Security & Economics — Part 4

Basic ideas about market

Dusko Pavlovic

Spring 2014

Outline

Introduction

Auctions

Matching demand and supply

Outline

Introduction

Where are we?

Market security

Auctions

Matching demand and supply

Two parts

1. pricing/costing of security investment
2. security of pricing/costing

Two parts

1. market view of security
2. security view of market

Two parts

The employment view

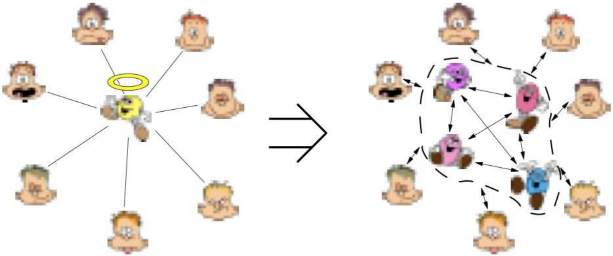
- **security manager**:
  - accounting tools for the market of security
- **mechanism designer**:
  - security tools for network economy

What is security?

Local requirements imposed on global processes

- access/availability of resources
- authenticity/confidentiality of information flows
- public and private benefit in social processes
  - voting
  - markets

Protocols



Social ⊆ Computational ⊆ Social

- Social processes are computations
    - market computes prices
    - voting computes joint preferences
- Network computations are social processes
    - wisdom of the crowds
    - information cascades

Ages of computation

ages	*ancient*	*middle*	*modern*
platform	computer	operating system	network
paradigms	Quicksort, compilers	MS Word, Oracle	WWW, botnets
tasks	correctness, termination	liveness, safety	security
tools	programming languages	specification languages	scripting languages

Security requirements are crucial

Individual choice

- Individual choices are guided by individual preferences, i.e. private utility functions
- Private benefit is achieved by maximizing the private utility.

Social choice

- Public benefit is achieved by maximizing the total utility, i.e. the sum of individual utilities.
- The goal of social choice protocols is to maximize public benefit.

Problem of social choice

- Individual preferences diverge; they are often inconsistent
- Reconciling them leads to strategic behaviors
- Public benefit get overwhelmed by private benefits: oligopoly, dictatorship

Protocols for social choice

Two forms of social choice

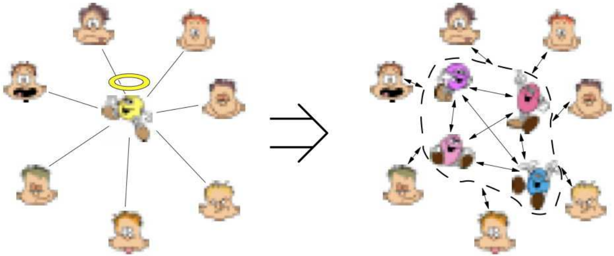
- market: aggregate utilities (quantitative)
- voting: aggregate preferences (qualitative)

Protocols for social choice

Two forms of social choice

- market: Lectures 5–7
- voting: Lecture 8

Market protocols



Market is a multi-party computation of the prices

Market and crime

Market and crime are

- security problems
  - multiparty computation, protocols, social processes
- economic processes
  - concerning goods, wealth and public/private property

Market computation modeling

- Market security

Market computation modeling

- Market security

$\Uparrow$

- Auction security

Market computation modeling

- Market security

  $\Uparrow$

- Auction security

  $\Uparrow$

- Games and mechanisms

Outline

Maket goal and setup

Setup

- every asset is owned by a single agent
- every agent has a utility for all assets

Maket goal and setup

Setup

- every asset is owned by a single agent
- every agent has a utility for all assets

Goal

Maximize everyone's utility by:

- general: redistributing the assets
- simple: exchanging the assets pairwise
- complex: sell and buy

Maket goal and setup

Exchange and surplus

*u*tility	wheat	wine
Alice	2	1
Bob	3	7

If Alice owns wine and Bob owns wheat

then their utilities are 1 and 3.

Maket goal and setup

Exchange and surplus

utility	wheat	wine
Alice	2	1
Bob	3	7

If Alice owns wheat and Bob owns wine

then they have utilities 2 and 7.

Maket goal and setup

Exchange and surplus

utility	wheat	wine
Alice	2	1
Bob	3	7

If Alice owns wheat and Bob owns wine

then they have utilities 2 and 7.

Their **surpluses** of exchange are 1 and 4.

