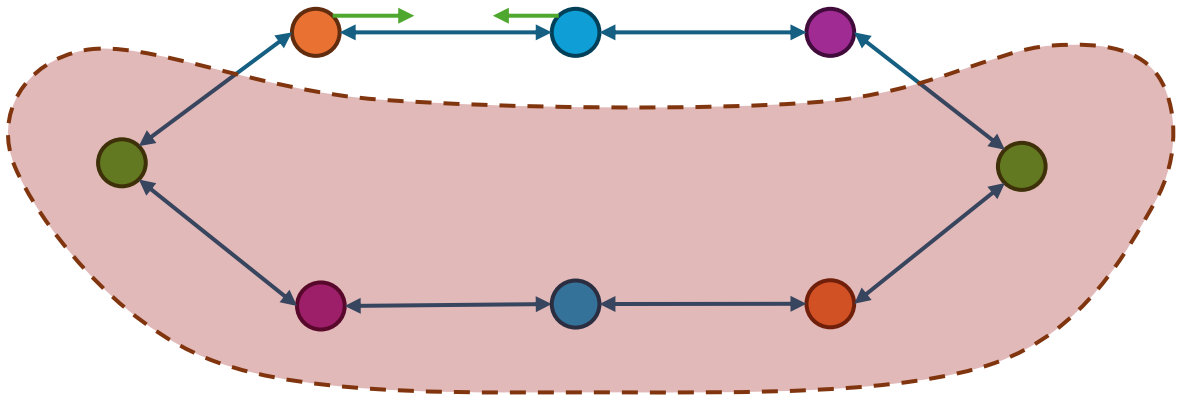


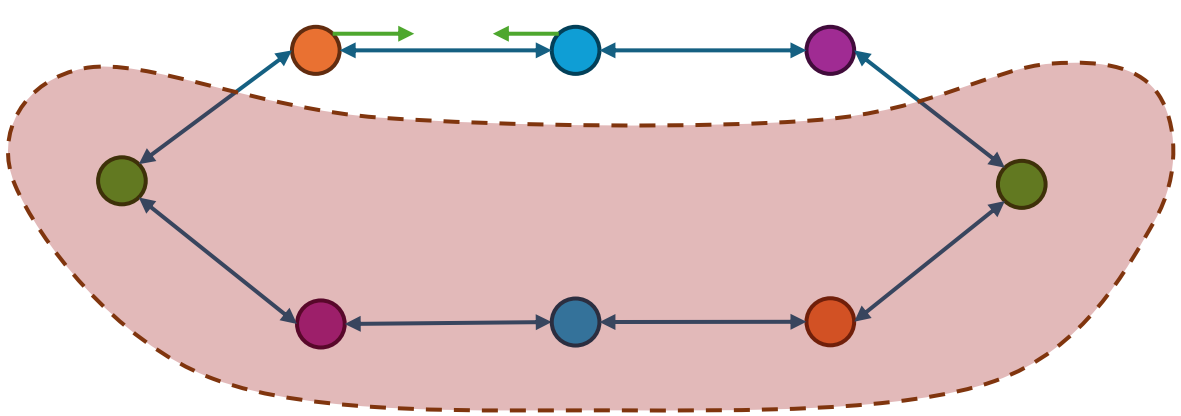


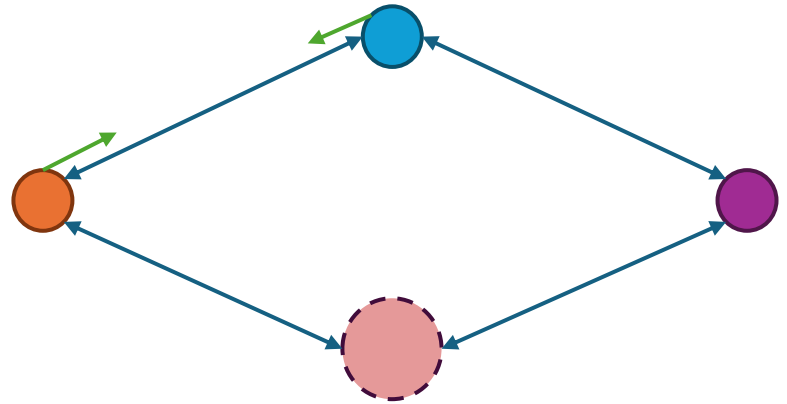


