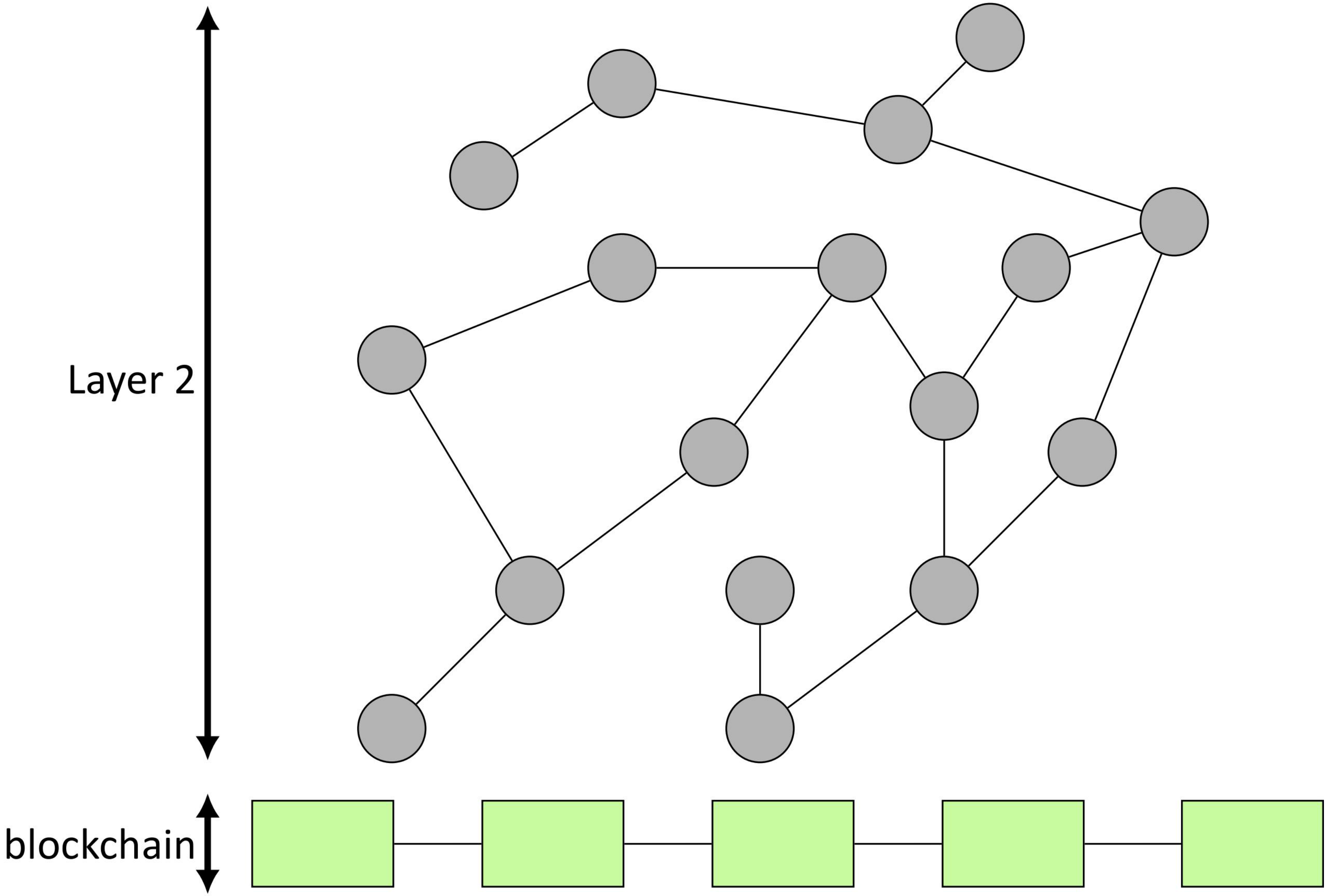
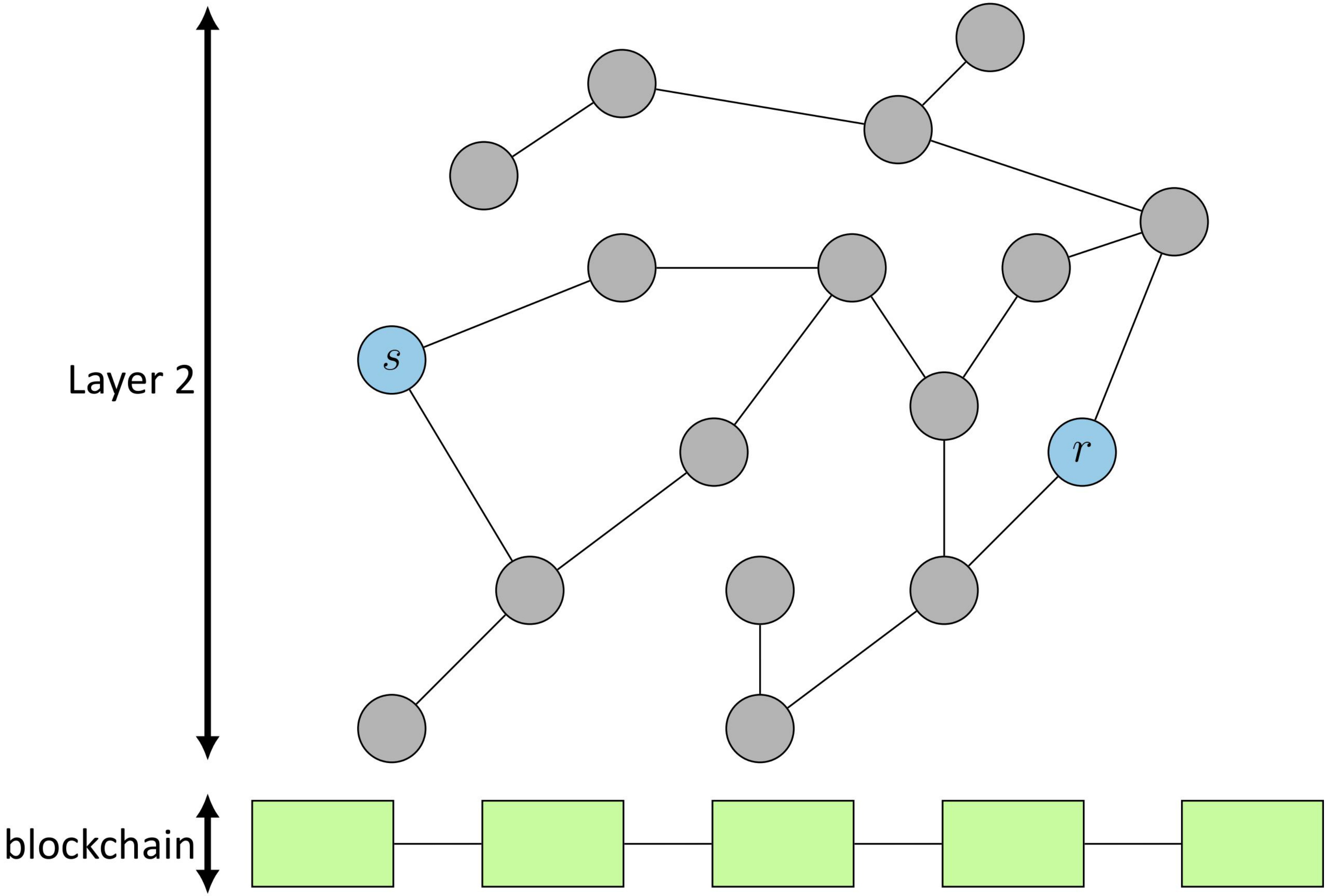
Ride the Lightning:
The Game Theory of Payment Channels

Zeta Avarikioti, Lioba Heimbach, Yuyi Wang, Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

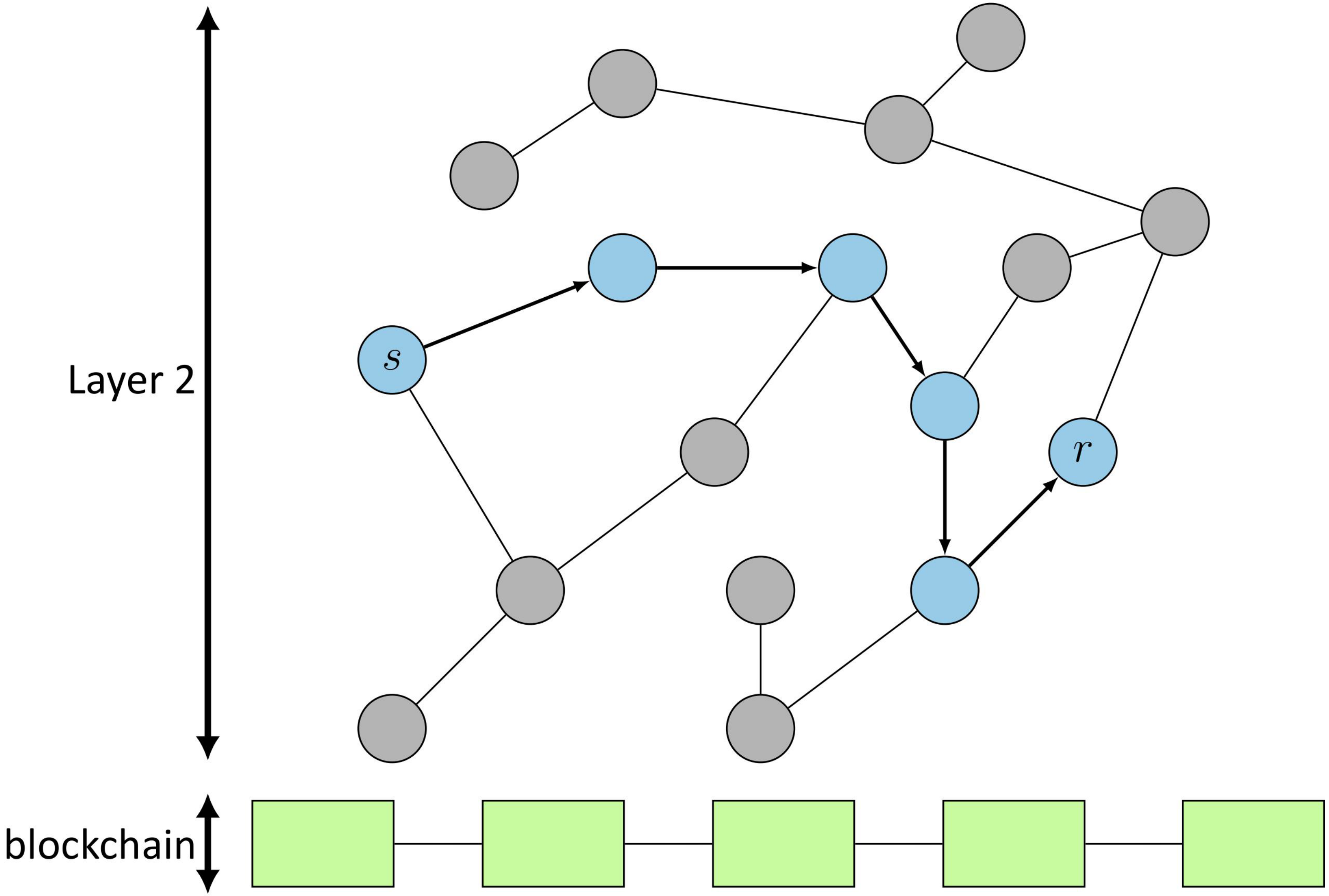
Payment channels



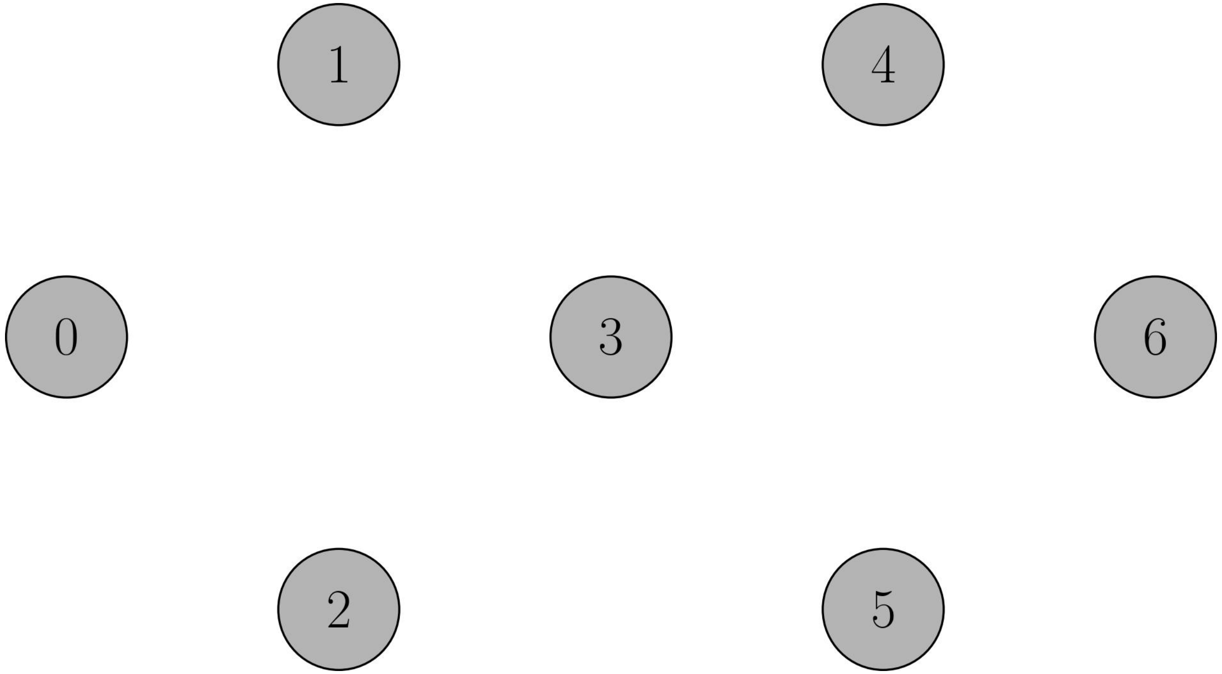
Off-chain transaction between neighbors



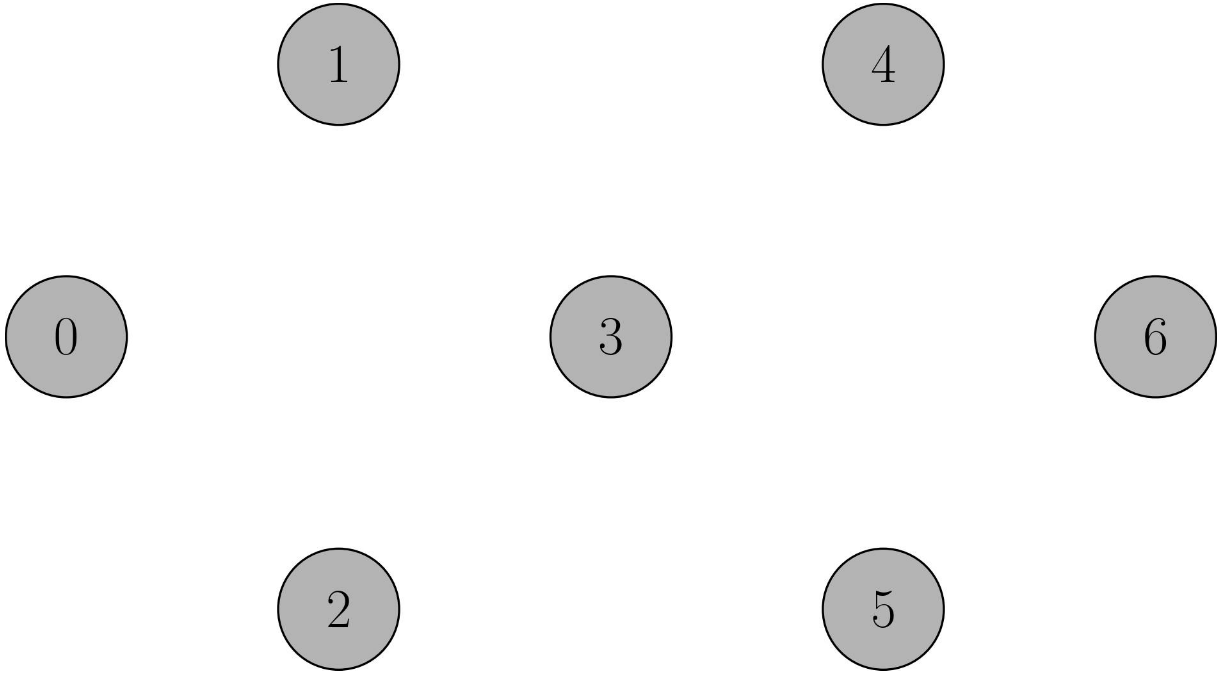
Off-chain transaction between neighbors



Network creation game

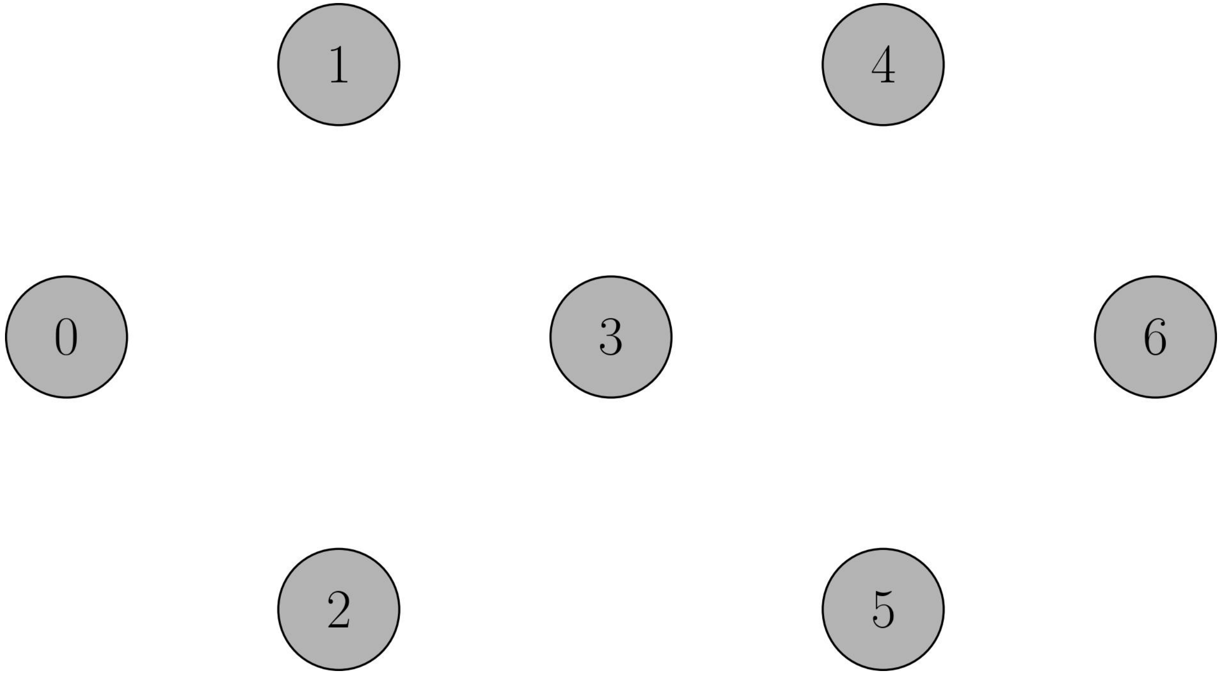


Network creation game



$s_0 = \{3\}$
$s_1 = \{3, 4\}$
$s_2 = \{3\}$
$s_3 = \{\}$
$s_4 = \{3, 6\}$
$s_5 = \{3, 6\}$
$s_6 = \{\}$