Market: Functional requirement

- optimal matching of the users and the goods

Market: Security requirement

- beneficial (stable, productive, fair) distribution of the surplus

Market: Functional problem

Computational obstacle

Optimal matching can be doubly exponential:

- every pair of goods may need to be compared for
- every pair of agents

Market: Functional solution

Idea

Mediate the comparisons through a *universal value*, by exchanging

- offered goods → universal value
- universal value → needed goods

Market: Functional solution

Idea

Mediate the comparisons through a *universal value*, by exchanging

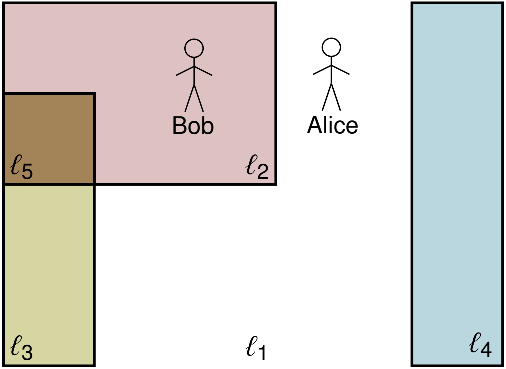
- offered goods → universal value
- universal value → needed goods

This requires a **protocol**.

First security protocol?

(if not from a science)

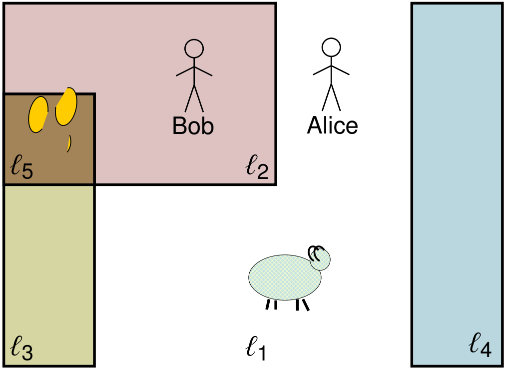
About 6000 years ago, Kain's son Bob built a secure vault



First security protocol?

(if not from a science)

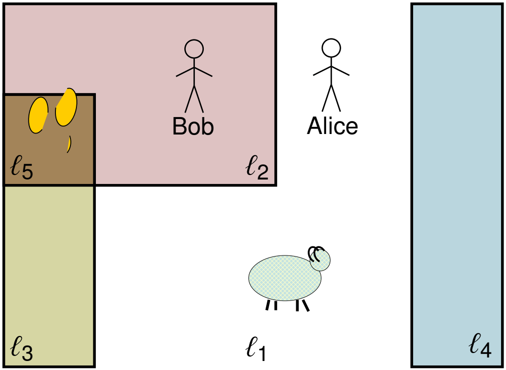
and stored his goods in it



First security protocol?

(if not from a science)

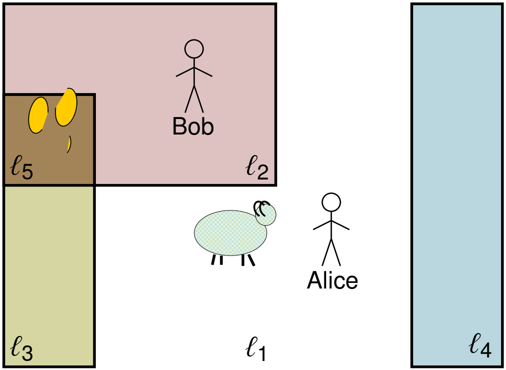
and stored his goods in it.



First security protocol?

(if not from a science)

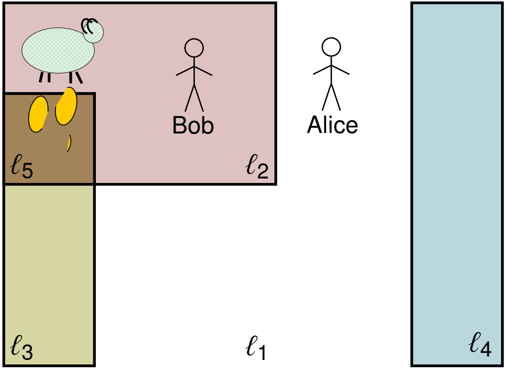
and stored his goods in it. When Alice wanted to go for a vacation



First security protocol?

(if not from a science)

and stored his goods in it. When Alice wanted to go for a vacation, she stored her goods there too.