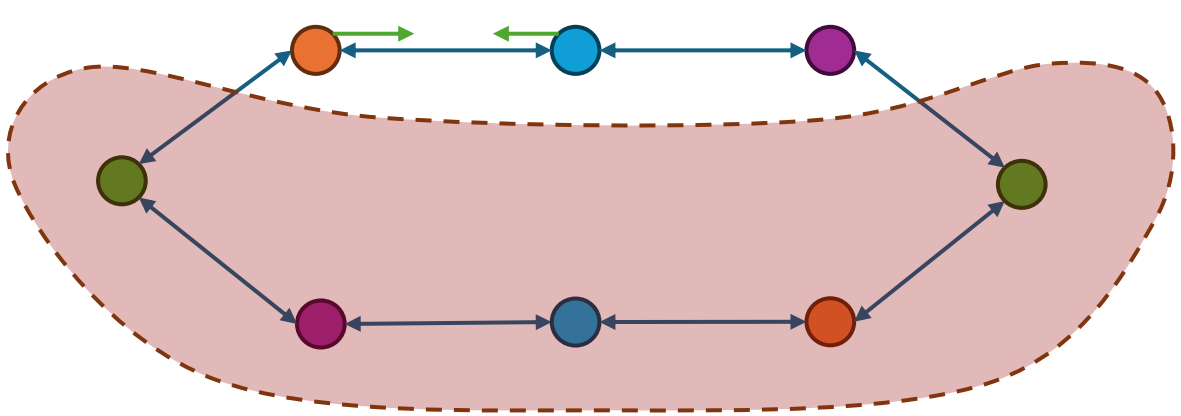


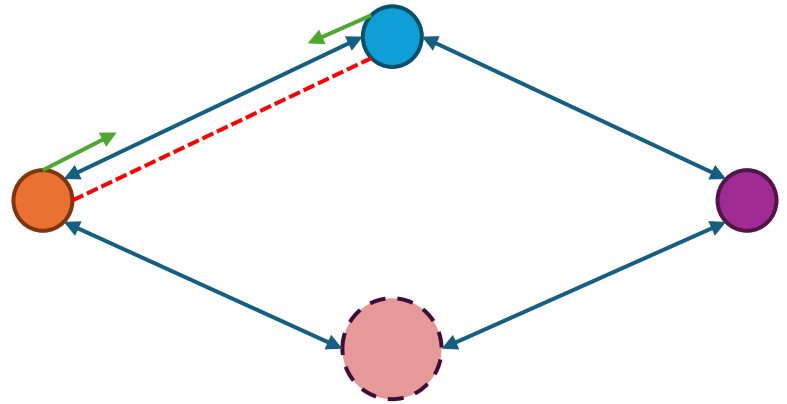


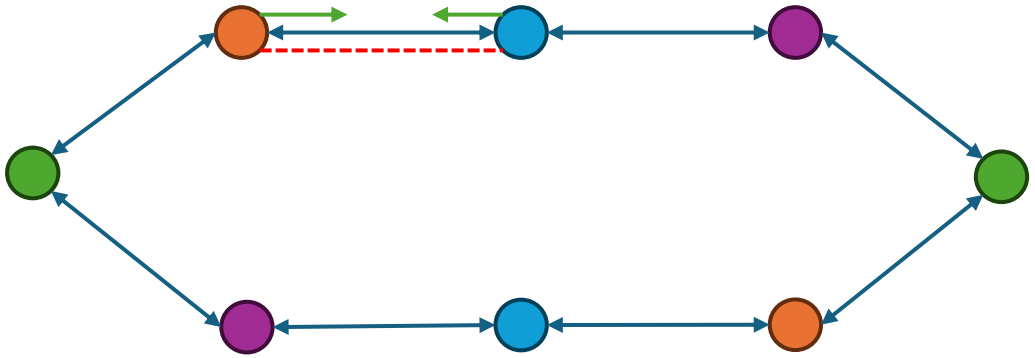


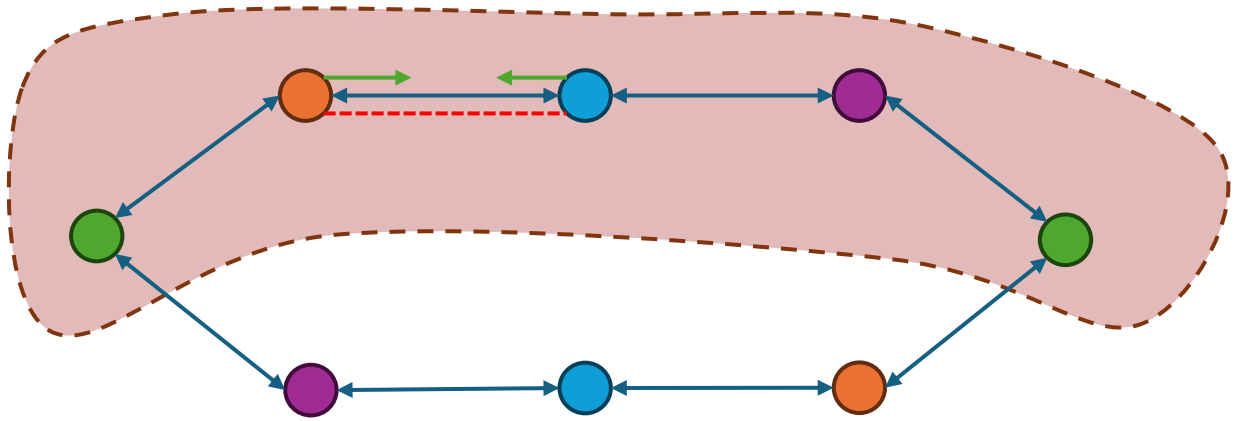