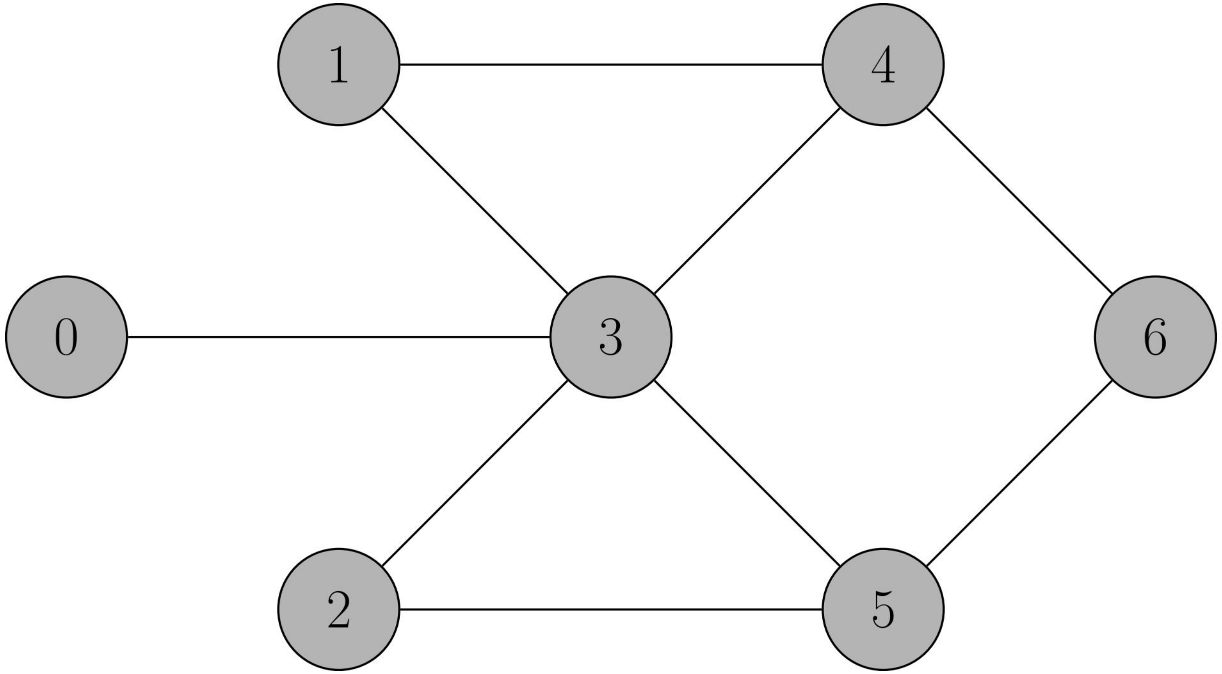
Network creation game



$s_0 = \{3\}$
$s_1 = \{3, 4\}$
$s_2 = \{3\}$
$s_3 = \{\}$
$s_4 = \{3, 6\}$
$s_5 = \{3, 6\}$
$s_6 = \{\}$

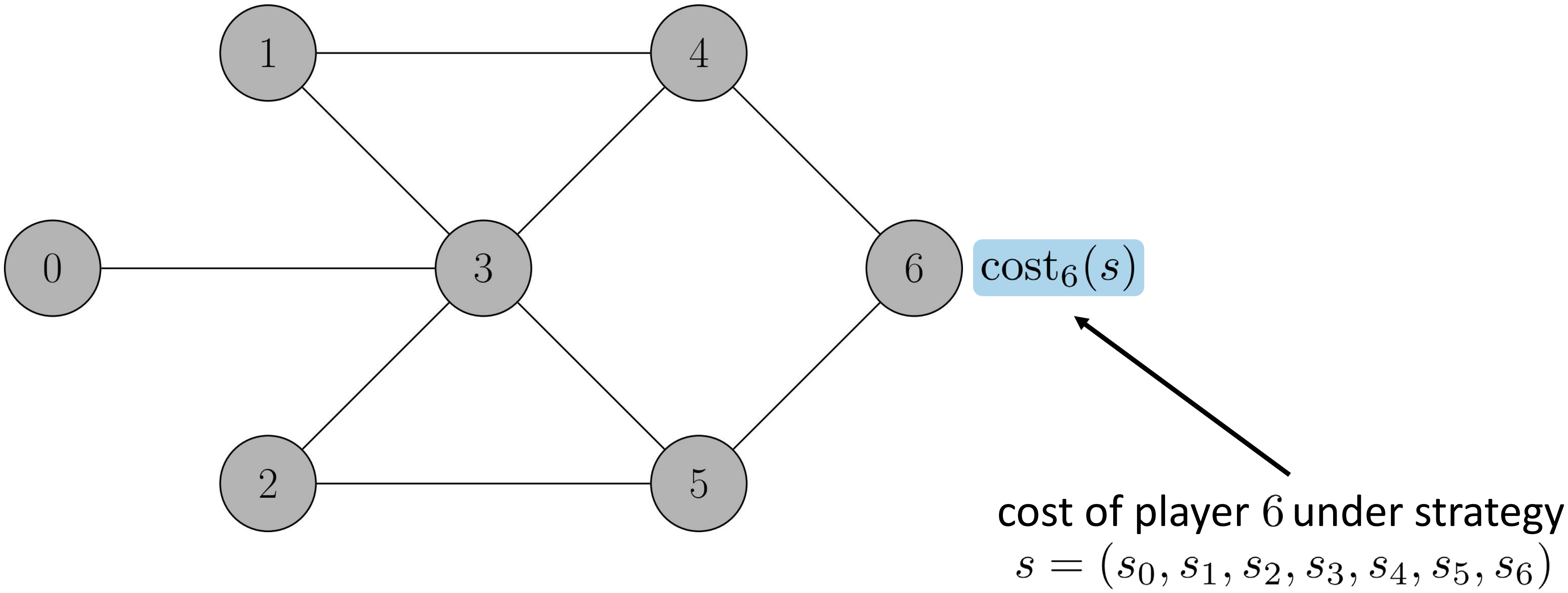
strategy of player 6

Network creation game

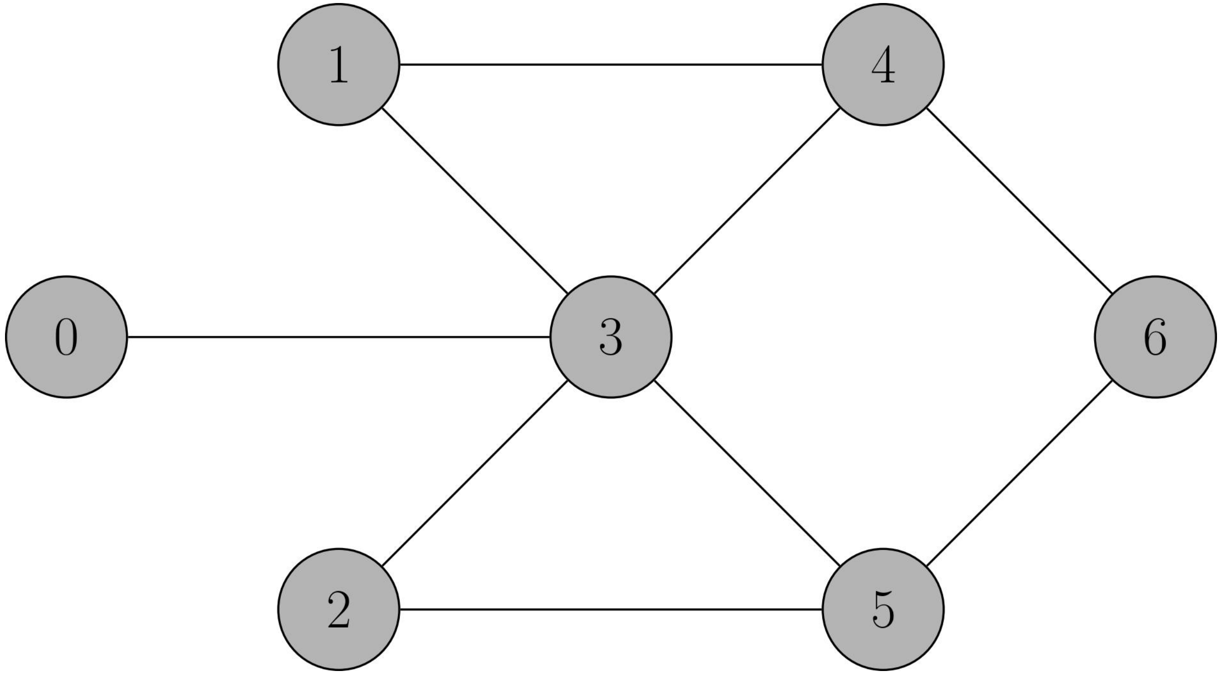


$$s_0 = \{3\}$$
$$s_1 = \{3, 4\}$$
$$s_2 = \{3\}$$
$$s_3 = \{\}$$
$$s_4 = \{3, 6\}$$
$$s_5 = \{3, 6\}$$
$$s_6 = \{\}$$

Network creation game

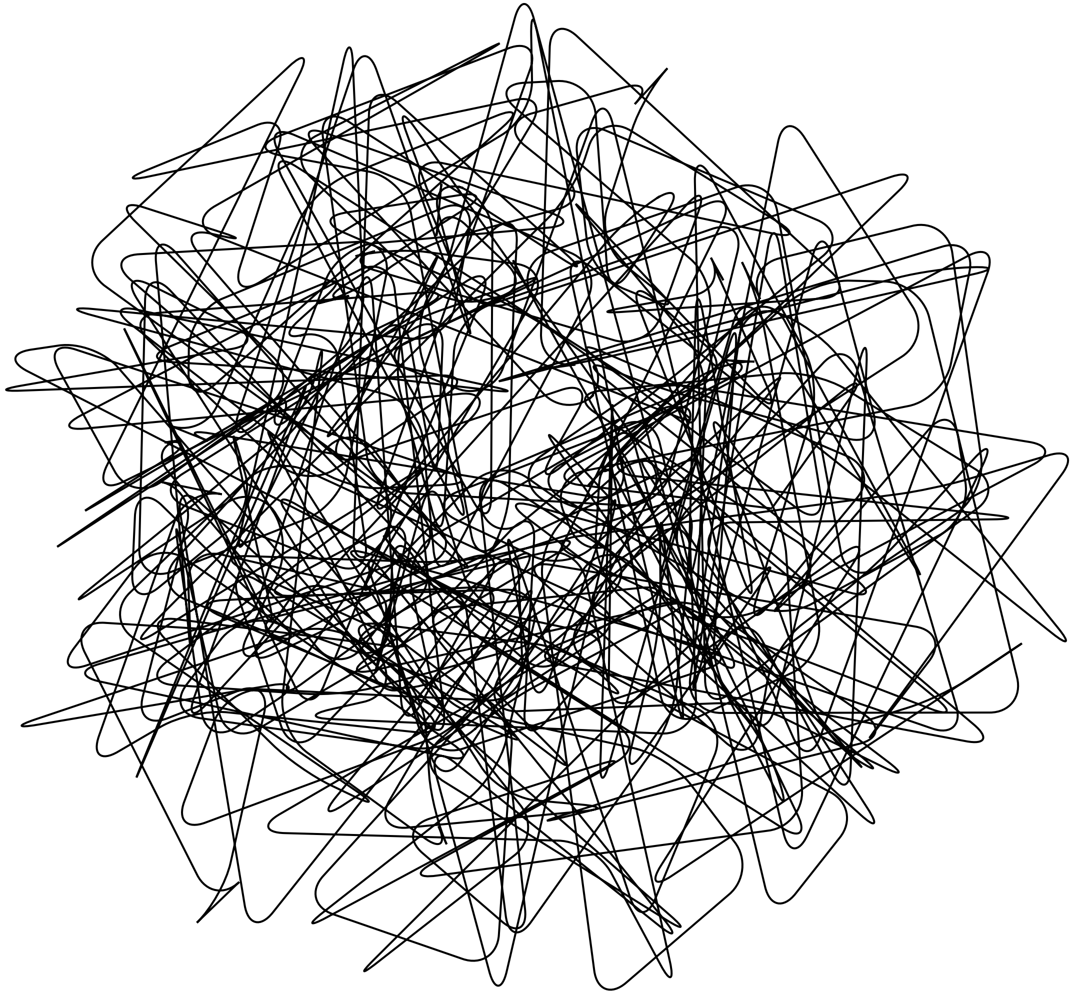


Nash equilibrium



A graph is a **Nash equilibrium** if no player can **reduce her cost** by unilaterally changing strategy.

Price of anarchy



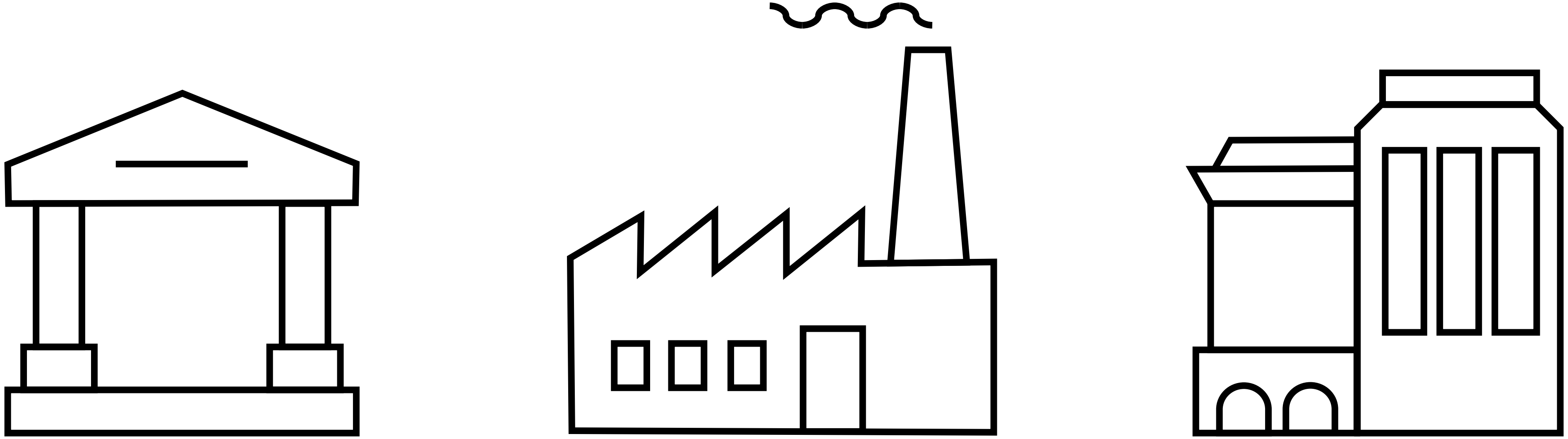
The **price of anarchy** is the ratio of the social costs of the **worst-case** Nash equilibrium and the **social optimum**.

Model

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

cost of player u
under strategy s

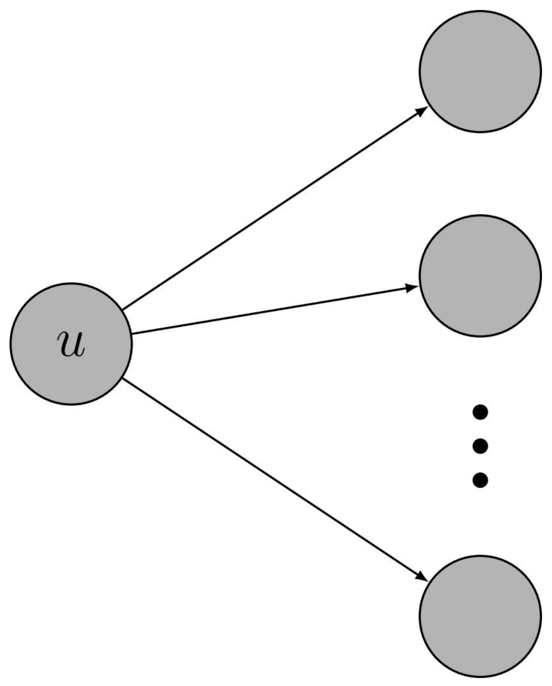
Players



Channel formation

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

number of outgoing channels of player u



Channel formation

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Assumption: capital considered unlimited.

Channel formation

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Assumption: capital considered unlimited.

Assumption: channels initiated unilaterally.

Betweenness Centrality

Reflection of the fees a node receives by forwarding the transaction of others.

Closeness Centrality

Measure of the costs encountered for making transactions in the network.

Betweenness Centrality

Closeness Centrality

Reflection of the fees a node receives by forwarding the transaction of others.

Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

betweenness weight

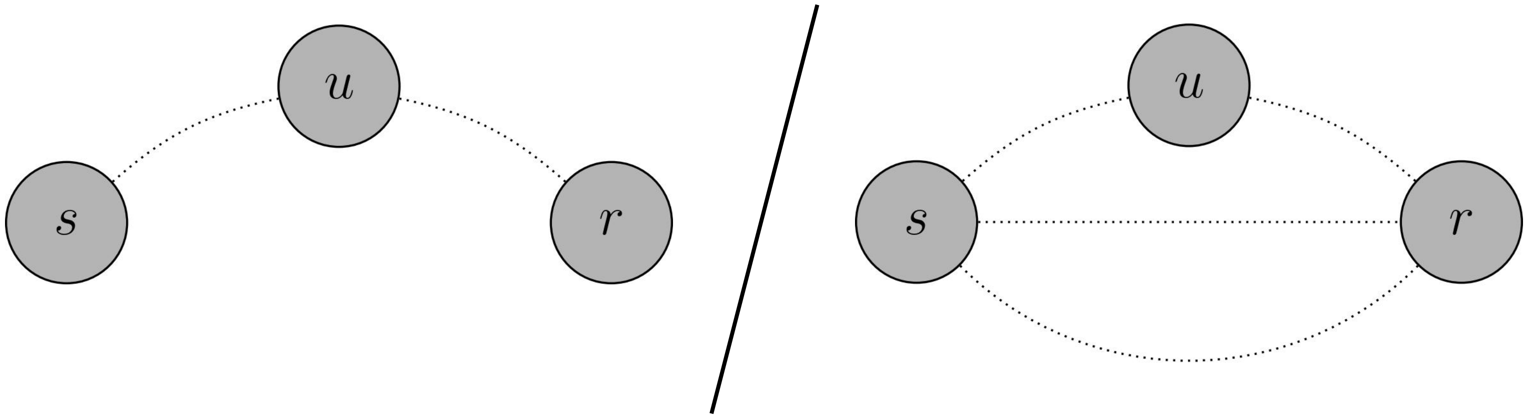
$$b \geq 0$$

Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Betweenness centrality

$$\mathrm{cost}_u(s) = |s_u| + b \cdot \mathrm{betweenness}_u(s) + c \cdot \mathrm{closeness}_u(s)$$



Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Assumption: uniform transactions.

Betweenness Centrality

Closeness Centrality

Measure of the costs encountered for making transactions in the network.

Closeness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

closeness weight

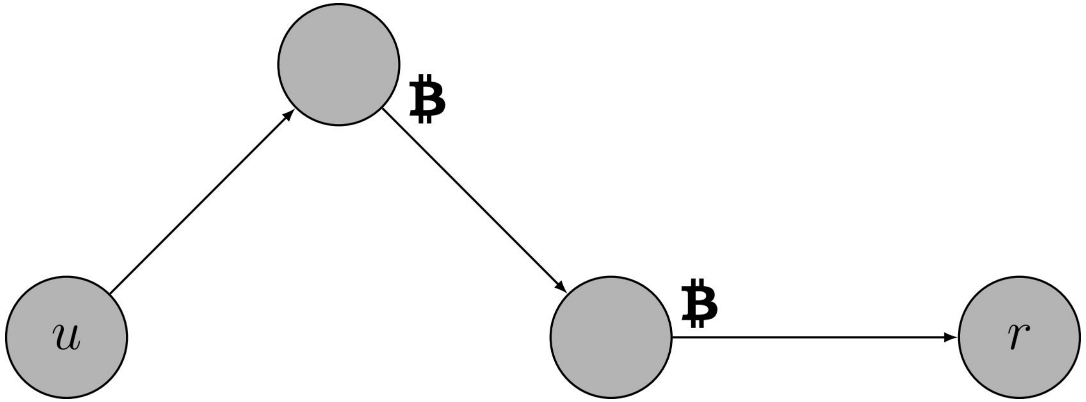
$c > 0$

Closeness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Closeness centrality

$$\mathrm{cost}_u(s) = |s_u| + b \cdot \mathrm{betweenness}_u(s) + c \cdot \mathrm{closeness}_u(s)$$



Closeness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Assumption: uniform transactions.

Closeness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

Assumption: uniform transactions.

Assumption: fixed transaction fees.