First security protocol?

(if not from a science)

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure : Louvre, Paris

First security protocol?

(if not from a science)

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure : Louvre, Paris

- To take the sheep, Alice must give the token.

First security protocol?

(if not from a science)

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure : Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.

First security protocol?

(if not from a science)

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure : Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.

First security protocol?

(if not from a science)

- This protocol goes back to Uruk (Irak), 4000 B.C.

First security protocol?

(if not from a science)

- This protocol goes back to Uruk (Irak), 4000 B.C.
- Money developed from security tokens.

First security protocol?

(if not from a science)

- This protocol goes back to Uruk (Irak), 4000 B.C.
- Money developed from security tokens.
- Numbers developed from security annotations.

First security protocol?

(if not from a science)

- This protocol goes back to Uruk (Irak), 4000 B.C.
- Money developed from security tokens.
- Numbers developed from security annotations.
- Cuneiform alphabet developed later.
- Science developed still later.

Market protocol is based on **money**

Idea: trade = sell + buy

Exchange goods through **money**:

- *sell:* offered goods → money
- *buy:* money → needed goods

Remaining market problem

Find the best

- buyers
- sellers

in order to

- *function:* maximize the surplus
- *security:* keep most of the surplus

Complete information ⇒ Bargaining

If the buyers and the sellers know each other's valuations, they only need to bargain how to split the surplus.

Asymmetric information ⇒ No market

- If the seller knows highest buyer's utility, he asks a price just below
  - and keeps all of the surplus
- If the buyer knows lowest seller's utility, he just offers a price just above
  - and keeps all of the surplus

Incomplete information ⇒ Auctions

If the buyers and the sellers do not know each other's valuations, they use auction protocols to *elicit price offers*.

Auction protocols: Requirement

Given a set of sellers and a set of buyers with *private utilities*, auction protocols are designed to

- maximize seller's revenue: supply auctions
- minimize buyer's cost: procurement auctions

Auction protocols: Problem

- To maximize revenue, the sellers must keep their utility private
- To minimize cost, the buyers must keep their utility private

Auction protocols: Goal

Elicit truthful bidding:

- the participants should bid as close as possible to their true valuations

Auction protocols: Goal

Definition

An auction mechanism is said to be *incentive compatible* if it elicits truthful bidding, i.e. provides the bidders with an incentive to bid their true valuations.

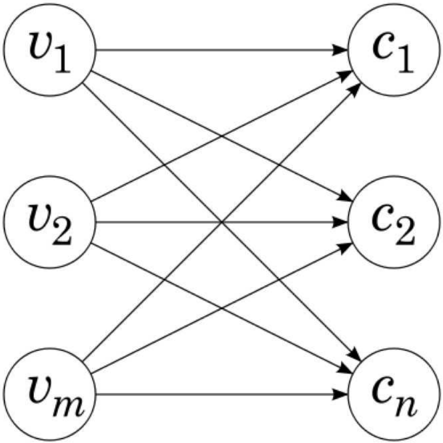
Auction protocols: Goal

- How is this goal fulfilled?

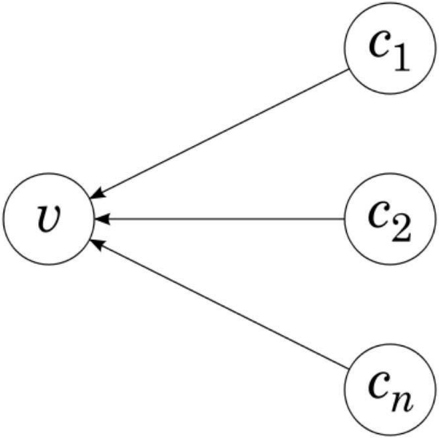
Auction protocols: Goal

- How is this goal fulfilled?
- How do auctions work?
- What types of auctions are there?