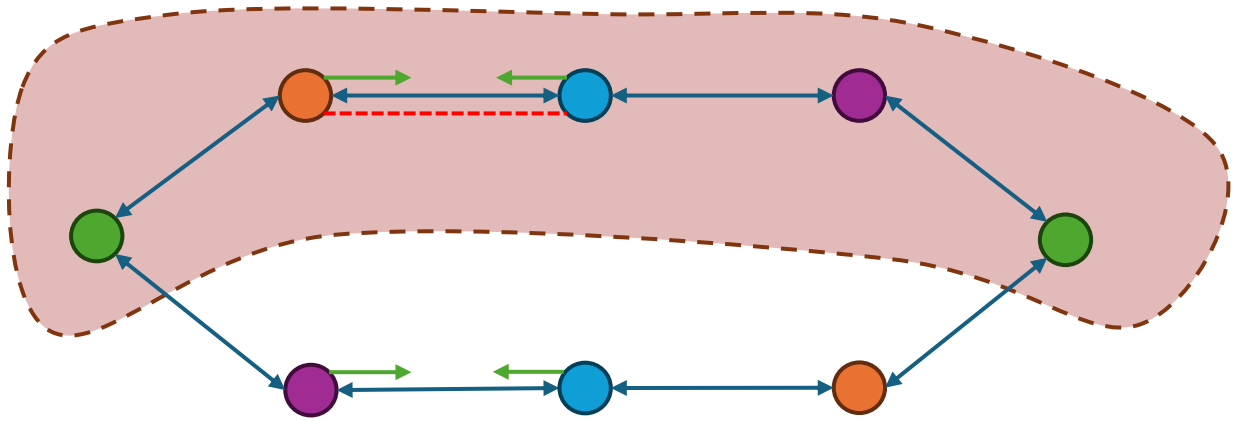


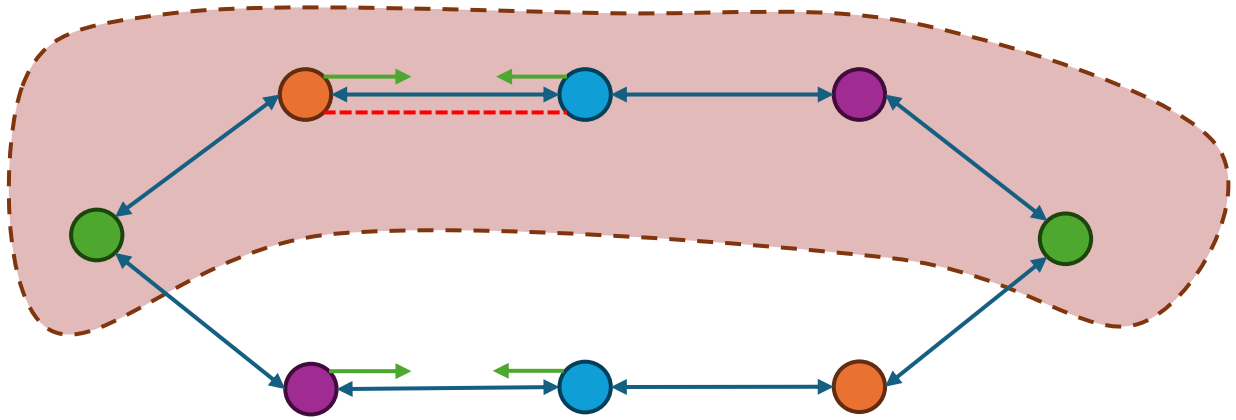


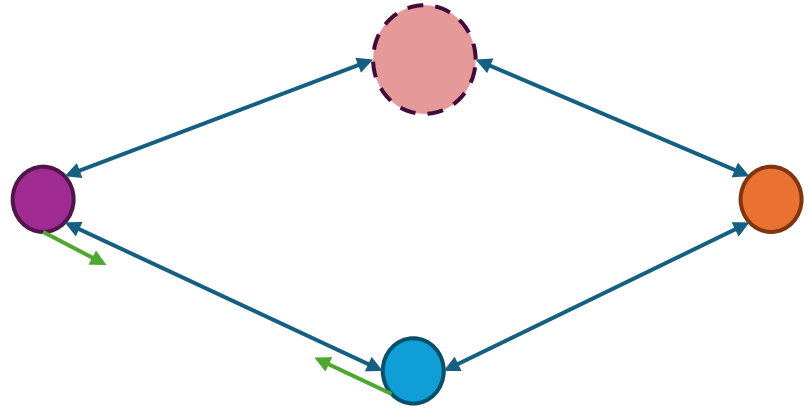