Social cost

$$\mathrm{cost}(s) = \sum_{u \in [n]} \mathrm{cost}_u(s)$$

Social optimum

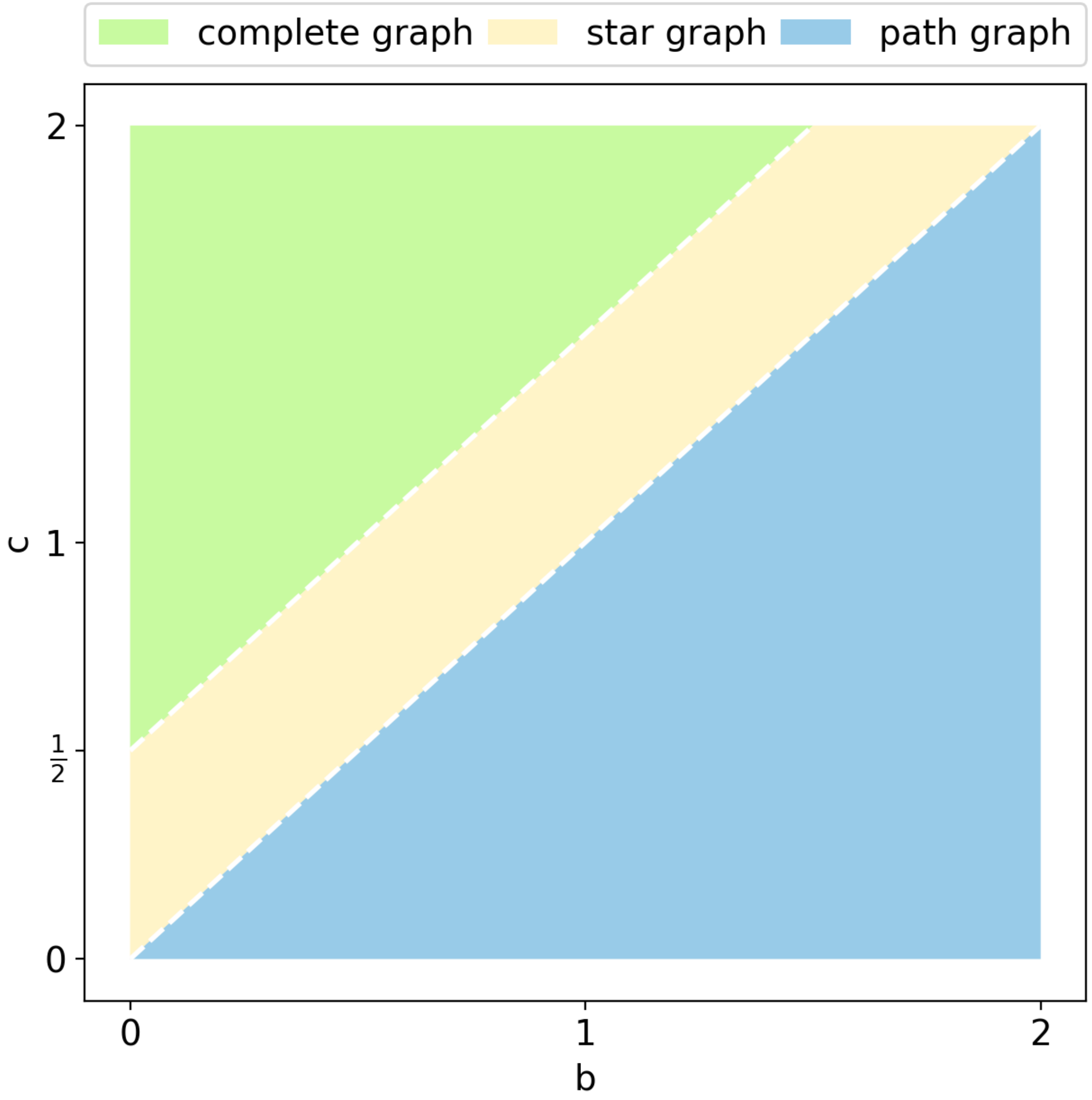
$$\mathrm{cost}(s) = \sum_{u \in [n]} \mathrm{cost}_u(s)$$

$$\min_s \mathrm{cost}(s)$$

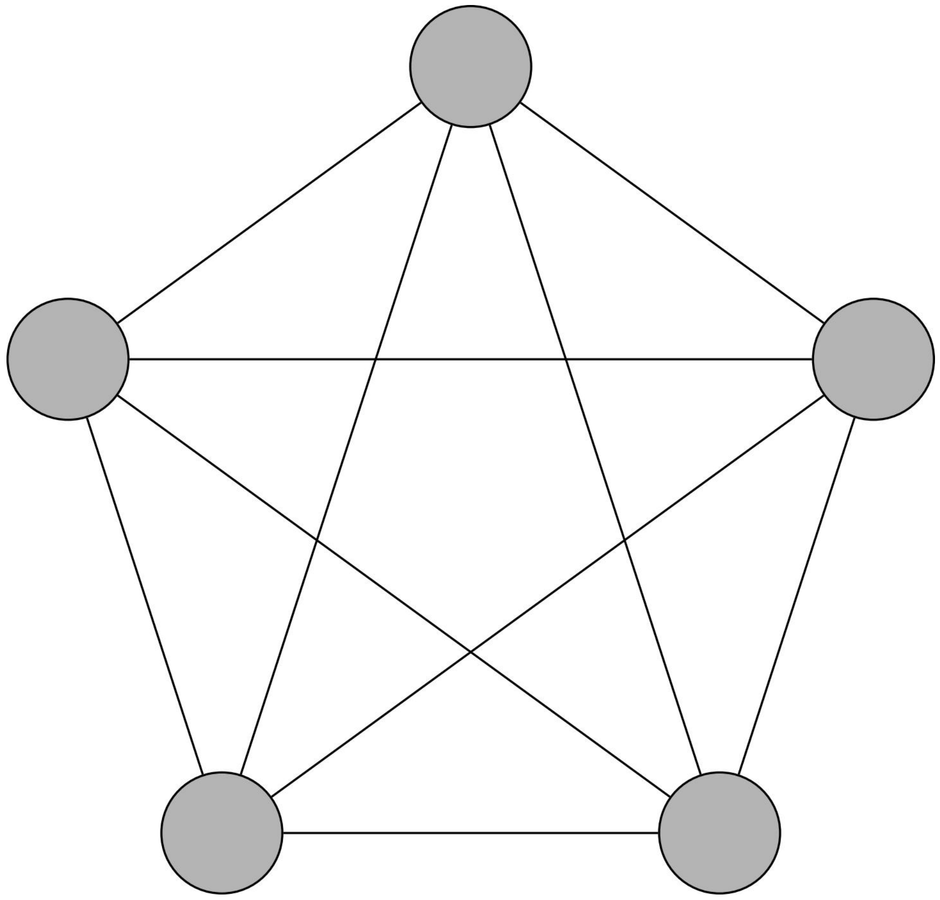
Social optimum

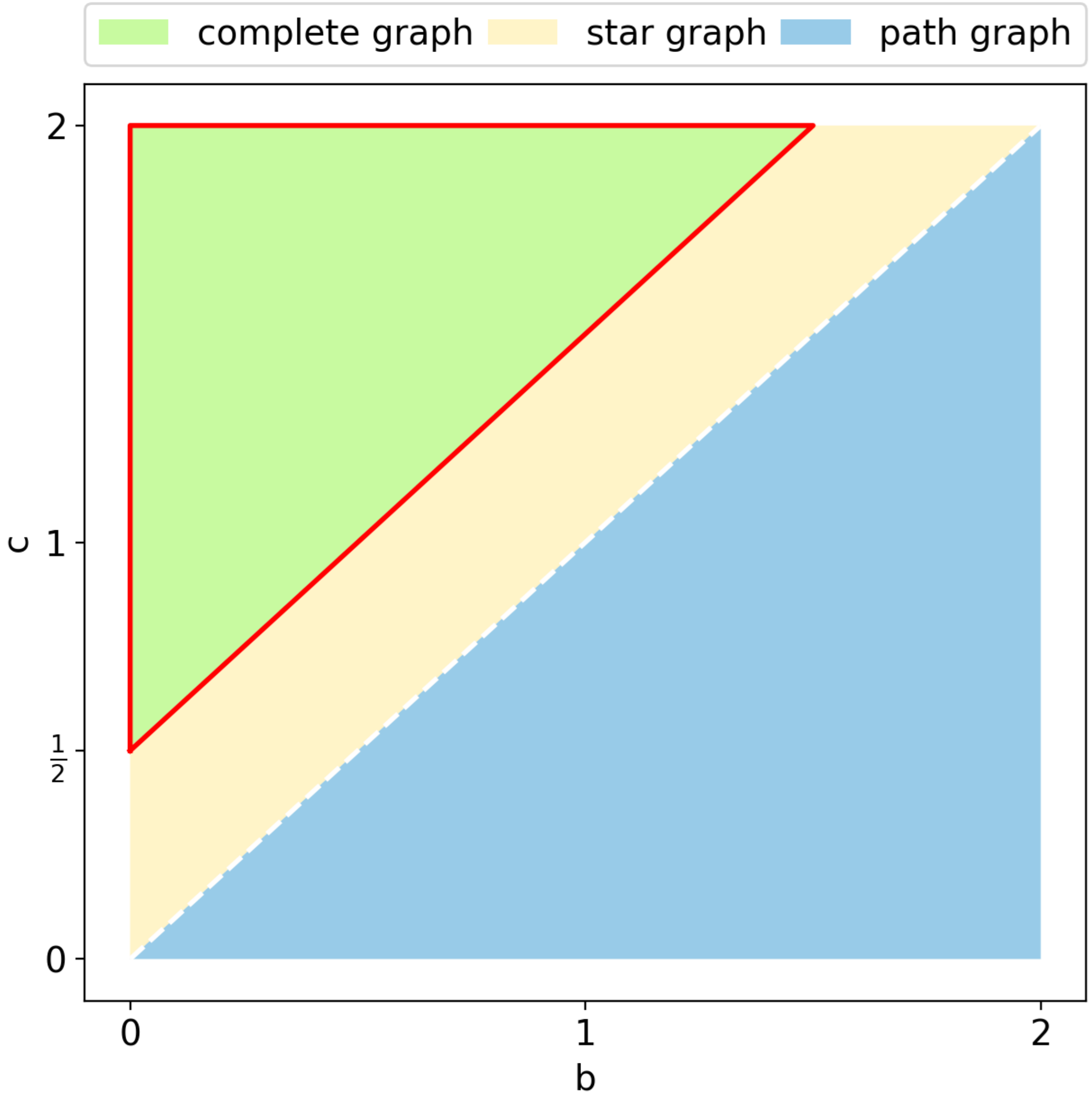
$$\mathrm{cost}(s) = \sum_{u \in [n]} \mathrm{cost}_u(s)$$