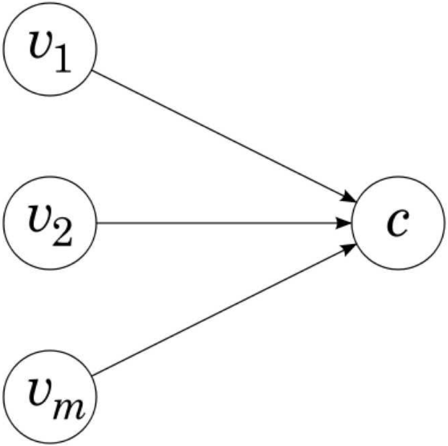
Multi-item auction



Single-user procurement (demand) auction



Single-item (supply) auction



Taxonomy of single item auctions

	interactive	sealed bid
strategic	descending	first price
truthful	ascending	second price

Equivalence of interactive and sealed bidding

- with the ascending auction, the highest bidder pays second highest bidder's valuation
- with the descending auction, the highest bidder pays the first announcememt below his own valuation

Explaining away interactive bidding

- Interactions only determine how much of the information about each other's bids to the bidders get
  - cf the difference between English and Japanese auction
- With sealed bid auction, they get a minimum: each bidder just learns whether his bid is the highest

Explaining away interactive bidding

- Interactions only determine how much of the information about each other's bids to the bidders get
  - cf the difference between English and Japanese auction
- With sealed bid auction, they get a minimum: each bidder just learns whether his bid is the highest
- We abstract away the interaction and study sealed bid auctions.

Modeling auctions as games

- players: $i = 1, 2, \ldots, n$
- moves: $A_i = \mathbb{R}$
- payoffs: $u = \langle u_i \rangle_{i=1}^{n} : A \to \mathbb{R}^n$

Modeling auctions as games

- players: $i = 1, 2, \ldots, n$
- moves: $A_i = \mathbb{R}$
- payoffs: $u = \langle u_i \rangle_{i=1}^{n} : A \to \mathbb{R}^n$, $A = \prod_i A_i = \mathbb{R}^n$

$$u_i(b) \quad = \quad \tau_i(b) \cdot \big(v_i - p(b)\big)$$

where

- $b = \langle b_i \rangle_{i=1}^{n} \in A$ is the bidding profile

Modeling auctions as games

- players: $i = 1, 2, \ldots, n$
- moves: $A_i = \mathbb{R}$
- payoffs: $u = \langle u_i \rangle_{i=1}^n : A \to \mathbb{R}^n$, $A = \prod_i A_i = \mathbb{R}^n$

$$u_i(b) \quad = \quad \tau_i(b) \cdot \big(v_i - p(b)\big)$$

where

- $b = \langle b_i \rangle_{i=1}^n \in A$ is the bidding profile
- $v = \langle v_i \rangle_{i=1}^n \in \mathbb{R}^n$ is the valuation profile

Modeling auctions as games

- players: $i = 1, 2, \ldots, n$
- moves: $A_i = \mathbb{R}$
- payoffs: $u = \langle u_i \rangle_{i=1}^{n} : A \to \mathbb{R}^n$, $A = \prod_i A_i = \mathbb{R}^n$

$$u_i(b) \quad = \quad \tau_i(b) \cdot \big(v_i - p(b)\big)$$

where

- $b = \langle b_i \rangle_{i=1}^{n} \in A$ is the bidding profile
- $v = \langle v_i \rangle_{i=1}^{n} \in \mathbb{R}^n$ is the valuation profile
- $p(b)$ is the winning price for the bids b

Modeling auctions as games

- players: $i = 1, 2, \ldots, n$
- moves: $A_i = \mathbb{R}$
- payoffs: $u = \langle u_i \rangle_{i=1}^n : A \to \mathbb{R}^n$, $A = \prod_i A_i = \mathbb{R}^n$

$$u_i(b) \quad = \quad \tau_i(b) \cdot \big(v_i - p(b)\big)$$

where

- $b = \langle b_i \rangle_{i=1}^n \in A$ is the bidding profile
- $v = \langle v_i \rangle_{i=1}^n \in \mathbb{R}^n$ is the valuation profile
- $p(b)$ is the winning price for the bids b
- $\tau_i(b) = \left\{\begin{matrix} 1 & \text{if } i = \omega(b) \\ 0 & \text{otherwise} \end{matrix}\right\}$ and

  $\omega(b) = \min\{j \leq n \mid \forall k.\ b_k \leq b_j\}$ is the auction winner

Modeling auctions as games

Explanations

- Only i knows v_i.
- In sealed bid auctions, only i and the auctioneer know b_i.
- The auctioneer calculates
  - the winning price $p(b)$
  - the auction winner $\omega(b)$

  and tells the price to the winner.

Modeling auctions as games

Remarks

- The auction implementation problems
  - winner's commitment to pay
  - auctioneer's integrity in calculations

are beyond the scope of this analysis.

Modeling auctions as games

Remarks

- The auction implementation problems
  - winner's commitment to pay
  - auctioneer's integrity in calculations

  are beyond the scope of this analysis.