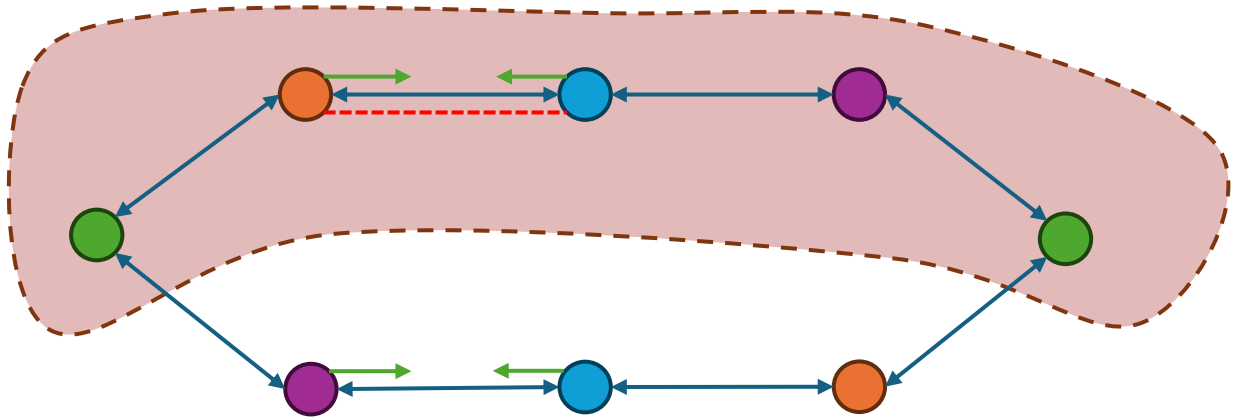


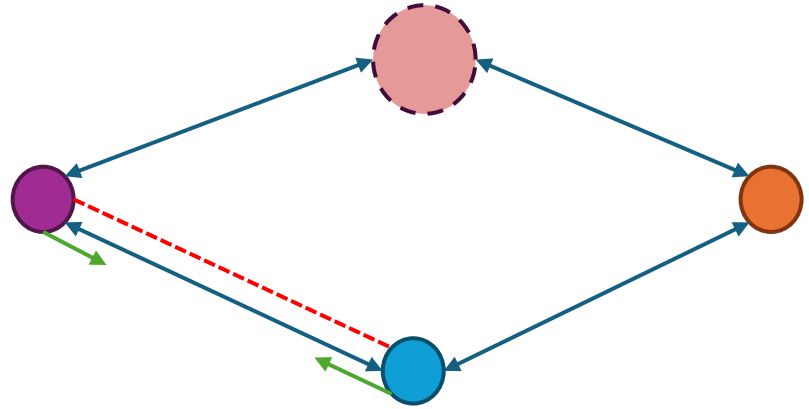


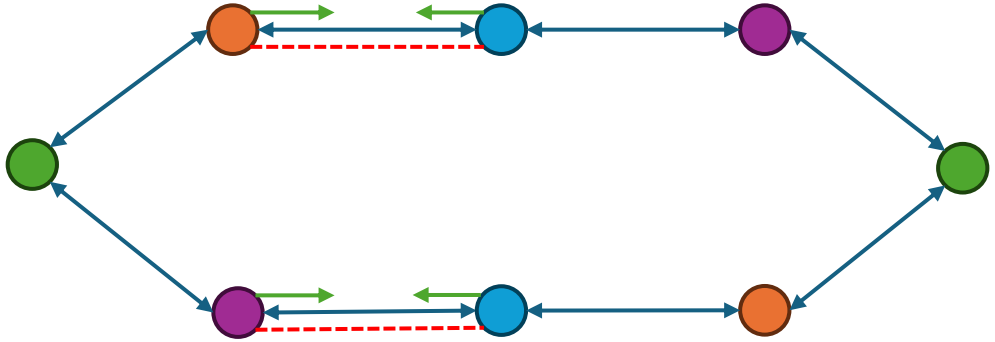