$$\min_s \mathrm{cost}(s)$$

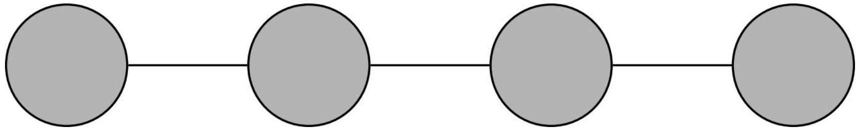


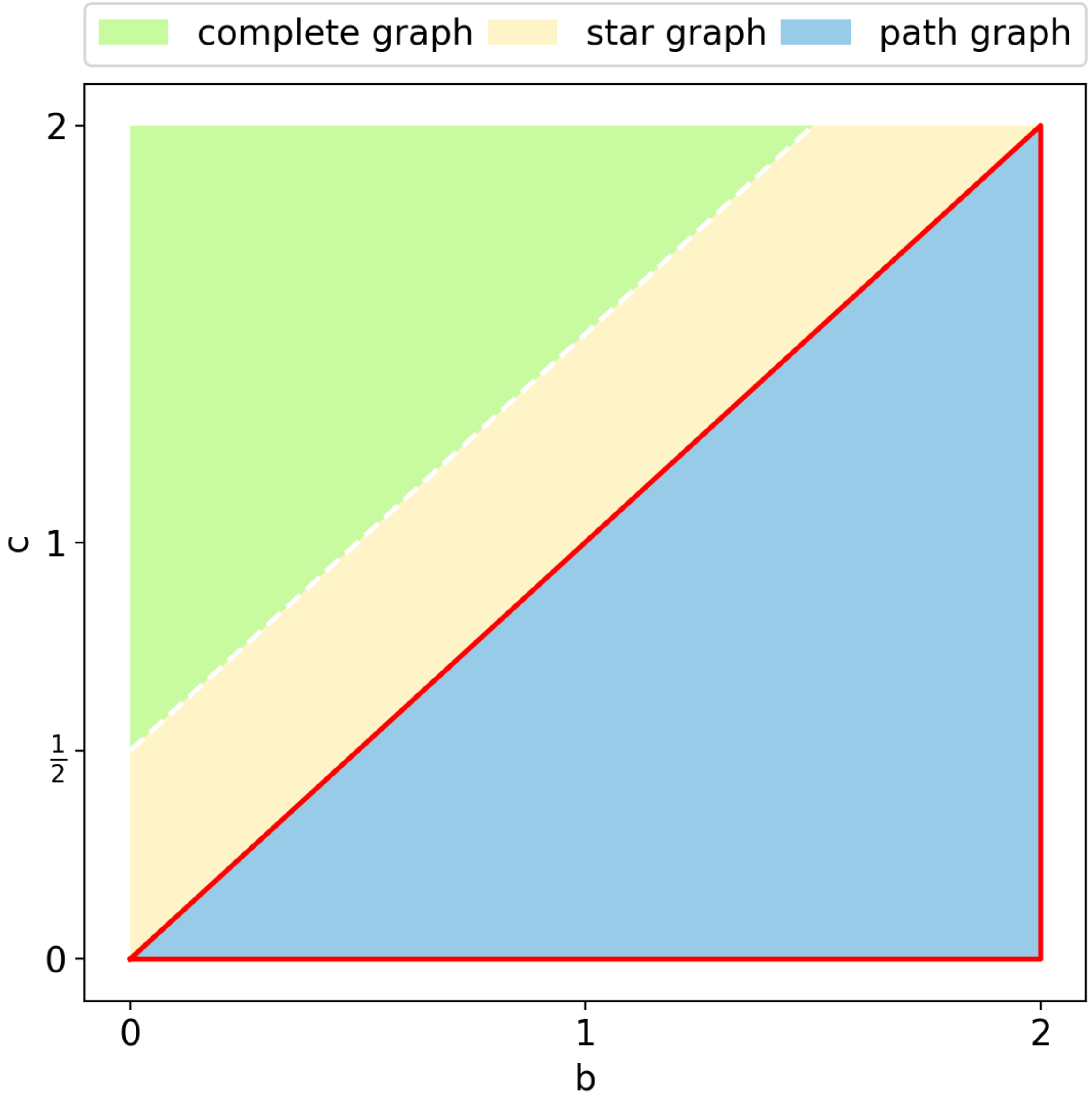
Social optimum



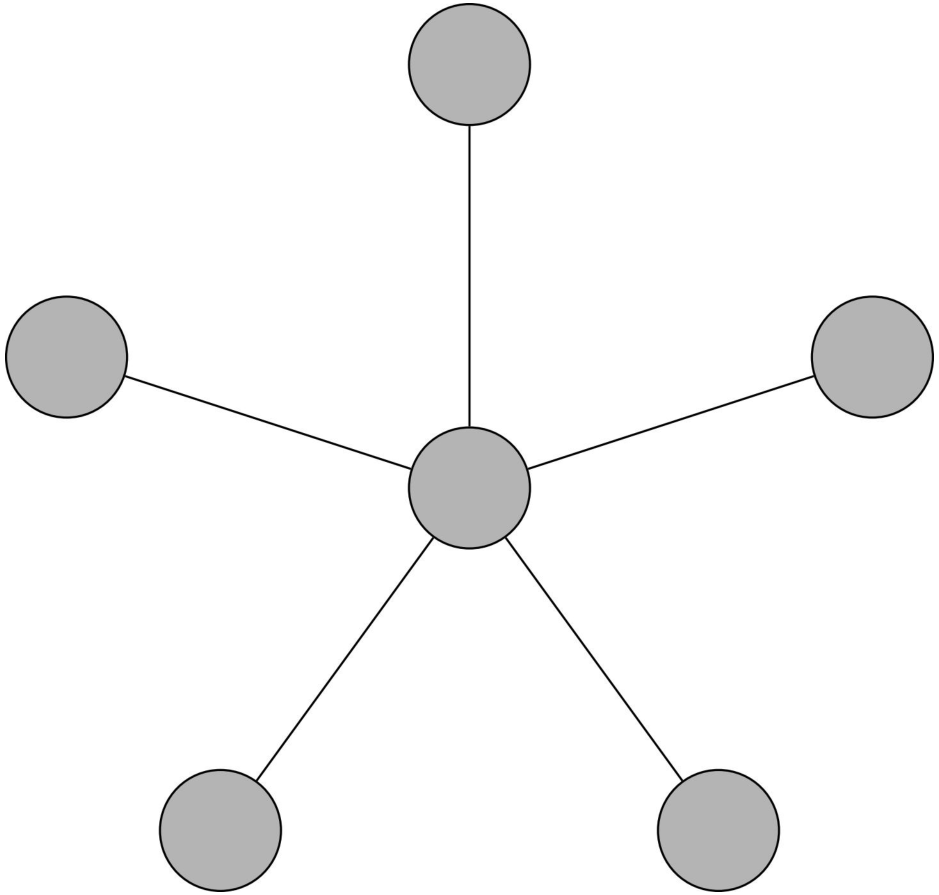


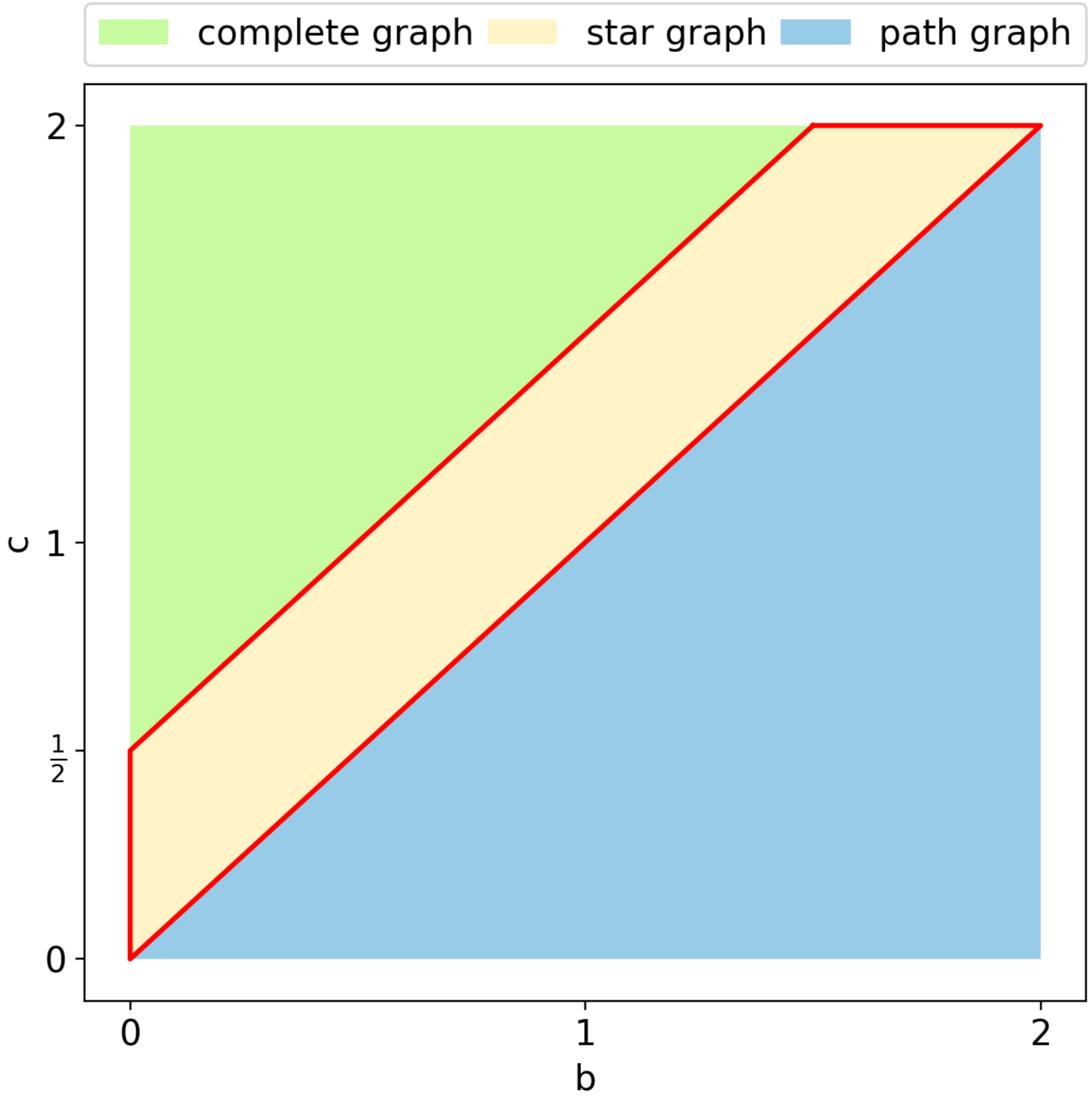
Social optimum





Social optimum

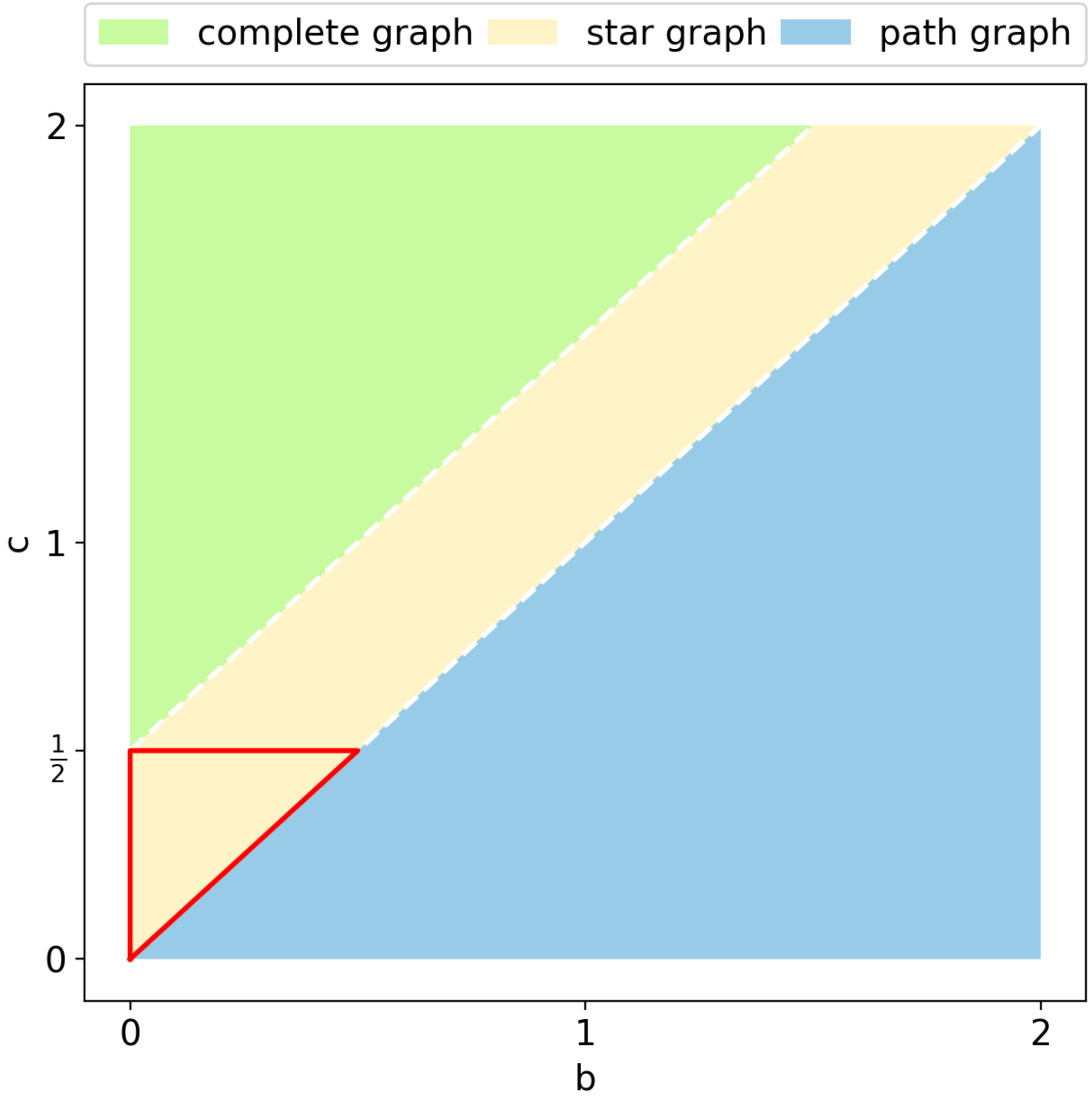




Social optimum

$$\mathrm{cost}(s) = \sum_{u \in [n]} \mathrm{cost}_u(s)$$

$$\min_s \mathrm{cost}(s)$$



Nash equilibria

Complete
Graph

Star
Graph

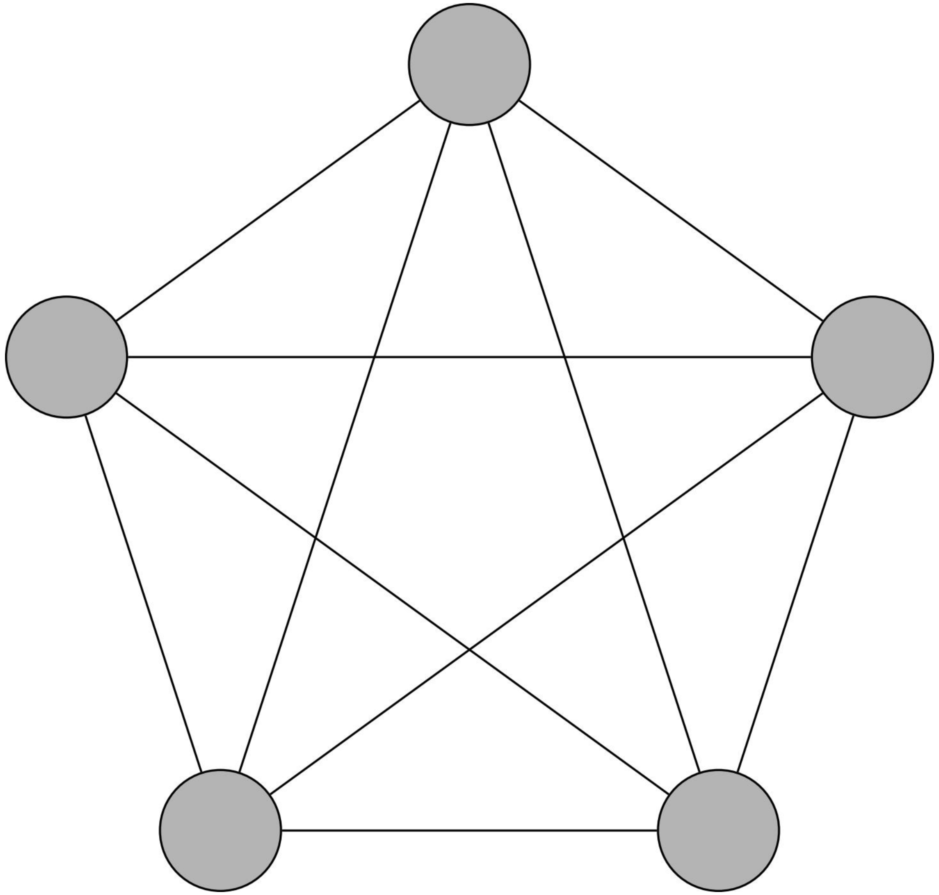
Complete
Bipartite Graph

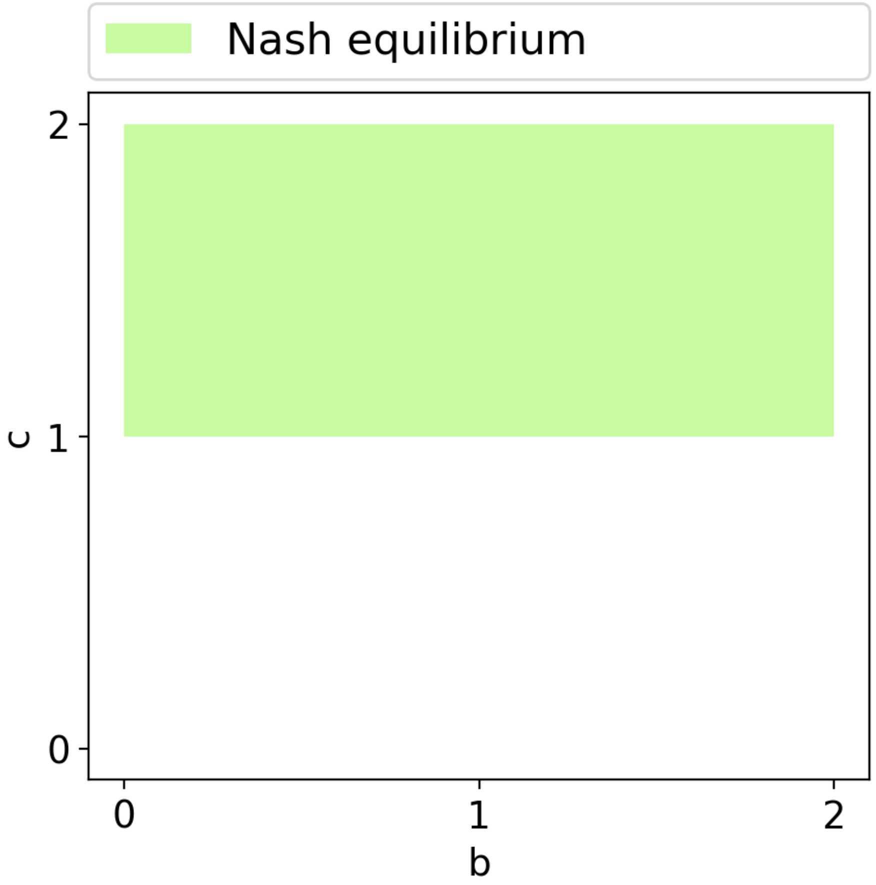
Complete
Graph

Star
Graph

Complete
Bipartite Graph