- The bidders do not know each other's utility.
  - The notion of Nash equilibrium is therefore dubious.
  - It does apply because of special circumstances.

Modeling auctions as games

Assumption

Without loss of generality, we assume that the bid vector $b = \langle b_1, b_2, \ldots, b_n \rangle$ is arranged in descending order

$$b_1 \geq b_2 \geq b_3 \geq \cdots \geq b_n$$

Modeling auctions as games

Assumption

Without loss of generality, we assume that the bid vector $b = \langle b_1, b_2, \ldots, b_n \rangle$ is arranged in descending order

$$b_1 \geq b_2 \geq b_3 \geq \cdots \geq b_n$$

Since only one bidder wins, and the priority of equal bidders is resolved lexicographically, nothing is lost if the equal bidders are ignored, so we assume that the bid vector is strictly descending

$$b_1 > b_2 > b_3 > \cdots > b_n$$

Modeling auctions as games

Definition

The winning price is

- in the first price auction:

$$p_1(b) = b_1$$

- in the second price auction:

$$p_2(b) = b_2$$

Rational bidding in second price auctions

Proposition

The truthful bidding

$$\overline{b}_i = v_i$$

is the dominant strategy for the second price sealed bid auctions.

Rational bidding in second price auctions

Proof

Bidders' payoffs are

$$u_i(\overline{b}) = \begin{cases} v_1 - v_2 & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}$$

The claim is that for all $b \in \mathbb{R}^n$ holds

$$u_i(\overline{b}) \geq u_i(b)$$

Rational bidding in second price auctions

Proof.

- If $b_i > \overline{b}_i = v_i$ then
  - if $i = 1$, then the outcome is unchanged
  - if $i > 1$, then
    - either $b_i > b_1 \geq \overline{b}_i = v_i$, and the bidder i wins the auction with the utility $u_i(b) = v_i - b_1 \leq 0$
    - or $b_i \leq b_1$, and the outcome remains unchanged.
- If $b_i < \overline{b}_i = v_i$ then
  - if $i > 1$, then the outcome is unchanged
  - if $i = 1$, then
    - either $b_1 < b_2 \leq \overline{b}_1 = v_1$, and the bidder 2 wins the auction, so that 1's utility is at most 0,
    - or $b_i \geq b_2$, and the outcome remains unchanged.

Rational bidding in first price auctions

Proposition

In a first price sealed bid auction

- with n players,
- with the valuations v_i uniformly distributed in an interval $[0, x]$

the Nash equilibrium consists of the bids

$$\overline{b}_i \quad = \quad \beta(v_i) \quad = \quad \frac{n-1}{n} \cdot v_i$$

where $\beta : \mathbb{R} \to \mathbb{R}$ denotes the equilibrium strategy used by all players.

Rational bidding in first price auctions

Proof

- Without loss of generality, divide all valuations by x.
  - v_i are uniformly distributed in $[0, 1]$.

Rational bidding in first price auctions

Proof

- Without loss of generality, divide all valuations by x.
  - v_i are uniformly distributed in $[0,1]$.
- In the mean, the utilities u_i can be approximated

$$\tau_i(b) \cdot \left(v_i - b_1\right) \quad \approx \quad v_i^{n-1} \cdot \left(v_i - \beta(v_i)\right)$$

  - $\beta(v_i)$ should give i the probability v_i to win against any other bidder
  - hence the probability v_i^{n-1} that the player i will win against $n-1$ other bidders

Rational bidding in first price auctions

Proof

- Suppose the bidders are in equilibrium, i.e. all play $\overline{b}_i = \beta(v_i)$.

Rational bidding in first price auctions

Proof

- Suppose the bidders are in equilibrium, i.e. all play $\overline{b}_i = \beta(v_i)$.
- i's attempt to deviate from the equilibrium can be viewed as supplying a valuation $\widetilde{v} \neq v_i$ and playing $b_i = \beta(\widetilde{v})$.