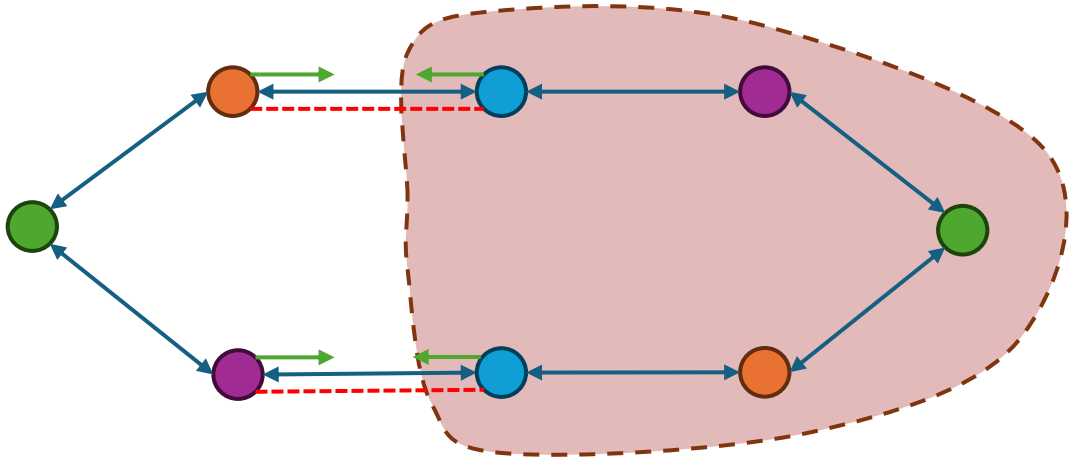


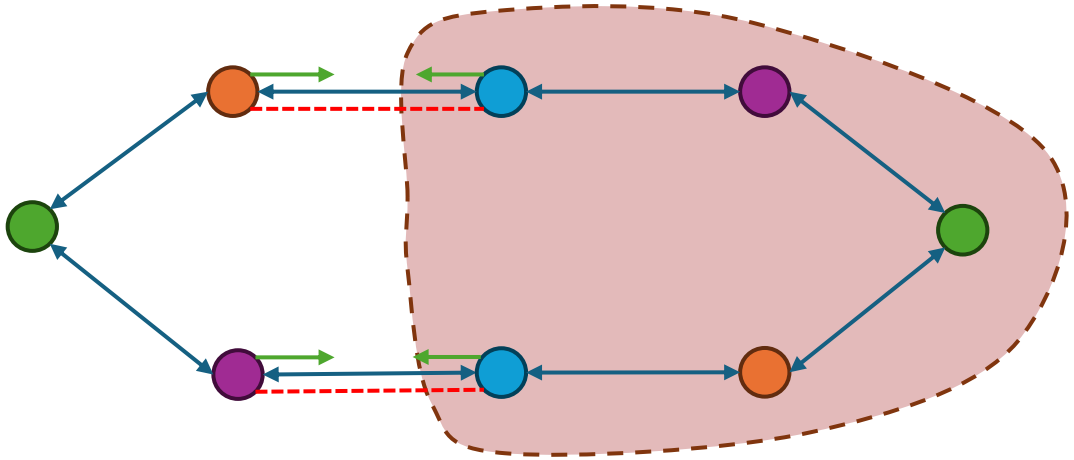


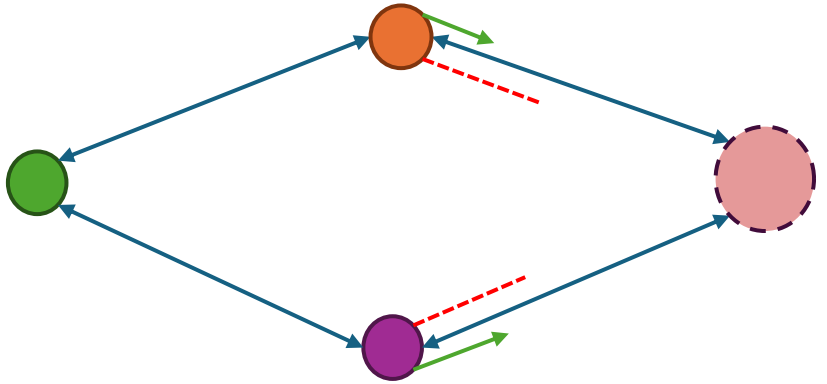


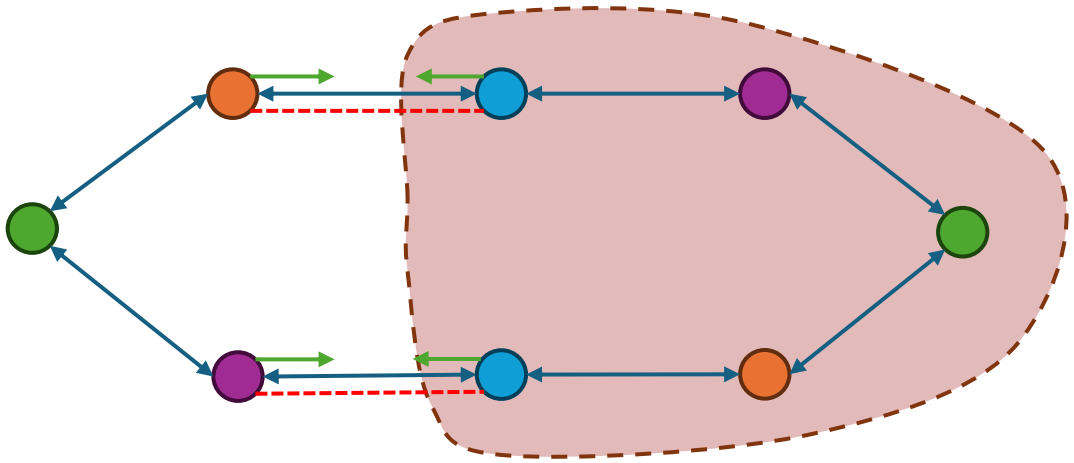