Complete graph



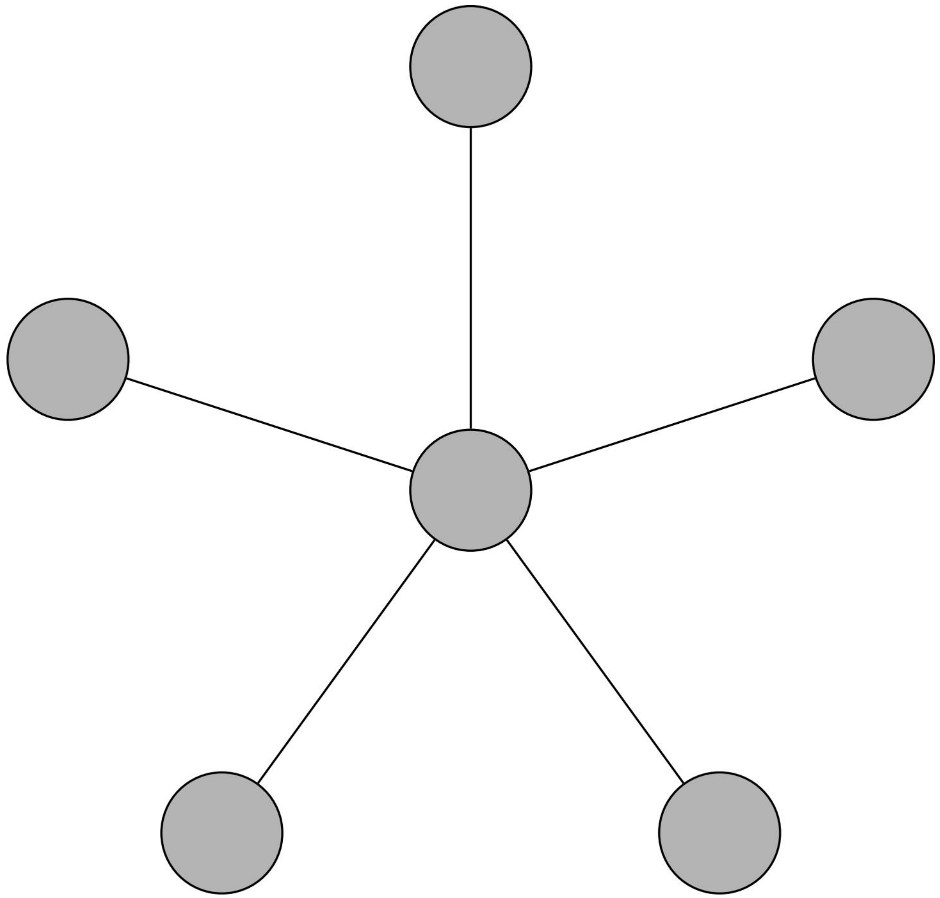


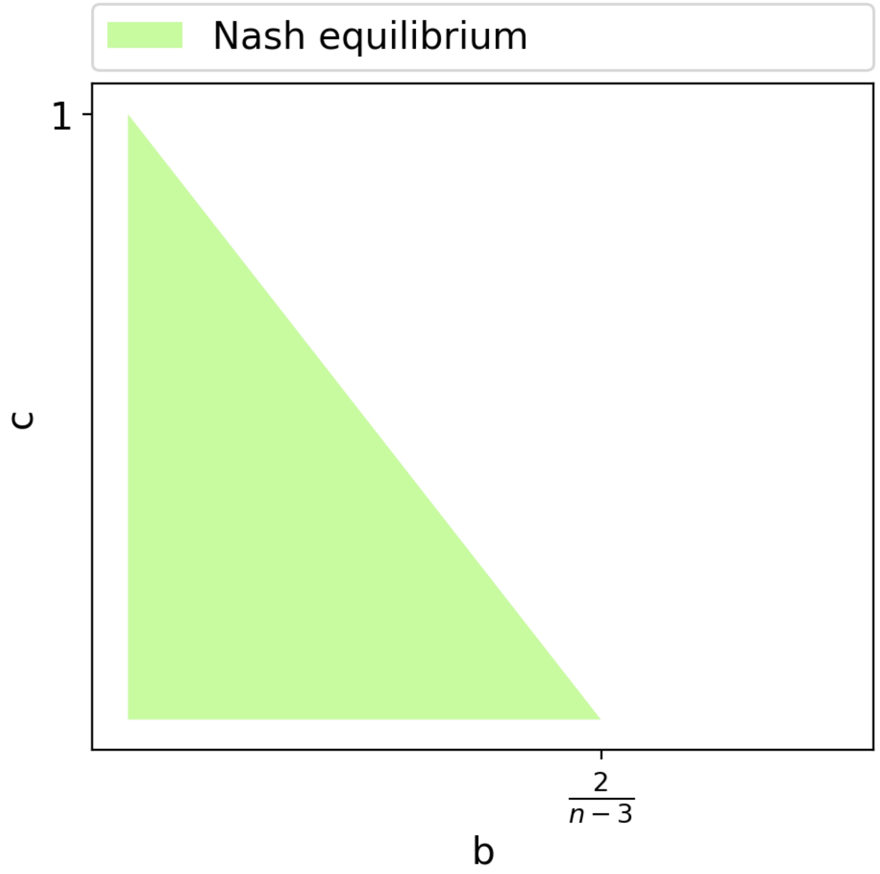
Complete
Graph

Star
Graph

Complete
Bipartite Graph

Star graph



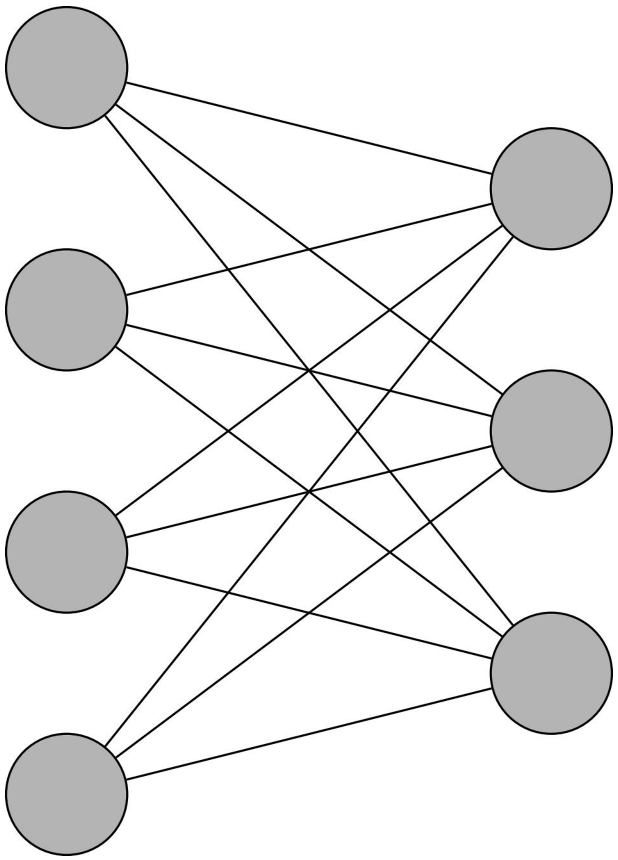


Complete
Graph

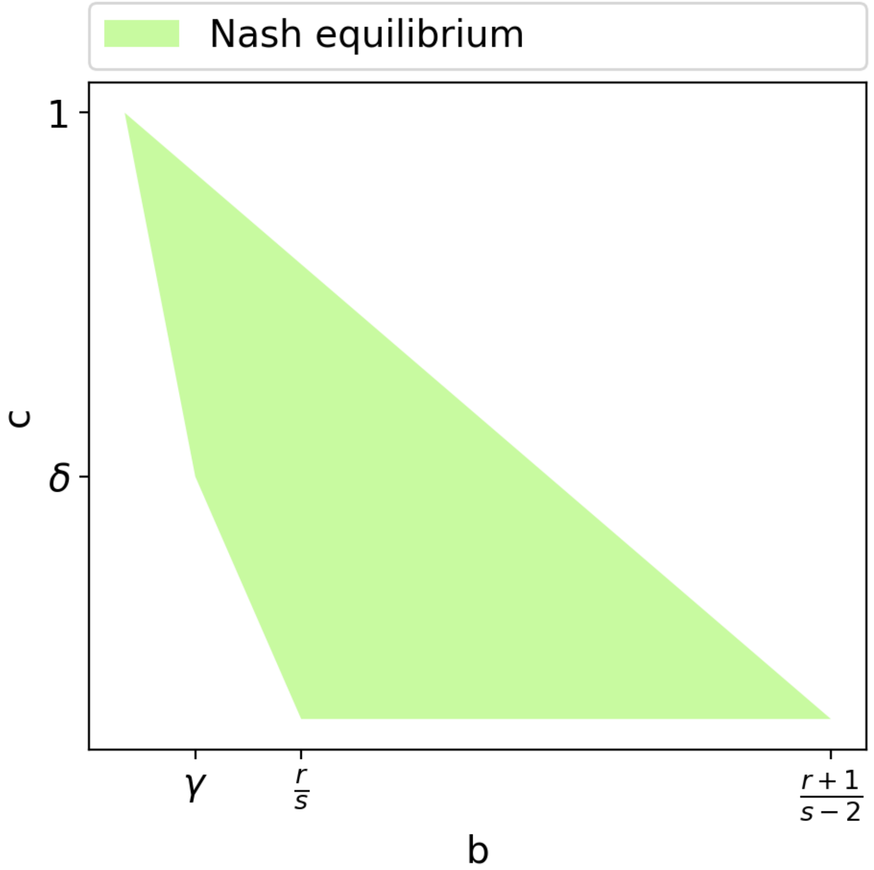
Star
Graph

Complete
Bipartite Graph

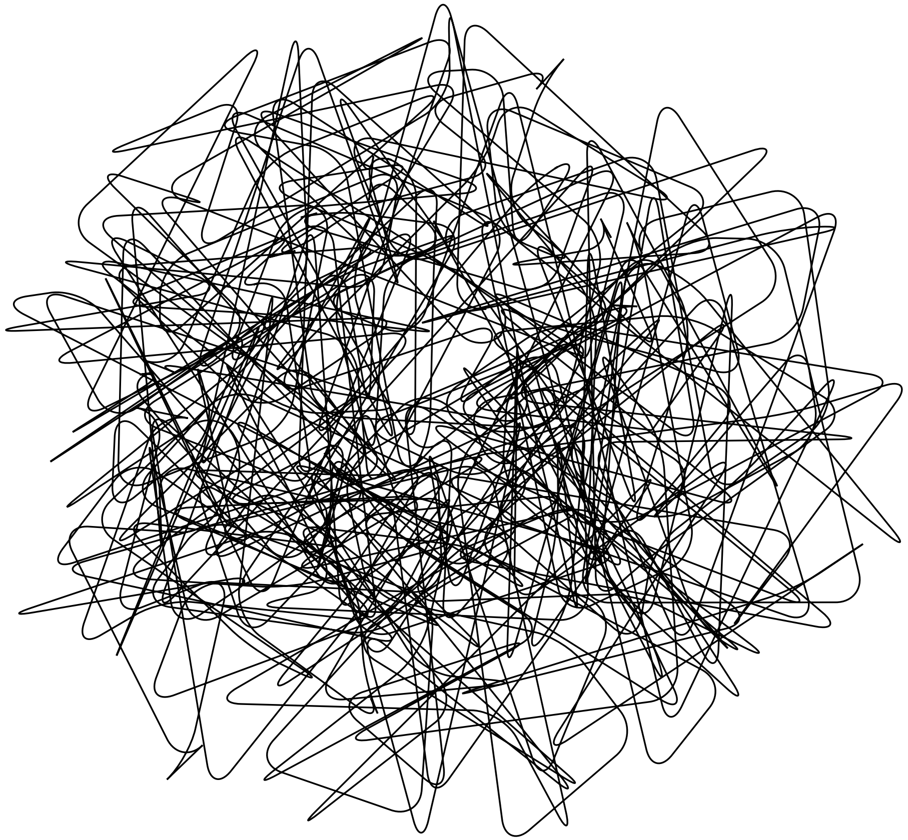
Complete bipartite graph



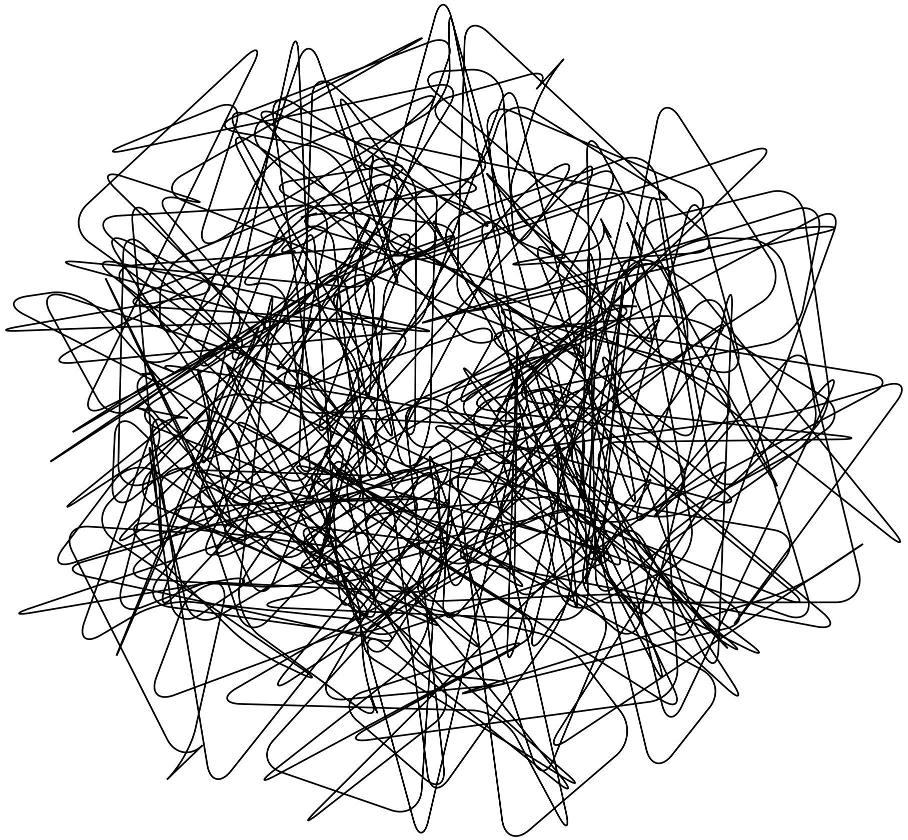
$s \geq r$ $r \geq 3$

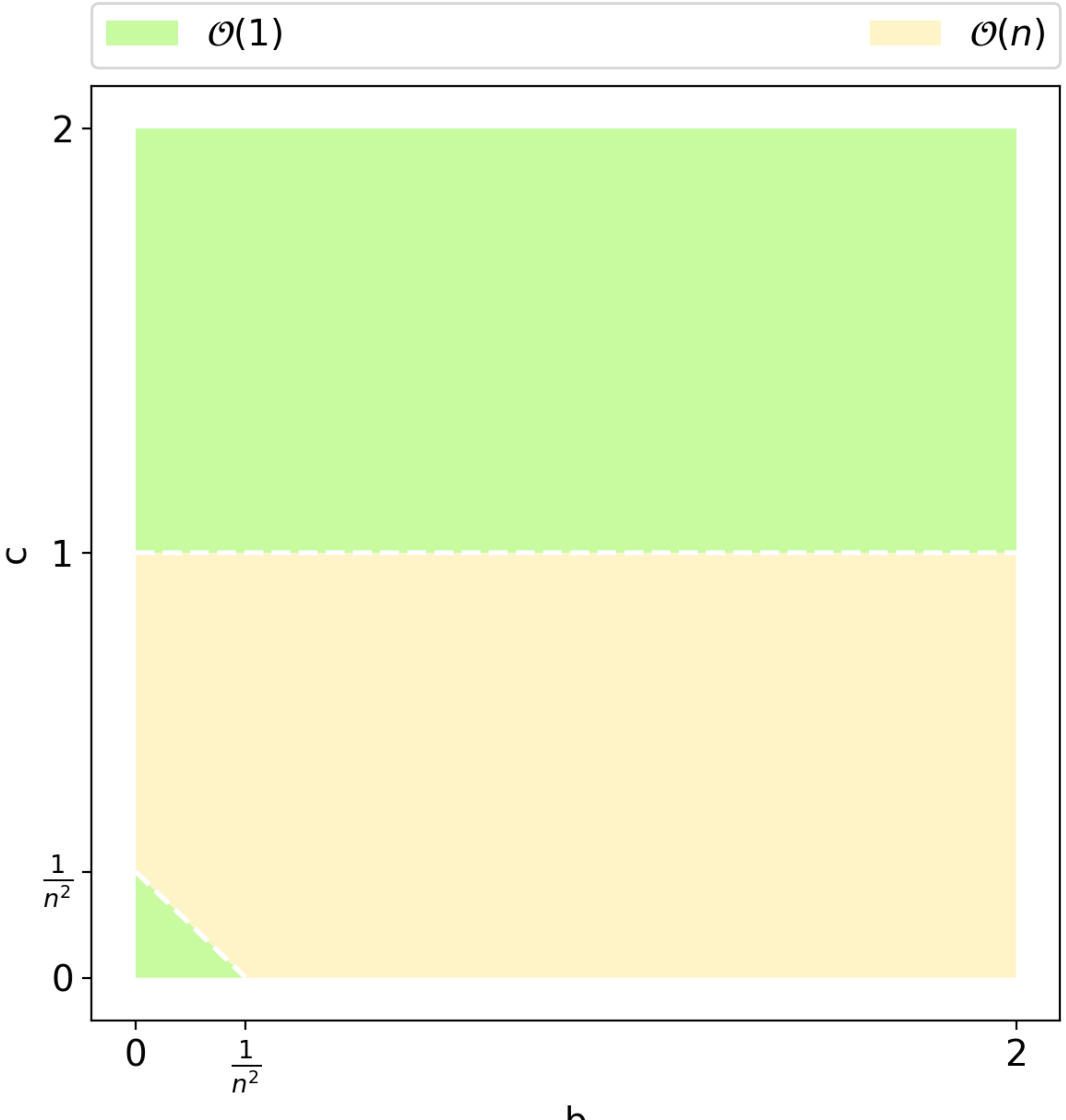


Price of anarchy

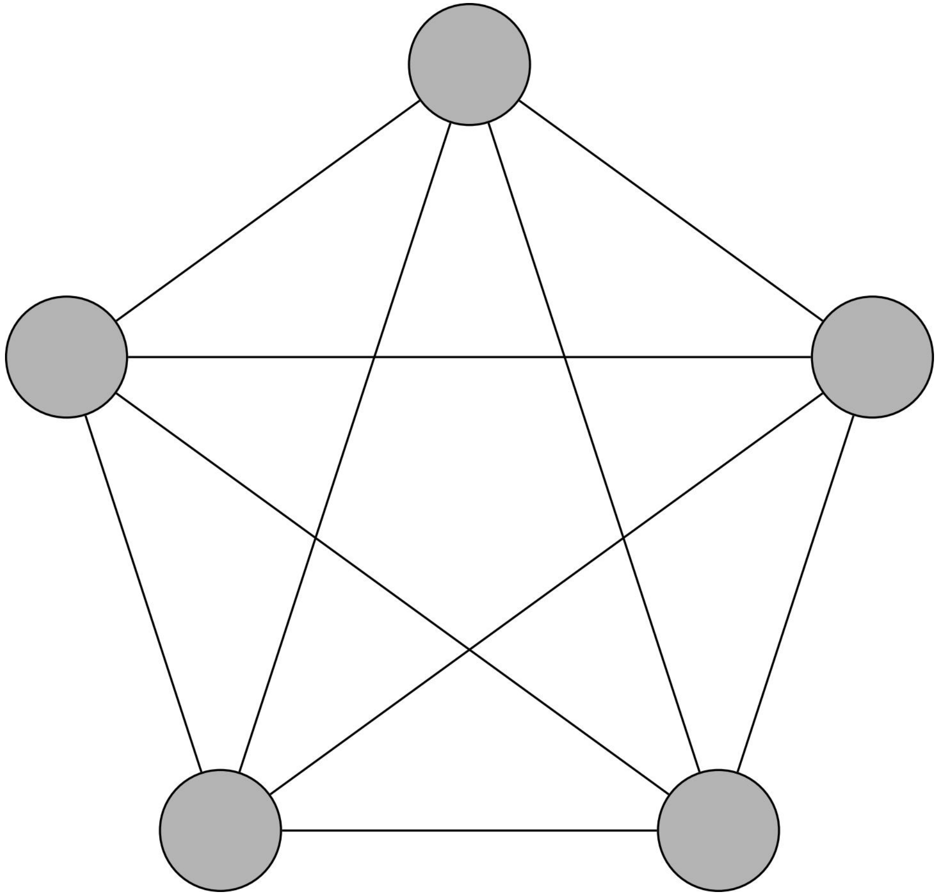


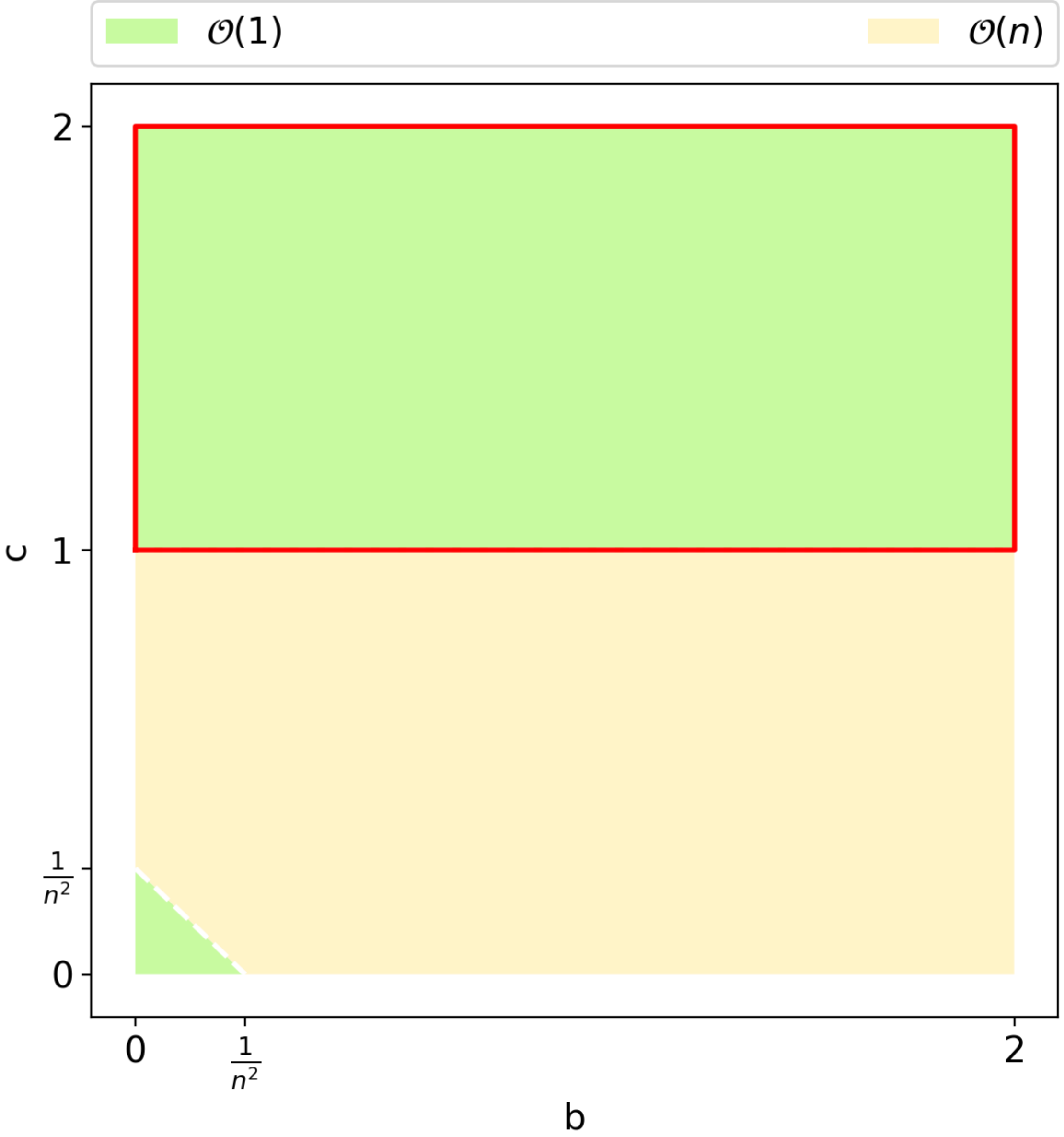
Price of anarchy



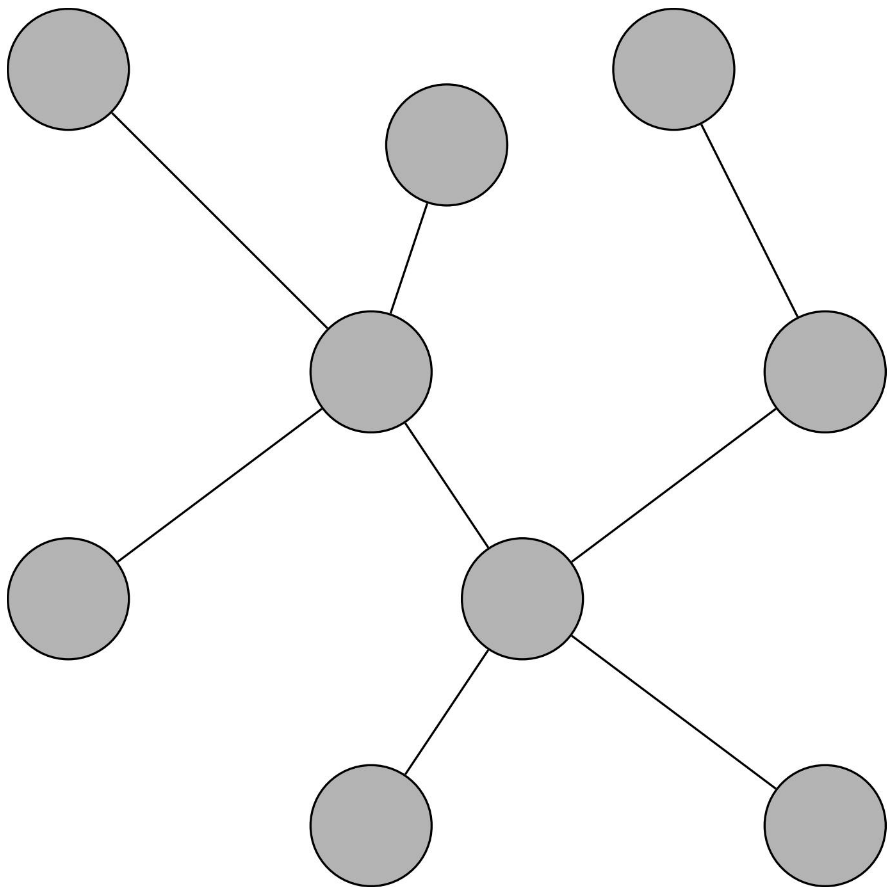