Rational bidding in first price auctions

Proof

- Suppose the bidders are in equilibrium, i.e. all play $\overline{b}_i = \beta(v_i)$.
- i's attempt to deviate from the equilibrium can be viewed as supplying a valuation $\widetilde{v} \neq v_i$ and playing $b_i = \beta(\widetilde{v})$.
- The statement that $\overline{b}_i = \beta(v_i)$ gives an equilibrium means that for all $\widetilde{v}$ holds

$$v_i^{n-1} \cdot \big(v_i - \beta(v_i)\big) \quad \geq \quad \widetilde{v}^{n-1} \cdot \big(v_i - \beta(\widetilde{v})\big)$$

Rational bidding in first price auctions

Proof

- A maximum of the function

$$\upsilon_i(v) \quad = \quad v^{n-1} \cdot \big(v_i - \beta(v)\big)$$

must thus be reached for $\widehat{v} = v_i$.

Rational bidding in first price auctions

Proof

- A maximum of the function

$$\upsilon_i(v) \quad = \quad v^{n-1} \cdot \big(v_i - \beta(v)\big)$$

must thus be reached for $\widehat{v} = v_i$.

- In other words, $\frac{d\upsilon}{dv}(v_i) = 0$ must hold for

$$\frac{d\upsilon}{dv} \quad = \quad (n-1)v^{n-2}\big(v_i - \beta\big) - v^{n-1}\frac{d\beta}{dv}$$

Rational bidding in first price auctions

Proof.

- Hence

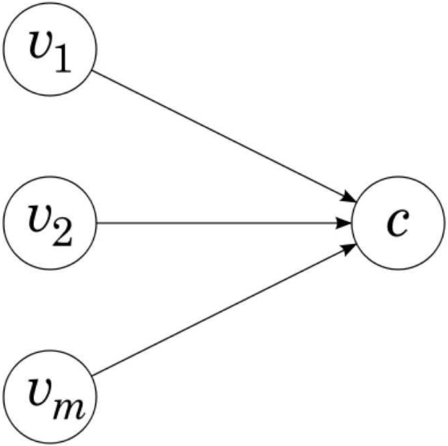
$$\frac{d\beta}{dv}(v_i) = (n-1)\left(1 - \frac{\beta(v_i)}{v_i}\right)$$

- Since this must hold for any v_i, we solve the differential equation, and get

$$\beta(v_i) = \frac{n-1}{n} \cdot v_i$$

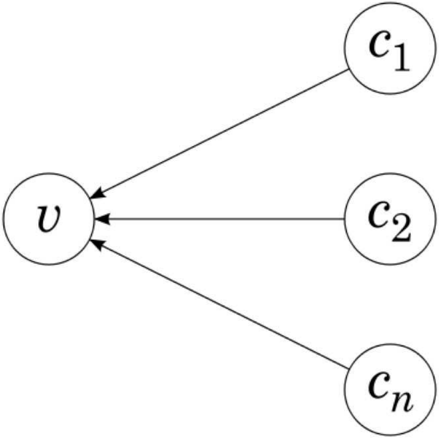
□

Summary



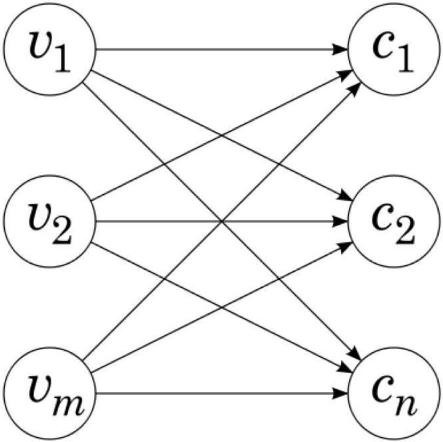
So much about single-item supply auctions

Summary



Single-user demand auctions are somewhat similar.

Sequel



Market also gives rise to another kind of problems.

Outline

Introduction

Auctions

Matching demand and supply

Yes/no-utility

Valuations

Market clearing problem

Summary

Market problem

Task

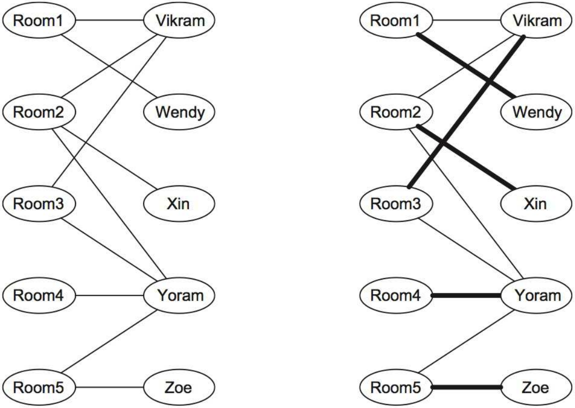
Provide the highest quality goods to the most interested buyers.