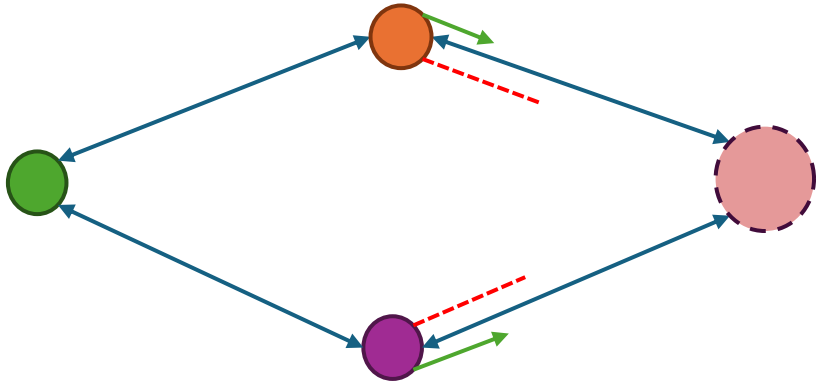








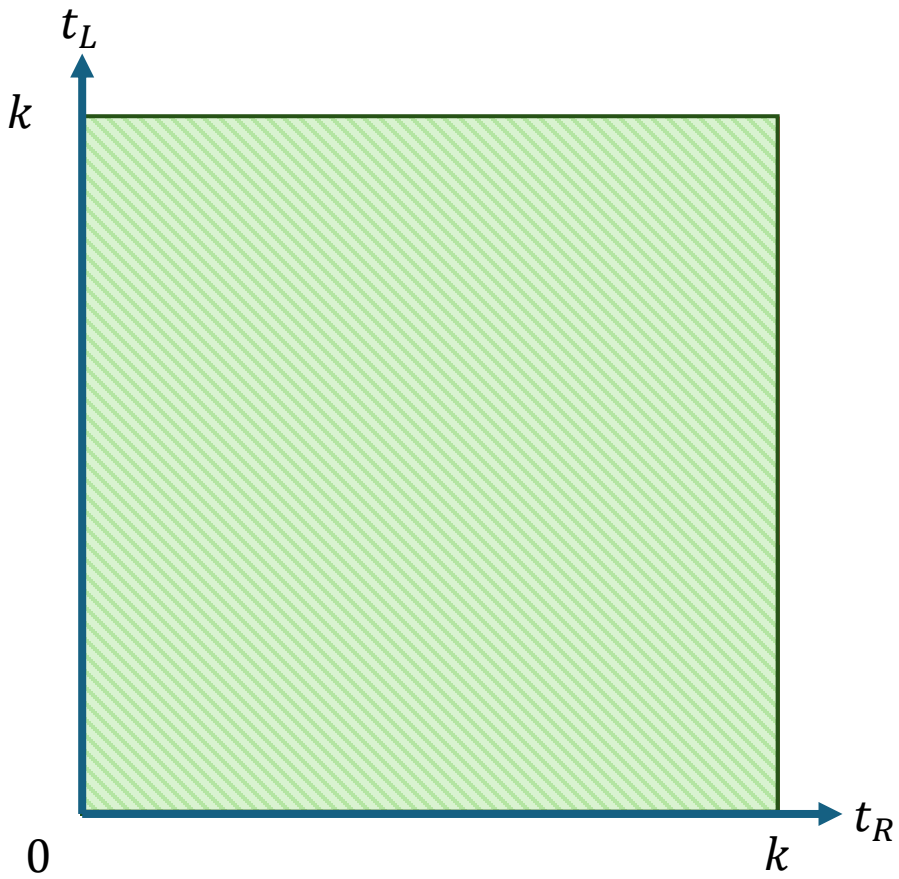




This contradicts the non-competition rule!