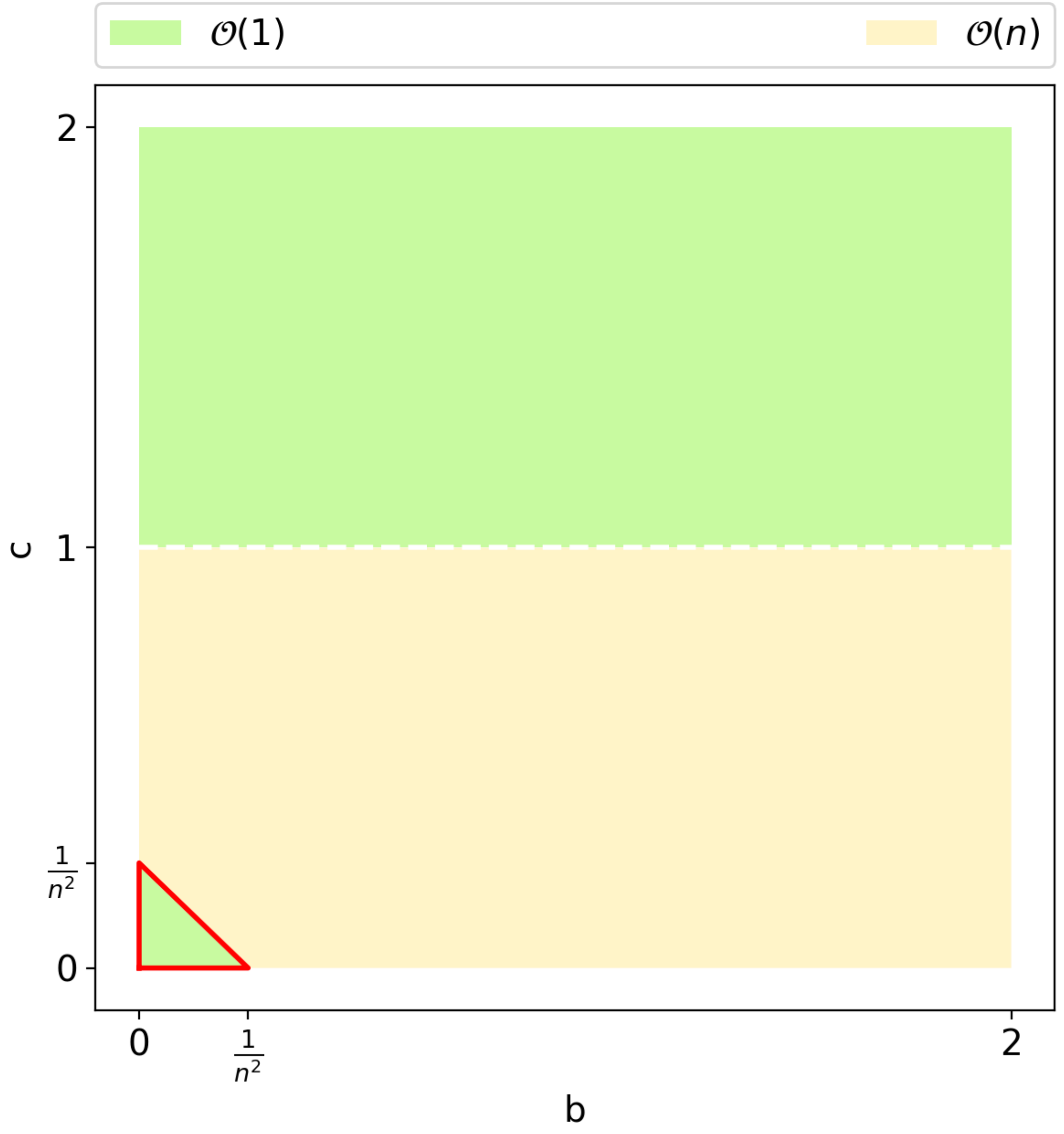
Price of anarchy





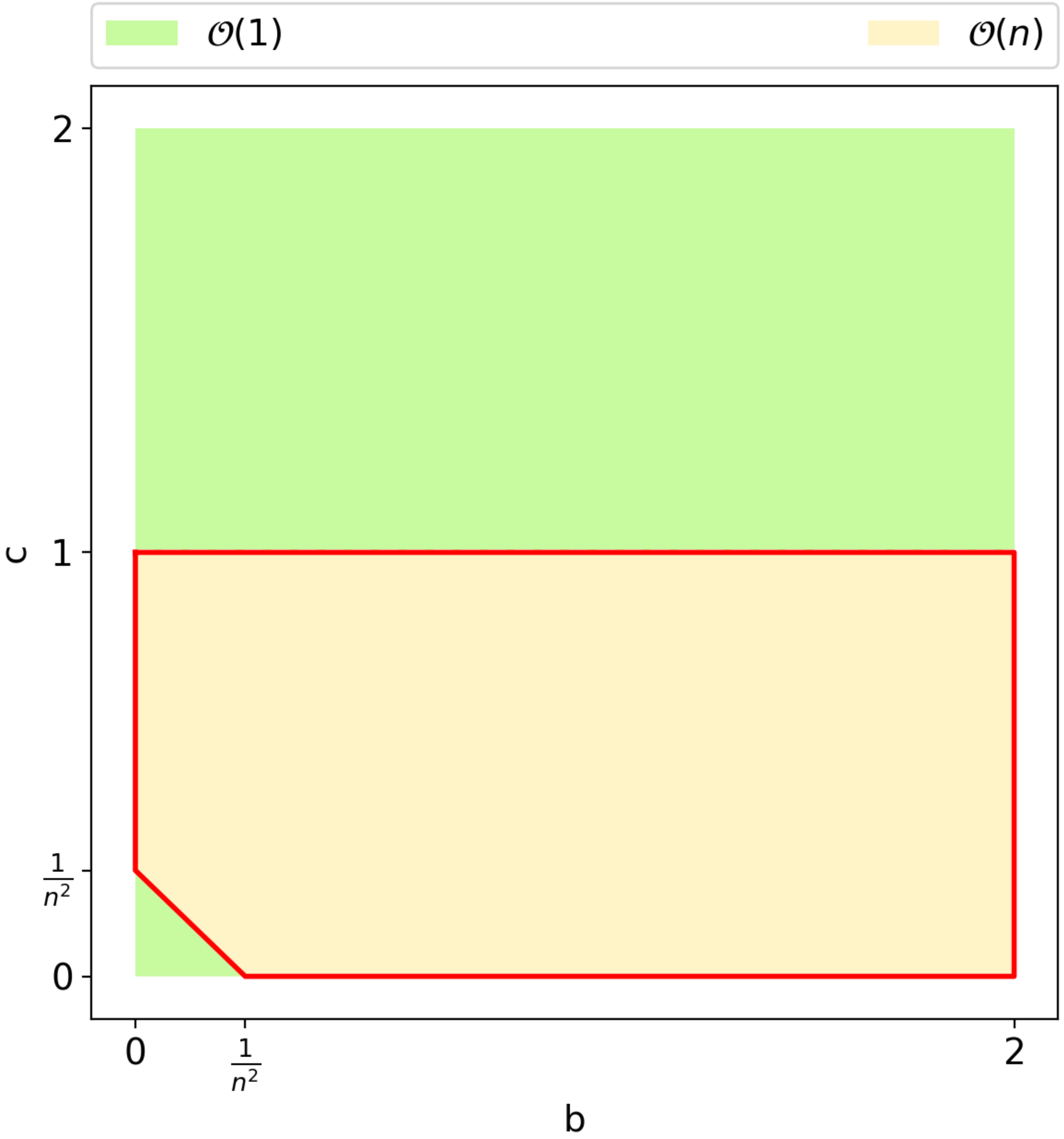
Price of anarchy



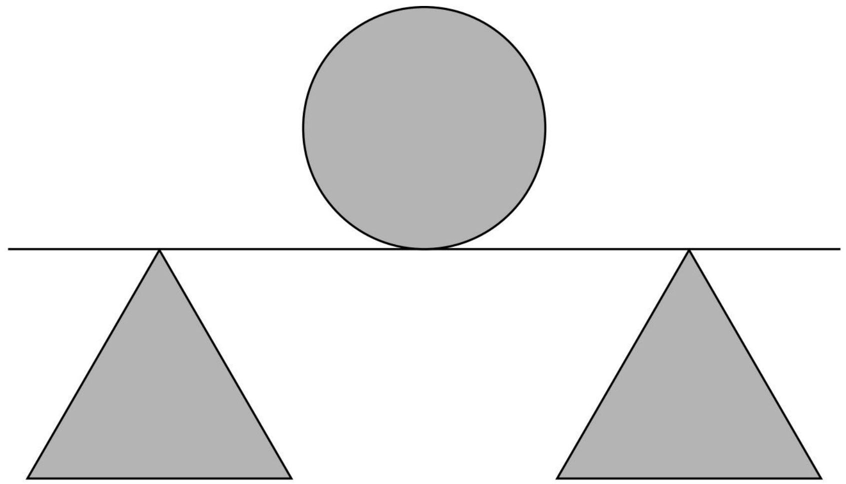


Price of anarchy

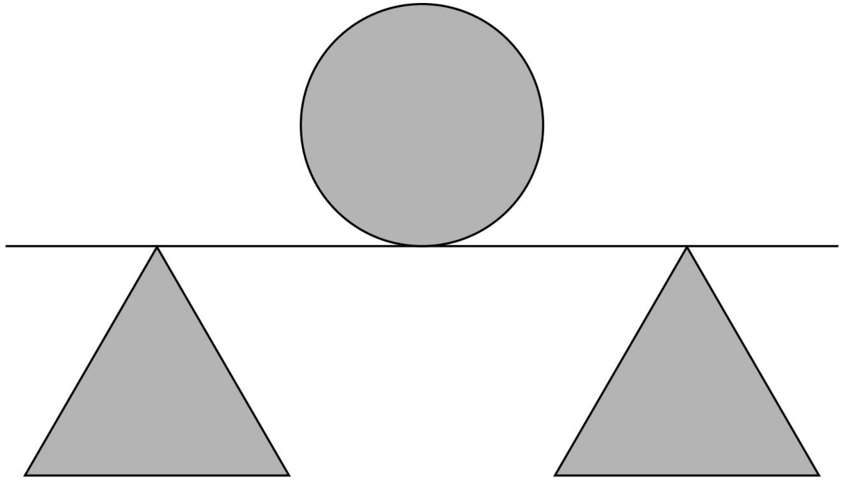
?

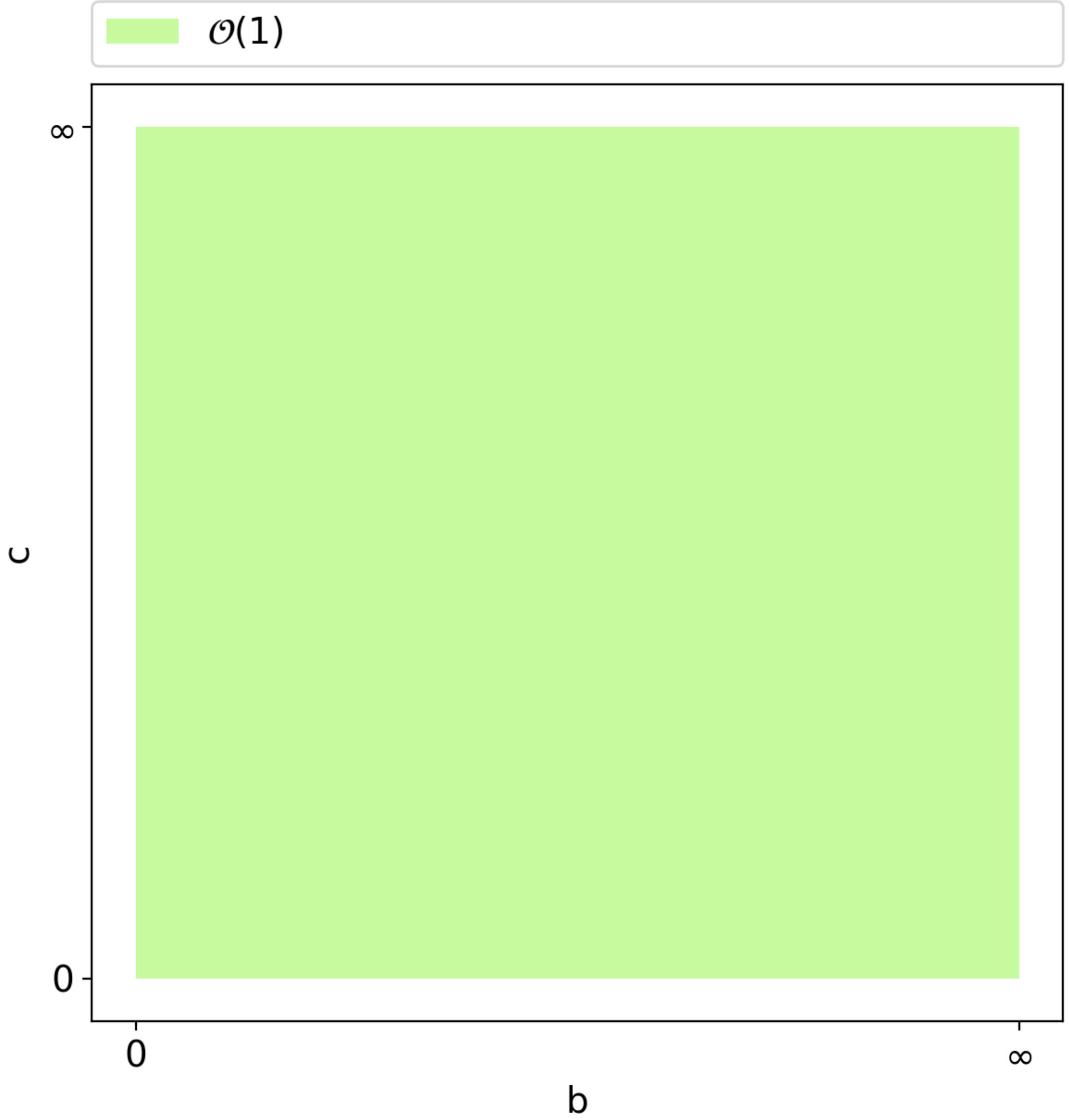


Price of stability

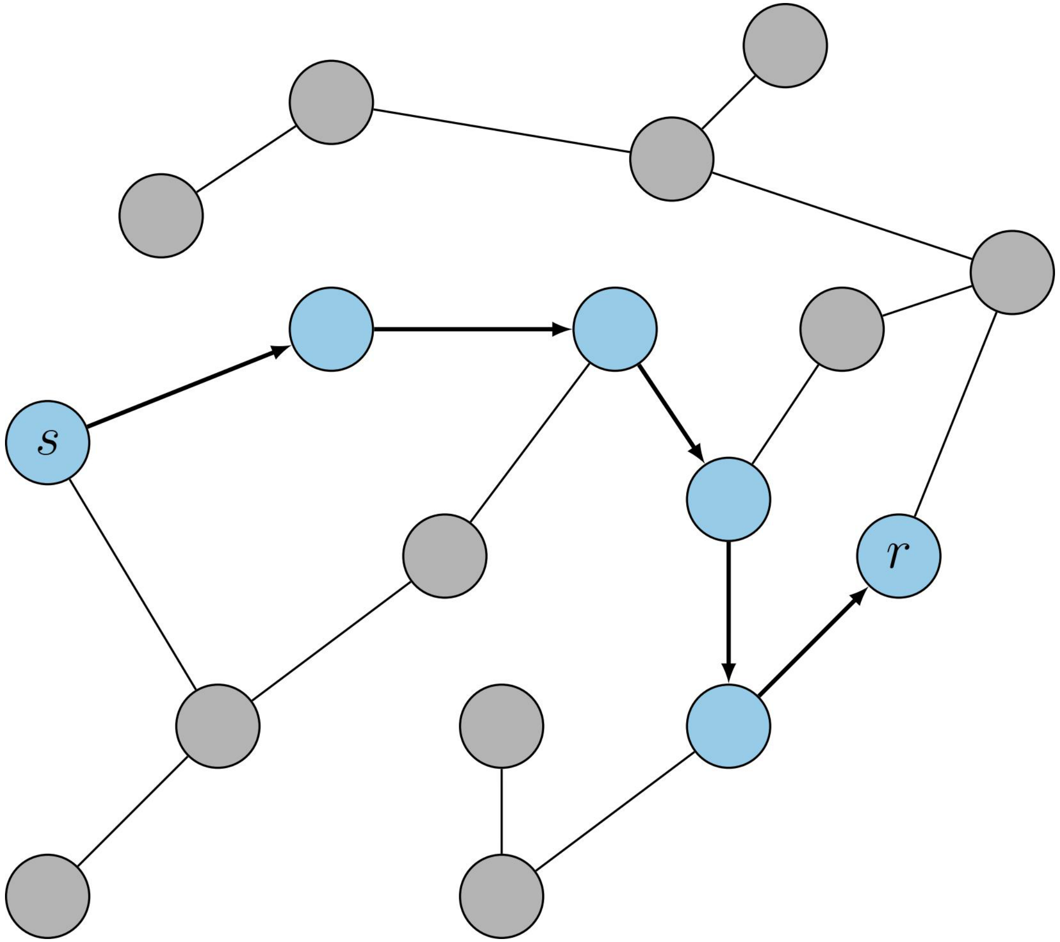


Price of stability

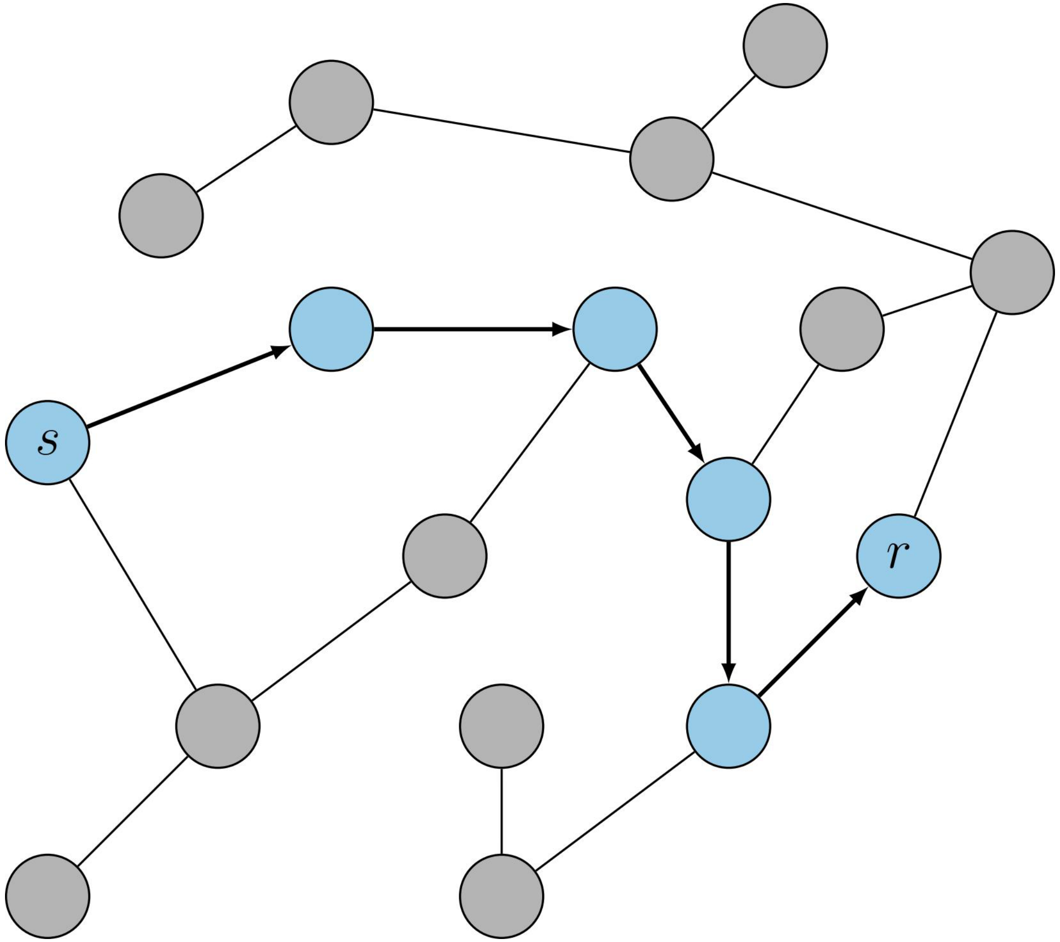


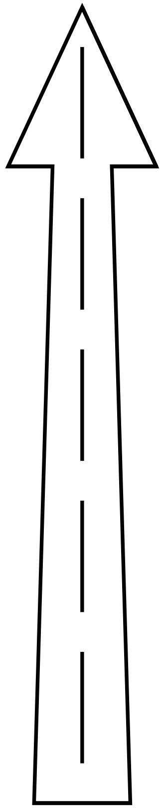


Ride the Lightning:
The Game Theory of Payment Channels



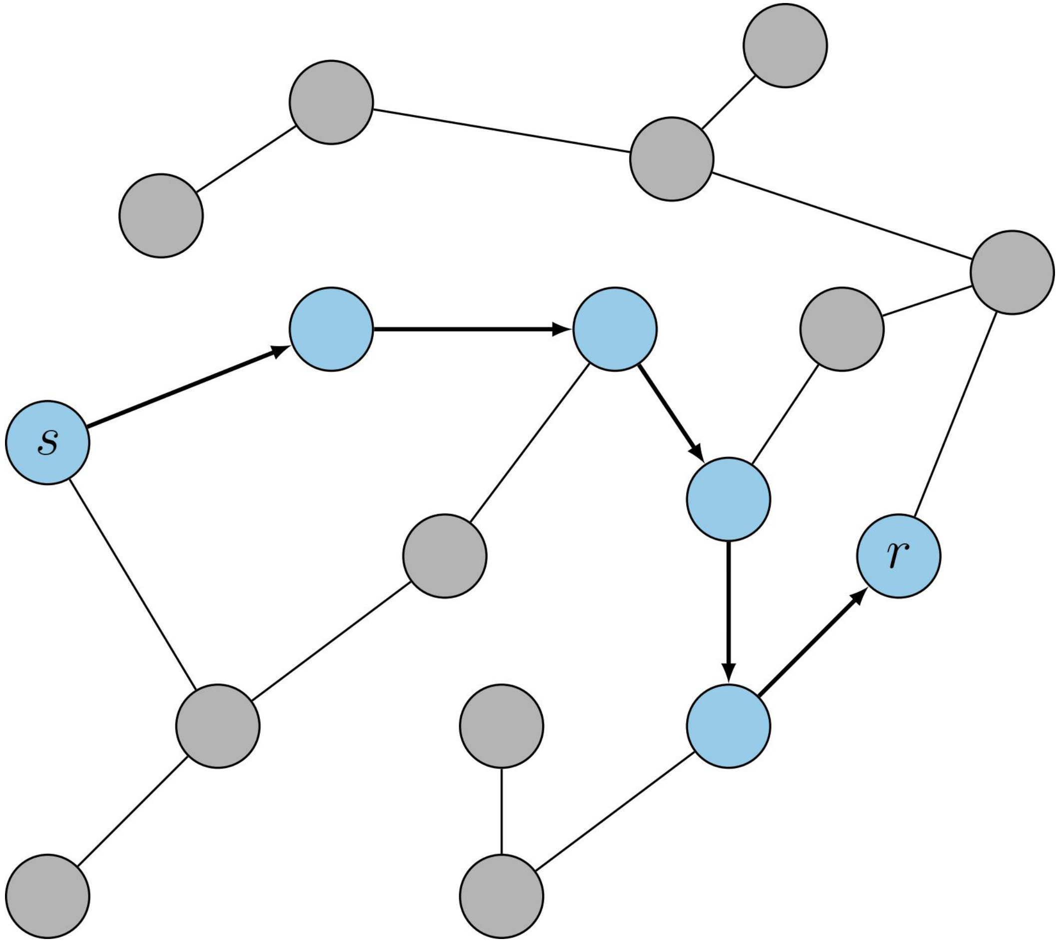
Ride the Lightning:
The Game Theory of Payment Channels