Matching problem

Task

Match users and the items to maximize utility.

Matching problem: yes/no-utility



Assign 5 students in 5 dorm rooms.

Matching problem: yes/no-utility

Bipartite graphs

A bipartite graph is a graphic view of

- a binary relation
- a 0/1-matrix

capturing the yes/no-utilities of a given set of users for a given set of items.

Matching problem: yes/no-utility

Definition

Perfect matching is a one-to-one assignment between the users and the items, such that each user is assigned one of the desired items.

Matching problem: yes/no-utility

Definition

Perfect matching is a bijection between the users and the items contained in their yes/no-utility relation.

Matching problem: yes/no-utility

Task

- Find a perfect matching and we are done.

Matching problem: yes/no-utility

Task

- Find a perfect matching and we are done.

Question

- Does every yes/no-utility allow perfect matching?
- Does every binary relation contain a bijection?

Matching problem: yes/no-utility

Question

- Can any set of users be satisfied with any set of items?

Constricted utilities

Answer

NO

Constricted utilities

Answer

NO, e.g. if

- all users only want the same item

Constricted utilities

Answer

NO, e.g. if

- all users only want the same item
- some of the users do not accept any of the items

Constricted utilities

Answer

NO, e.g. if

- all users only want the same item
- some of the users do not accept any of the items
- there is a set of n users who only accept $m < n$ items

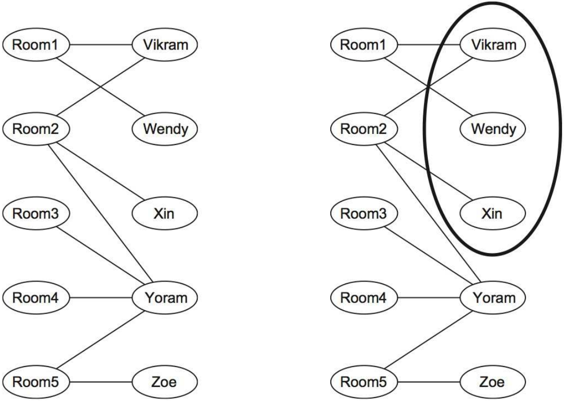
Constricted utilities

Answer

NO, e.g. if

- all users only want the same item
- some of the users do not accept any of the items
- there is a set of n users who only accept $m < n$ items
- there is a set of n items accepted by $m < n$ users

Constricted sets



Constricted sets

Definition

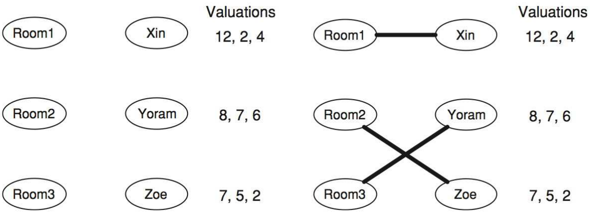
A *constricted set of users* is a set of n users who only accept $m < n$ items.

Matching Theorem

Theorem 1 (König)

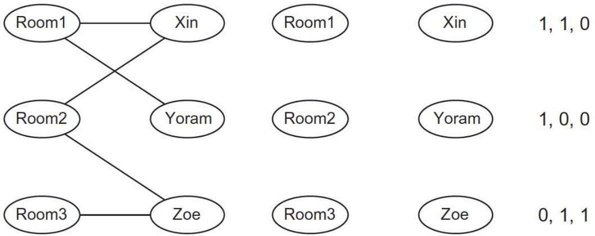
A yes/no-utility allows perfect matching if and only if it does not contain a constricted set of users.

Matching problem: Valuations



Valuations quantify preferences, and matchings

Matching problem: Valuations



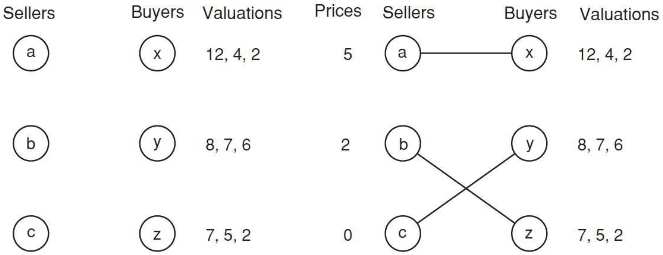
The yes/no-utilities are a special case of valuations

Market is different

Market does not match

- users (with valuations) and items (passive), but
- buyers (with valuations) and sellers (pricing items).