Results: With PKI

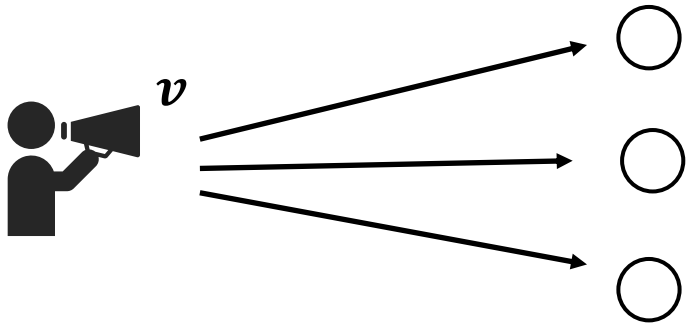
Complete communications:



Upper bounds

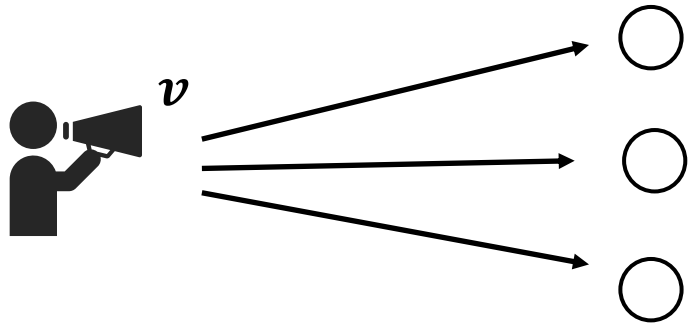
Upper bounds

Byzantine broadcast: A party broadcasts its value. If the sender is honest, everyone receives its value. Otherwise everyone receives the same value.



Upper bounds

Byzantine broadcast: A party broadcasts its value. If the sender is honest, everyone receives its value. Otherwise everyone receives the same value.

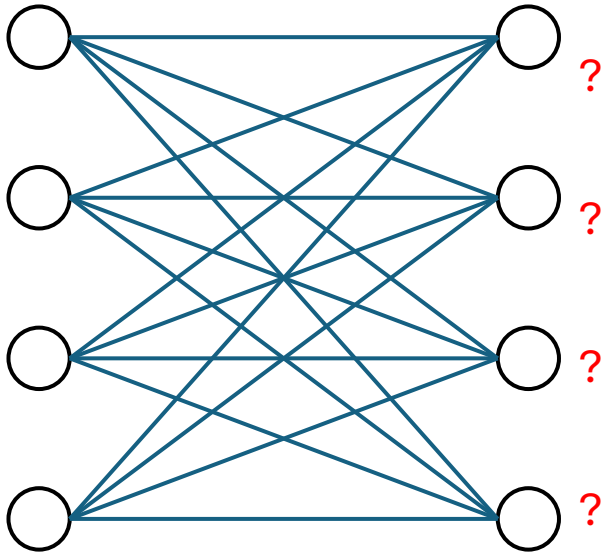


Byzantine broadcast → **Stable matching**

Are there cases where byzantine broadcast is not possible but stable matching is solvable?

Are there cases where byzantine broadcast is not possible but stable matching is solvable?

Bipartite setting, $t_R = k$ and $t_L = 0$



NO

NO

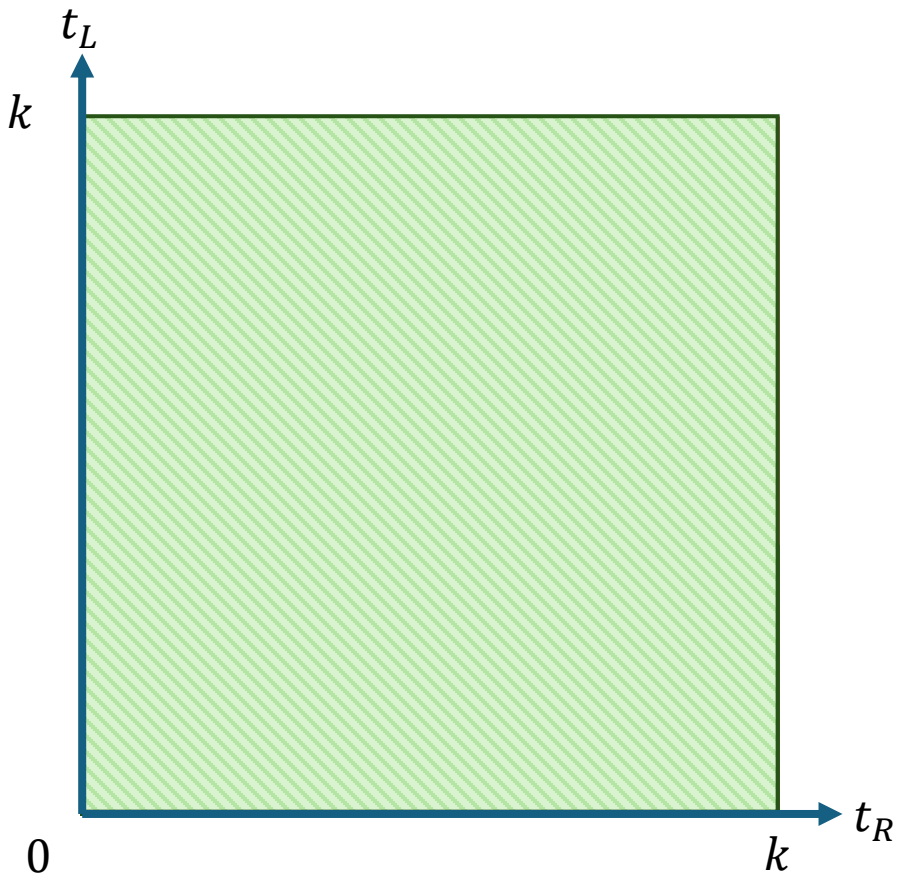
(without PKI)