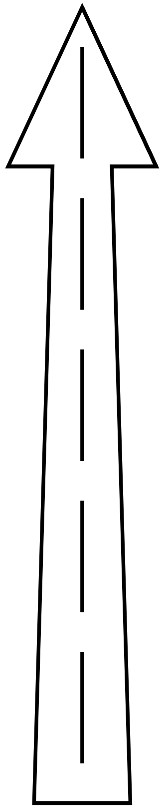




tight bound of
price of anarchy

Ride the Lightning: The Game Theory of Payment Channels

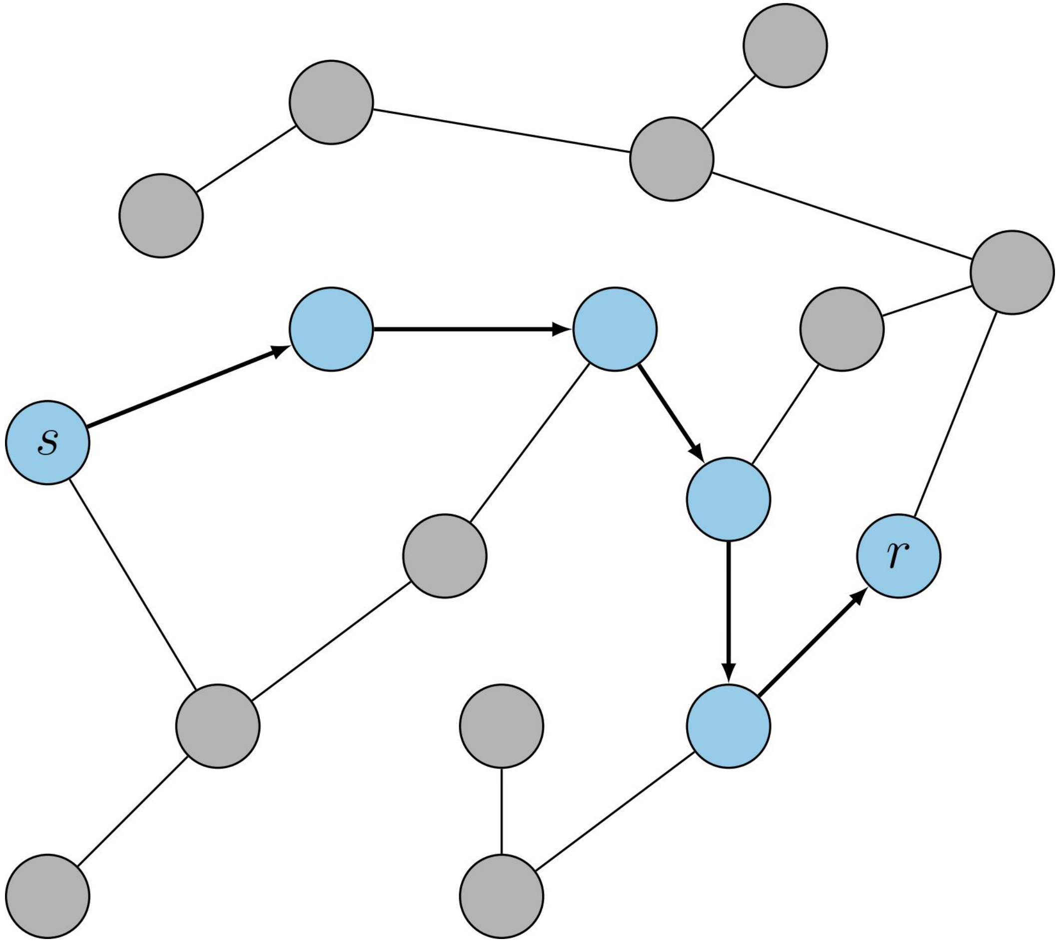




tight bound of price of anarchy

modify model for channel initiation

Ride the Lightning: The Game Theory of Payment Channels



tight bound of price of anarchy

modify model for channel initiation

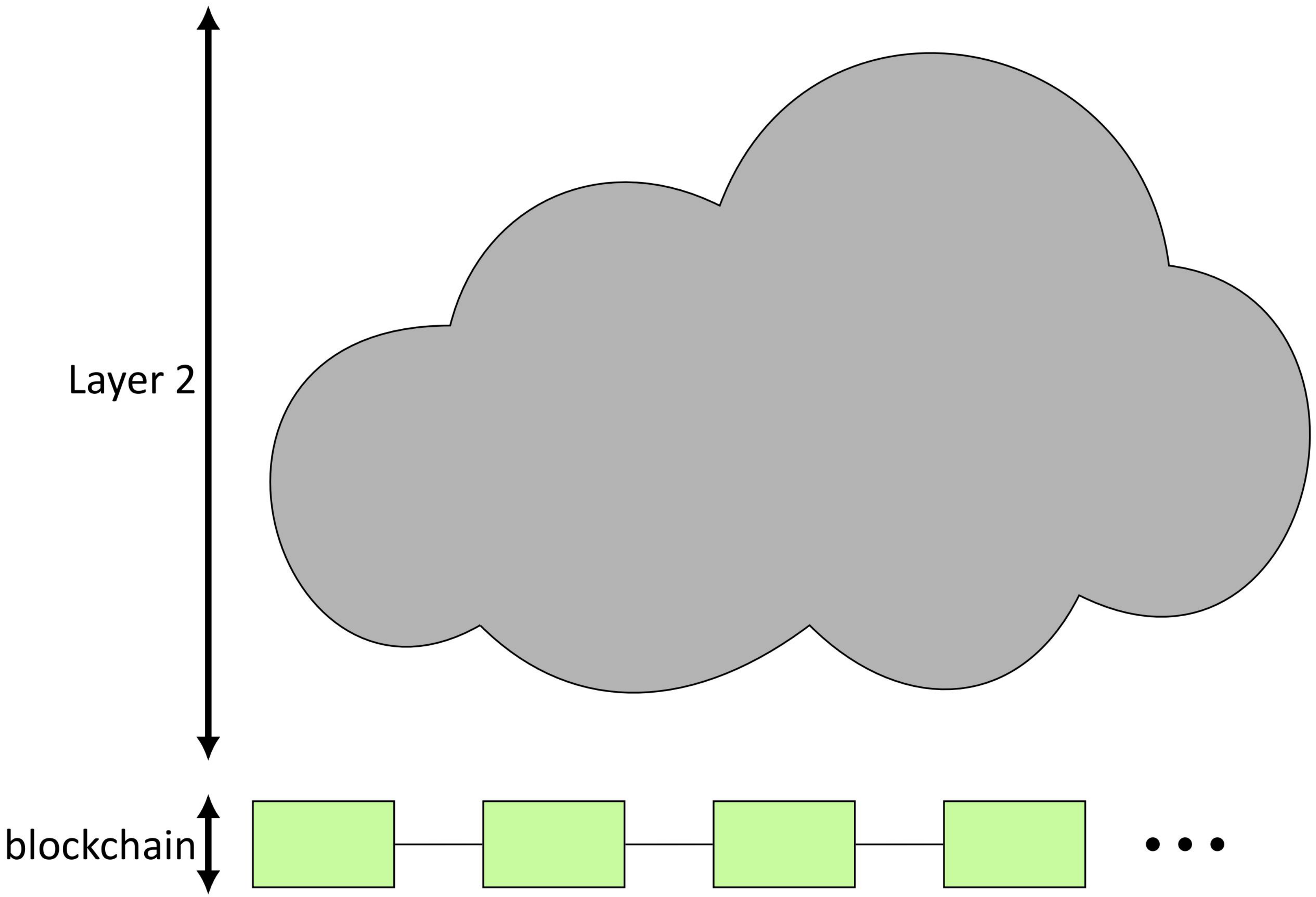
weights for players and pairs

Thank You!

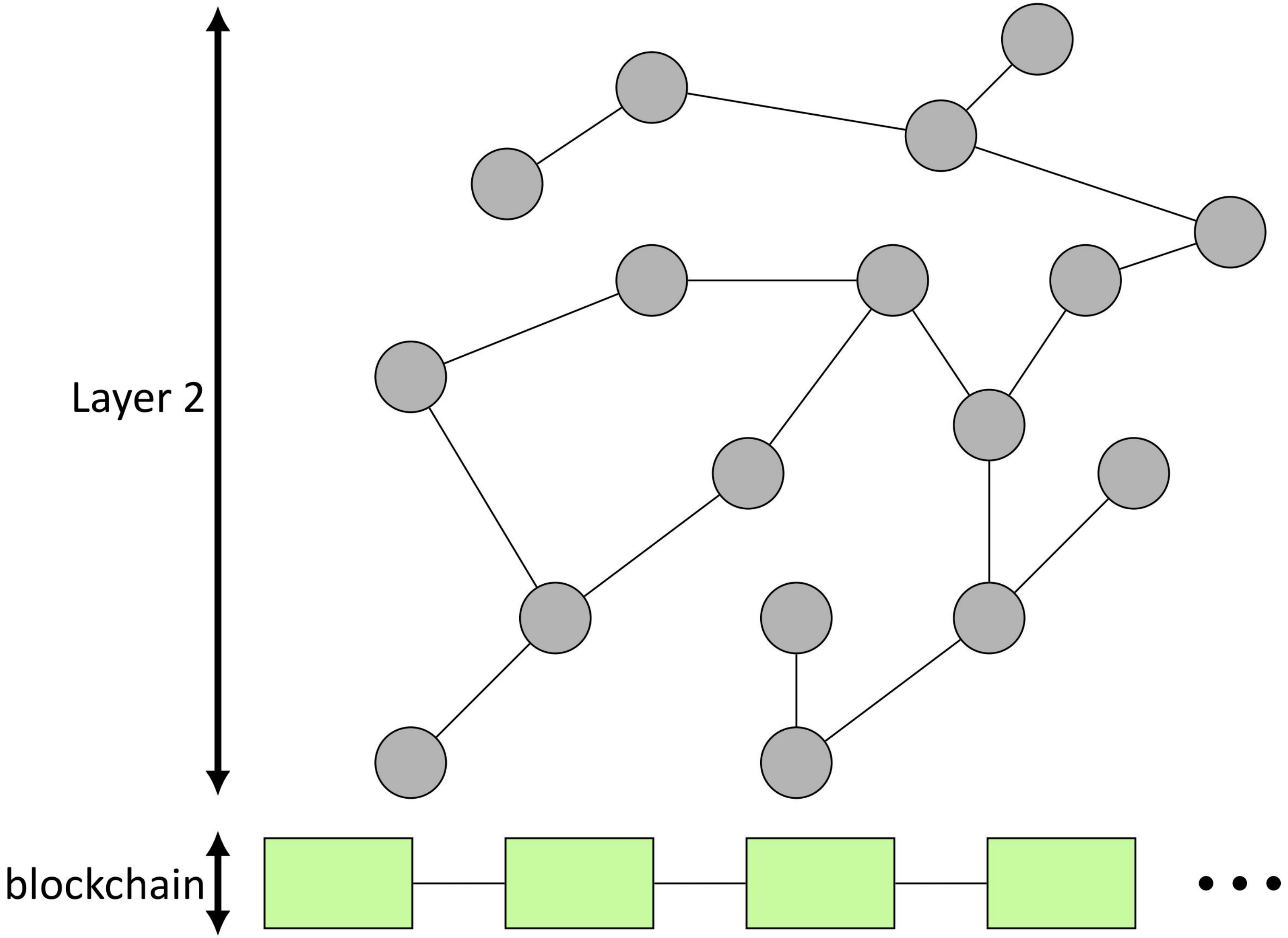
Questions & Comments?

Zeta Avarikioti, Lioba Heimbach, Yuyi Wang , Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