Market relations: Preferred seller



Buyer B seeks seller S so that $u_B^S = v_{BS} - p_S$ is maximal.

Market relations: Preferred seller

Each buyer may have multiple preferred sellers.

Market clearing

Definition

A *(toy) market* consists of

- a set of buyers, and
- a set of sellers,

and moreover

- each seller determines a price for a single item,
- each buyer determines a valuation for each of the items.

Market clearing

Definition

Buyer B's utility for the item of the seller S is

$$u_B^S = v_{BS} - p_S$$

Market clearing

Definition

Buyer B's utility for the item of the seller S is

$$u_B^S = v_{BS} - p_S$$

The set of preferred sellers for the buyer B is

$$\mathrm{Prs}_B = \left\{ \overline{S} \mid \forall S.\ u_B^S \leq u_B^{\overline{S}} \right\}$$

Market clearing

Definition

Let the preferred seller relation for a given market be presented by a bipartite graph obtained by connecting each buyer with her preferred sellers.

We say that the market is *cleared* by a perfect matching contained in this bipartite graph.

Market clearing

Definition

Let the preferred seller relation for a given market be presented by a bipartite graph obtained by connecting each buyer with her preferred sellers.

We say that the market is *cleared* by a perfect matching contained in this bipartite graph.

The *market clearing prices* are the prices paid to the sellers when the market is cleared.

Market Clearing Theorem

Theorem 2

For any matrix of buyers' valuations, there is a vector of market clearing prices.

Market clearing optimality

Definition

For any perfect matching that clears a market,

- the *total valuation* is the sum of all buyers' valuations for the items that they get, and
- the *total payoff* is the sum of all buyers' utilities for the items that they get.

Market clearing optimality

Theorem 3

For any matrix of buyers' valuations, there may be several market clearing vectors, but each of them achieves the maximal total valuation.

Market clearing optimality

Exercise

Prove Theorem 3.

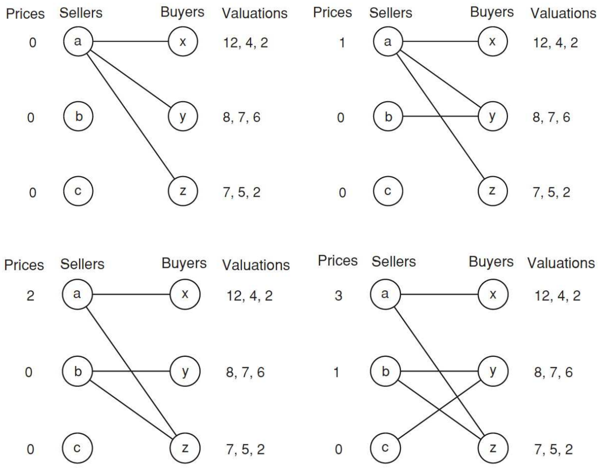
Market clearing prices

Sketch of the proof of Theorem 2

1. Initialize all prices to 0.
2. Build the graph of preferred sellers.
3. If there is a perfect matching, clear the market and exit.
4. Else find a minimal constricted set (using Theorem 1).
    - Increase all constricted prices.
    - Go to 2.

Market clearing prices

Does this have to terminate? Example:



Market clearing prices

Remark

Single-item auctions as a special case of market clearing:

Summary

- Market protocols maximize the total utility through exchange of goods

Summary

- **Auctions** are the exchange protocols organized by the seller, or by the buyer
- The goal of auctions is to maximize auctioneer's revenue by eliciting true valuations from the bidders

Summary

- **Matching** algorithms aggregate individual preferences to maximize social benefit
- An honest market maker can maximize social benefit by clearing the market through perfect matching

Path ahead

Lecture 5: A closer look at markets-as-auctions

- In auctions, the market maker is a seller (or a buyer).
- Nevertheless, social benefit is maximized
  - the bidders follow their own utilities
  - if the auction is not *compatible with bidders' incentives*, then it yields no revenue
- What if the auctioneer sells (or buys) multiple items?
- What if the market maker is neither the seller nor the buyer?

Path ahead

Lectures 6–7: Problems of matching

- Interdependencies of valuations
  - values of goods may change through their market reception
  - positive or negative externalities
  - network effects
- Information asymmetries
  - distributed matching depends on the available information
  - market of information
  - advertising
  - differential pricing, tracking, predictive analytics