YES!

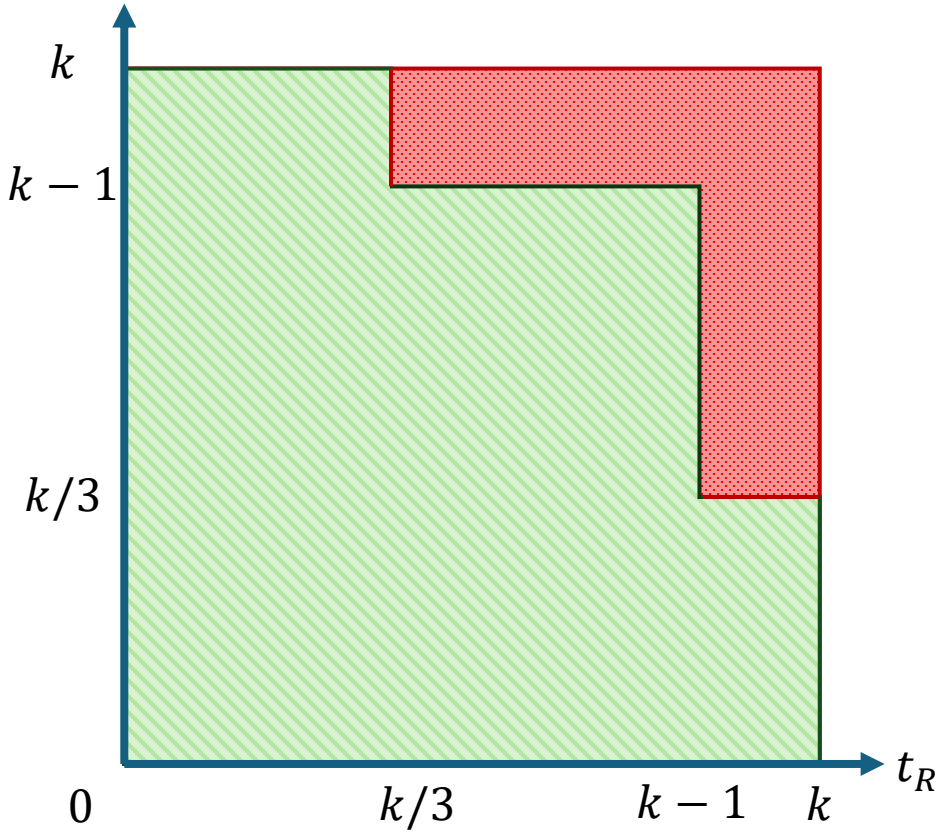
(with PKI)

Results: With PKI

Complete communications:



Bipartite communications:



Open questions

Open questions

- Communication complexity

Open questions

- Communication complexity
  - Without byzantines there is a $\Omega(n^2)$ bits lower bound

Open questions

- Communication complexity
  - Without byzantines there is a $\Omega(n^2)$ bits lower bound

- Partially synchronous / asynchronous setting

Open questions

- Communication complexity
  - Without byzantines there is a $\Omega(n^2)$ bits lower bound
- Partially synchronous / asynchronous setting
  - Not solvable even with a single byzantine party

Open questions

- Communication complexity
  - Without byzantines there is a $\Omega(n^2)$ bits lower bound
- Partially synchronous / asynchronous setting
  - Not solvable even with a single byzantine party
- Stable roomates problem

Open questions

- Communication complexity
  - Without byzantines there is a $\Omega(n^2)$ bits lower bound
- Partially synchronous / asynchronous setting
  - Not solvable even with a single byzantine party
- Stable roomates problem
  - There does not always exist a solution

Questions ?