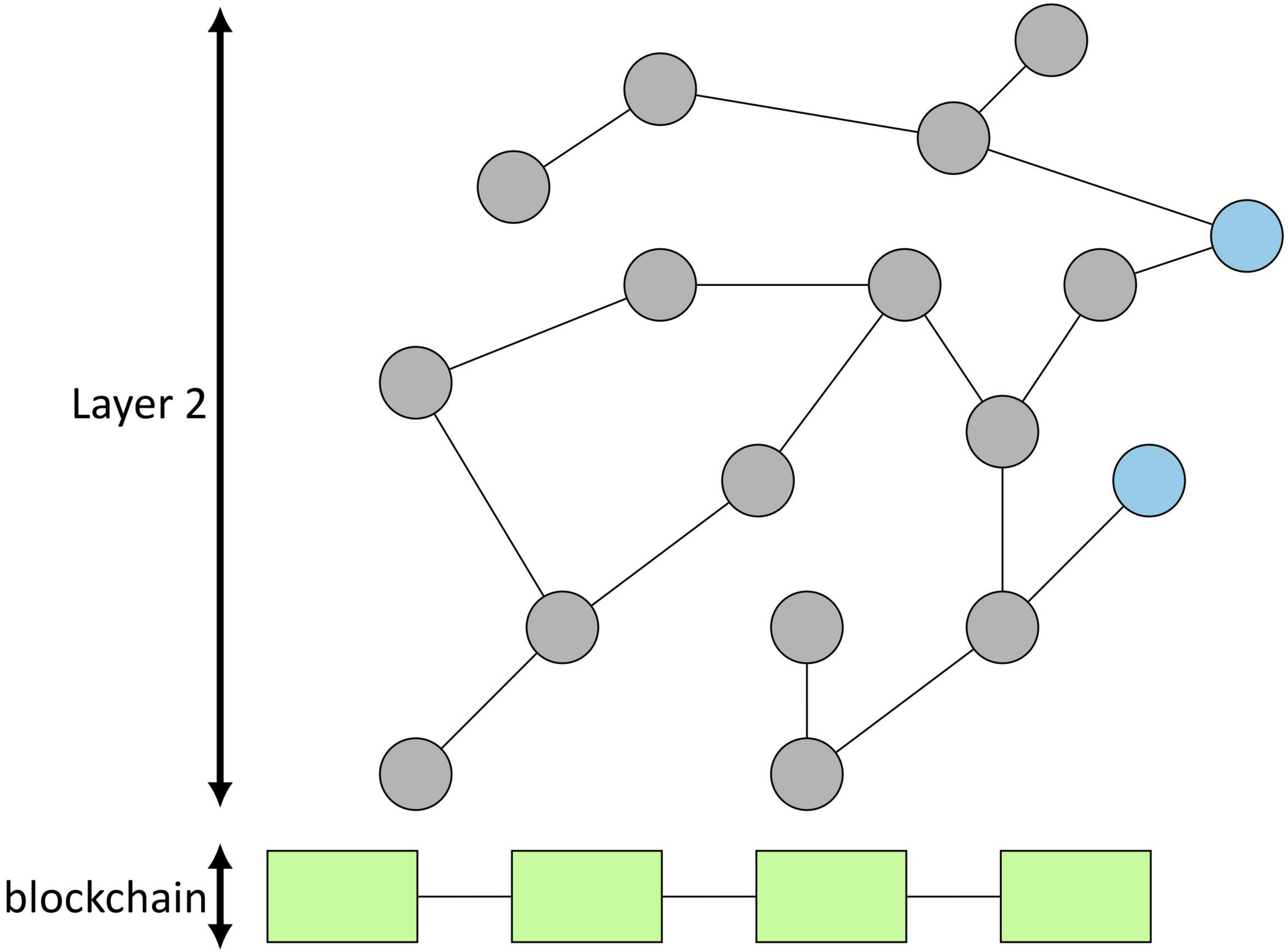
Payment channels network



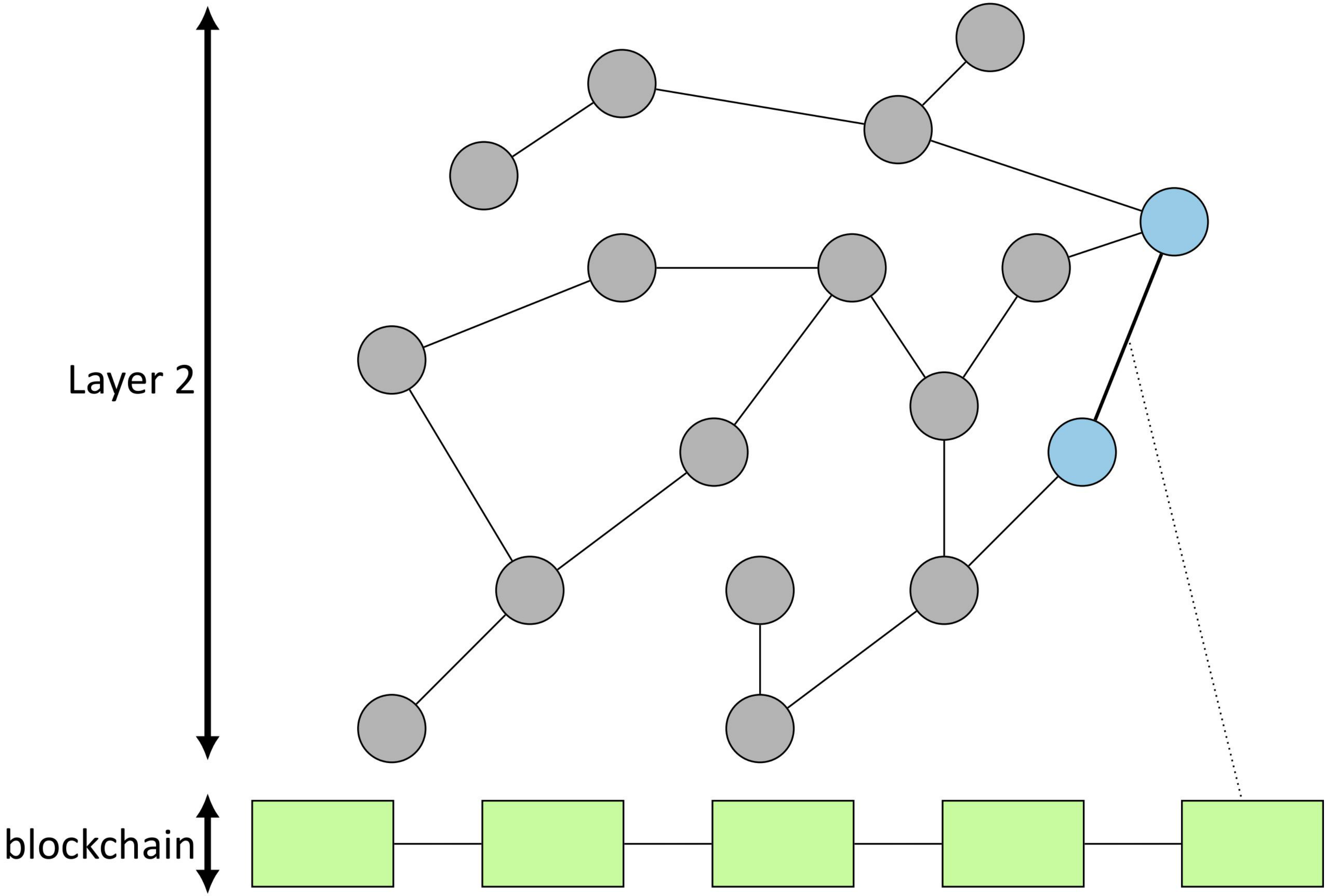
Payment channels network



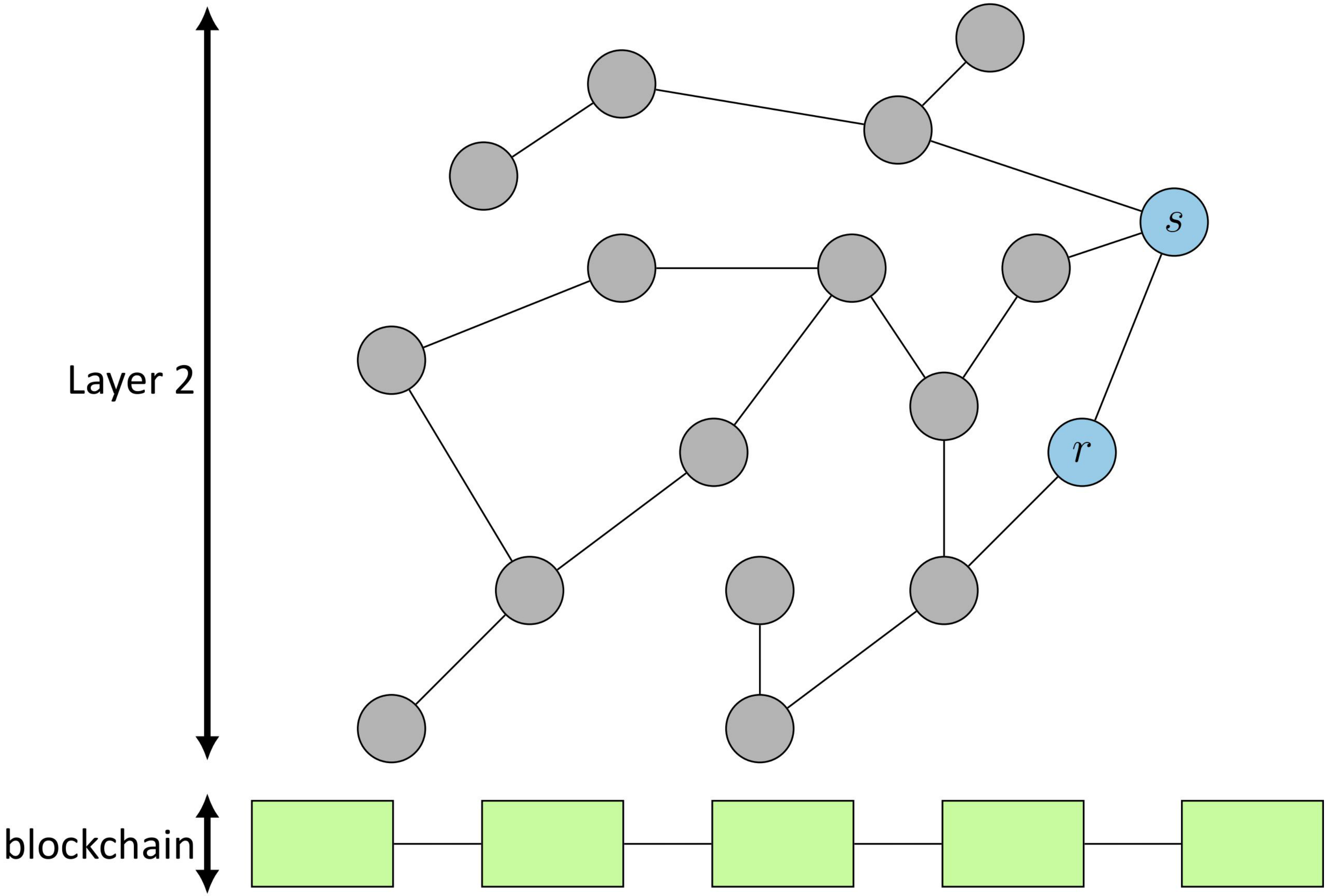
On-chain channel creation



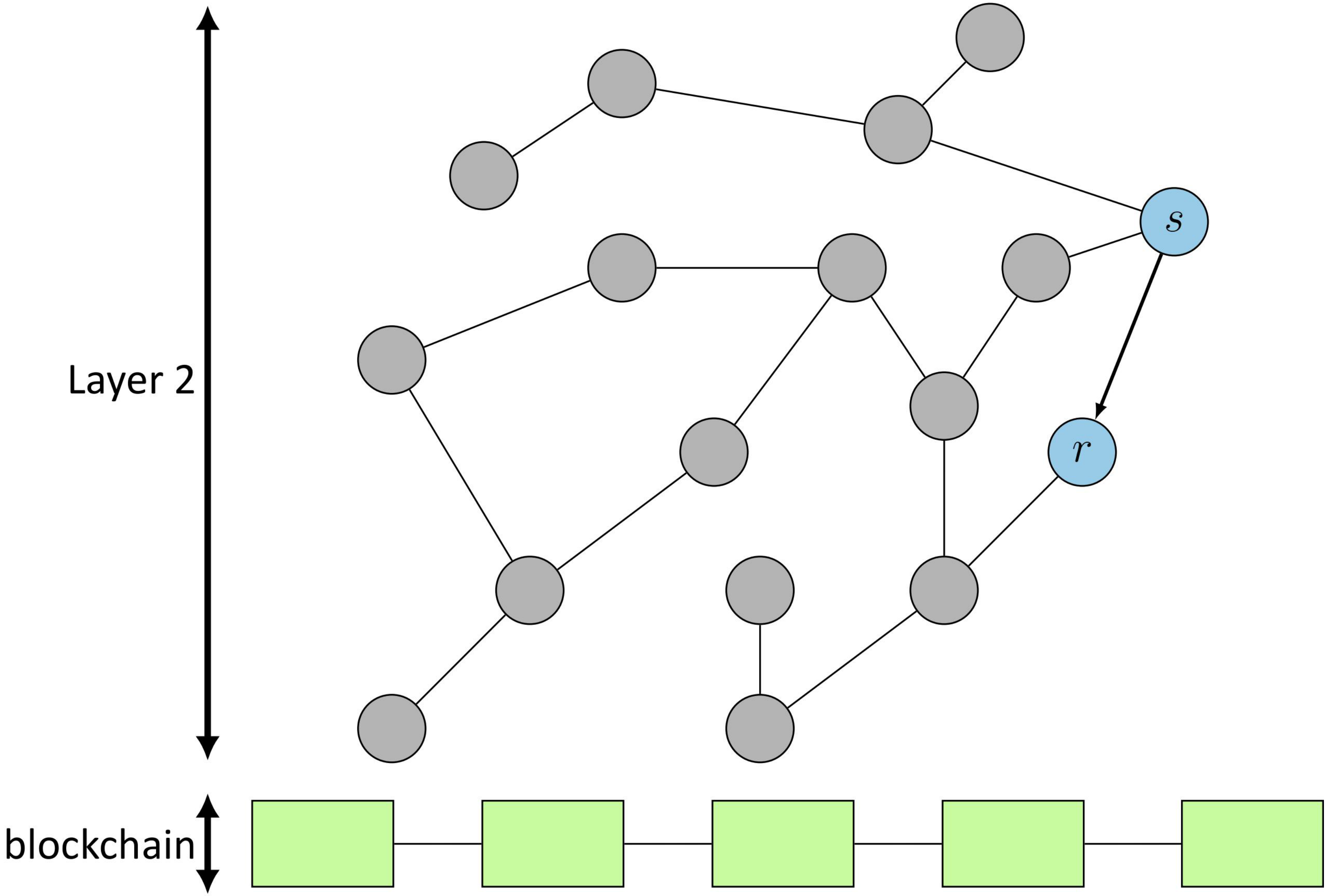
On-chain channel creation



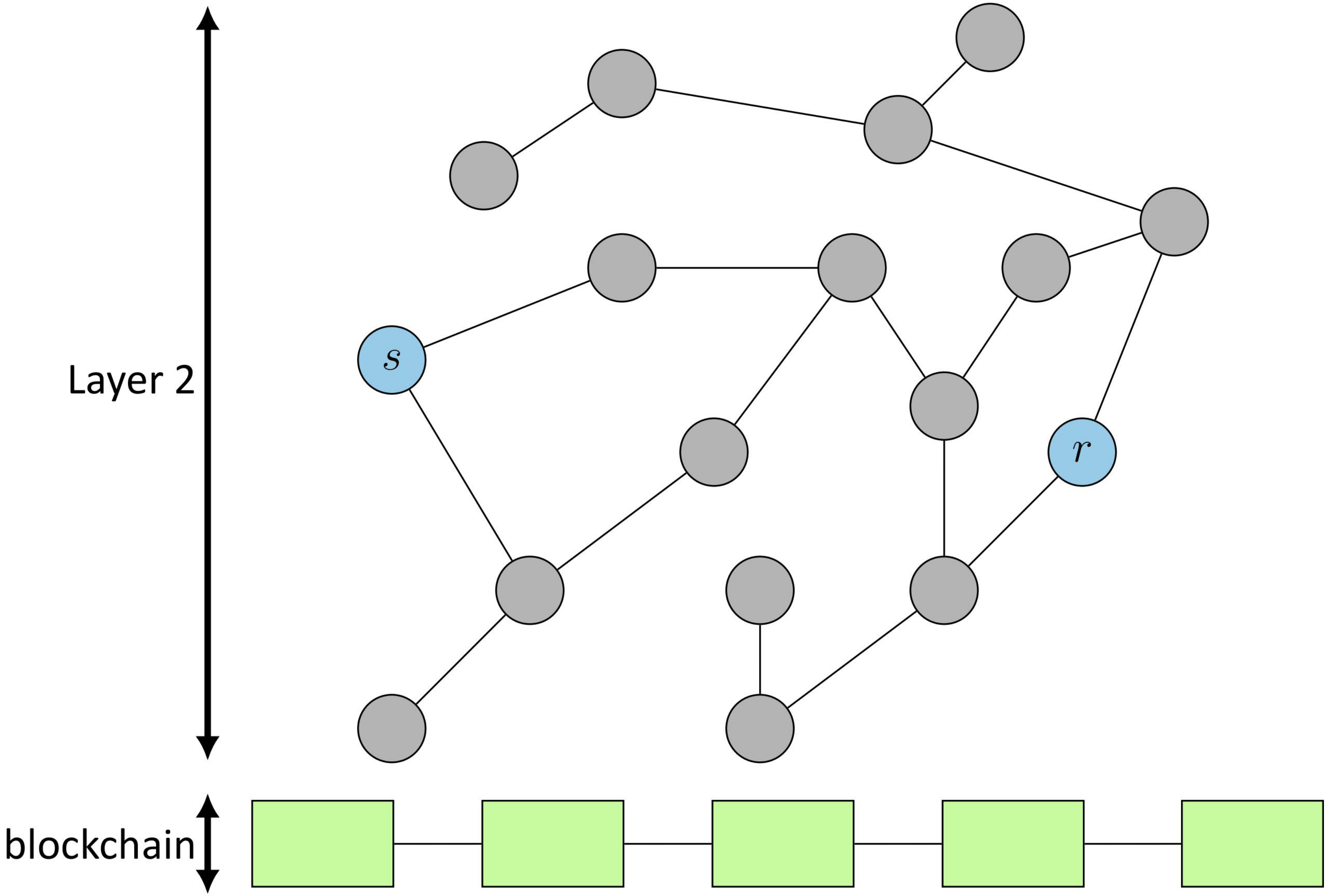
Off-chain transaction between neighbors



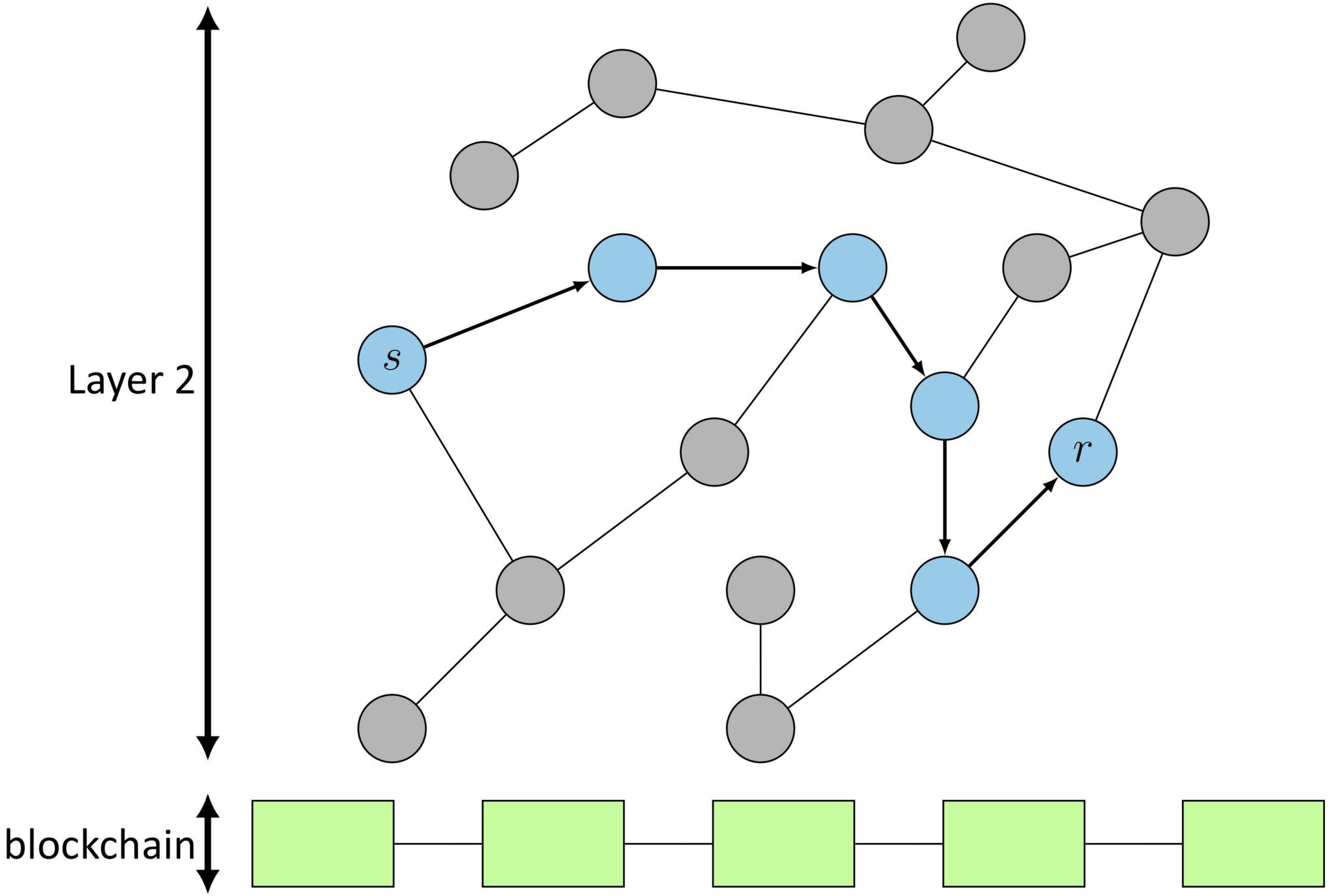
Off-chain transaction between neighbors



Off-chain transaction between neighbors



Off-chain transaction between neighbors



Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

$$\text{betweenness}_u(s) = (n-1)(n-2) - \sum_{\substack{s,r \in [n]: \\ s \neq r \neq u, m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)}$$

Betweenness centrality

$$\mathrm{cost}_u(s) = |s_u| + b \cdot \mathrm{betweenness}_u(s) + c \cdot \mathrm{closeness}_u(s)$$

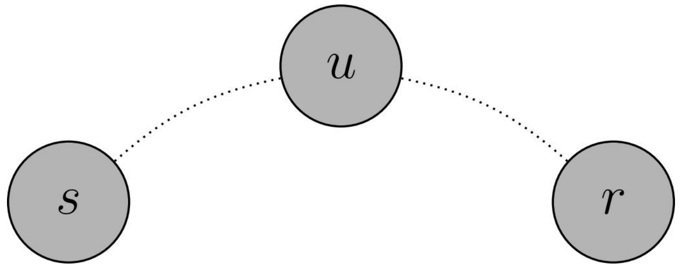
$$\mathrm{betweenness}_u(s) = (n-1)(n-2) - \sum_{\substack{s,r\in[n]:\\ s\neq r\neq u, m(s,r)>0}} \frac{m_u(s,r)}{m(s,r)}$$

ensures positivity of cost function

Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

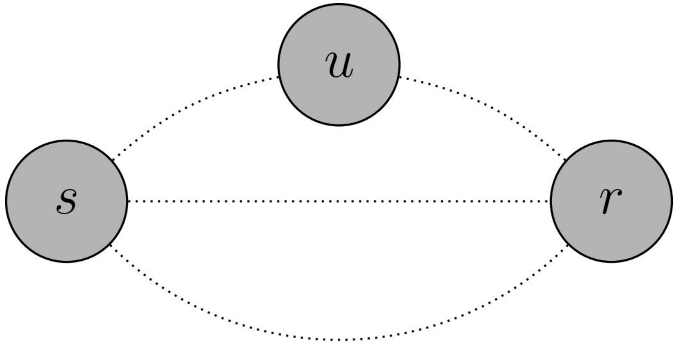
$$\text{betweenness}_u(s) = (n-1)(n-2) - \sum_{\substack{s,r \in [n]: \\ s \neq r \neq u, m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)}$$



Betweenness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

$$\text{betweenness}_u(s) = (n-1)(n-2) - \sum_{\substack{s,r \in [n]: \\ s \neq r \neq u, m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)}$$



Closeness centrality

$$\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$$

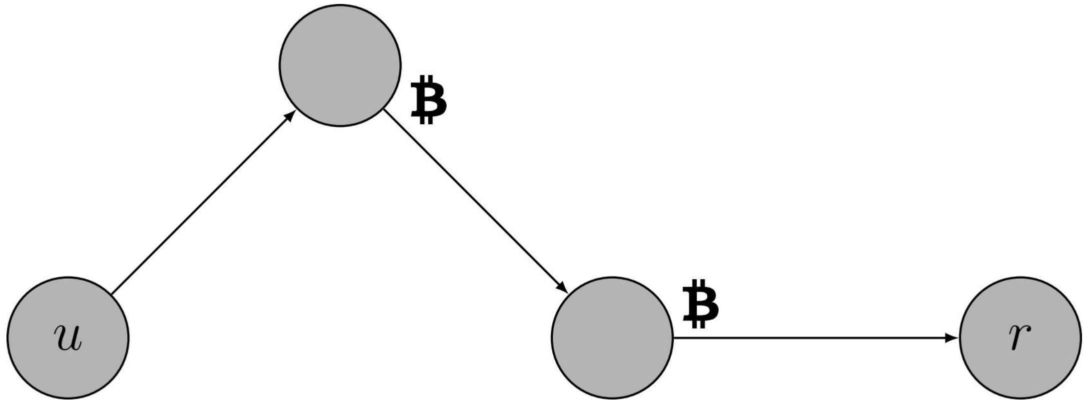
$$\text{closeness}_u(s) = \sum_{r \in [n]-u} d_{G[s]}(u, r) - 1$$

Closeness centrality

$$\mathrm{cost}_u(s) = |s_u| + b \cdot \mathrm{betweenness}_u(s) + c \cdot \mathrm{closeness}_u(s)$$

$$\mathrm{closeness}_u(s) = \sum_{r \in [n]-u} d_{G[s]}(u, r) - 1$$

transaction fees encountered



Social cost

$$
\begin{aligned}
\text{cost}(s) &= \sum_{u\in[n]} \text{cost}_u(s) \\
&= |E(G)| + b \sum_{u\in[n]} \text{betweenness}_u(s) + c \sum_{u\in[n]} \text{closeness}_u(s) \\
&= |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b) \cdot \sum_{u\in[n]} \text{closeness}_u(s)
\end{aligned}
$$

Social cost

$$\text{cost}(s) = \sum_{u\in[n]} \text{cost}_u(s)$$

$$= |E(G)| + b \sum_{u\in[n]} \text{betweenness}_u(s) + c \sum_{u\in[n]} \text{closeness}_u(s)$$

☆ $$= |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b) \cdot \sum_{u\in[n]} \text{closeness}_u(s)$$

☆ $$\overline{B}(G) = (n-1)(\bar{l}(G) - 1)$$

$\overline{B}(G)$ average betweenness

$\bar{l}(G)$ average distance

Social optimum ($b \leq c$)

$$\begin{aligned}
\mathrm{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) + \underbrace{(c-b)}_{\geq 0} \sum_{u \in [n]} \sum_{r \in [n]-u} \big(d_{G[s]}(u,r) - 1\big) \\
&\geq |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1) - 2|E|) \\
&= (1 - 2 \cdot (c-b)) \cdot |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1))
\end{aligned}$$

Social optimum ($b \leq c$)

$$\begin{aligned}
\text{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) + \underbrace{(c-b)}_{\geq 0} \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1\right) \\
&\overset{\star}{\geq} |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1) - 2|E|) \\
&= (1 - 2 \cdot (c-b)) \cdot |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1))
\end{aligned}$$

★ all nodes that are not connected by an edge are at least distance two apart

Social optimum ($b \leq c$)

$$\begin{aligned}\text{cost}(s) =& |E(G)| + b \cdot n \cdot (n-1)(n-2) + \underbrace{(c-b)}_{\geq 0} \sum_{u \in [n]} \sum_{r \in [n]-u} \big(d_{G[s]}(u,r) - 1\big) \\ \geq& |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1) - 2|E|) \\ =& (1 - 2 \cdot (c-b)) \cdot |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1))\end{aligned}$$

$c > \frac{1}{2} + b$ complete graph

$b \leq c \leq \frac{1}{2} + b$ star graph

Social optimum ($b > c$)

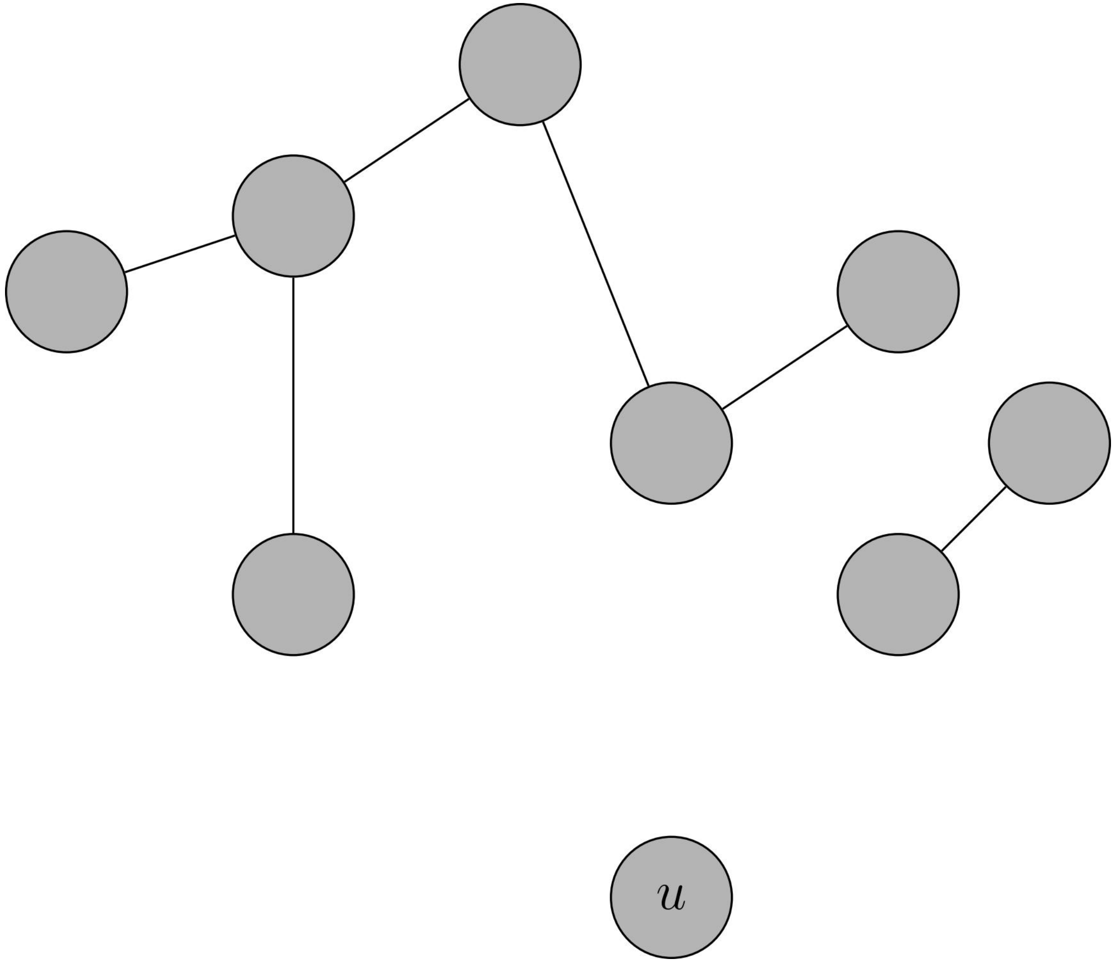
$$
\begin{aligned}
\mathrm{cost}(s) =& |E(G)| + b \cdot n \cdot (n-1)(n-2) - (b-c) \cdot \sum_{u \in [n]} \sum_{r \in [n]-u} \big(d_{G[s]}(u,r) - 1\big) \\
=& |E(G)| - 2 \cdot (b-c) \cdot d(G) + b \cdot n \cdot (n-1)(n-2) + (b-c) \cdot n \cdot (n-1) \\
\geq& \left(1 + b \cdot n \cdot (n-2) + \frac{b-c}{3} n \cdot (n-2)\right)(n-1)
\end{aligned}
$$

Social optimum ($b > c$)

$$\begin{aligned}
\text{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) - (b-c) \cdot \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1\right) \\
&= |E(G)| - 2 \cdot (b-c) \cdot d(G) + b \cdot n \cdot (n-1)(n-2) + (b-c) \cdot n \cdot (n-1) \\
&\overset{\star}{\geq} \left(1 + b \cdot n \cdot (n-2) + \frac{b-c}{3} n \cdot (n-2)\right)(n-1)
\end{aligned}$$

☆ path graph

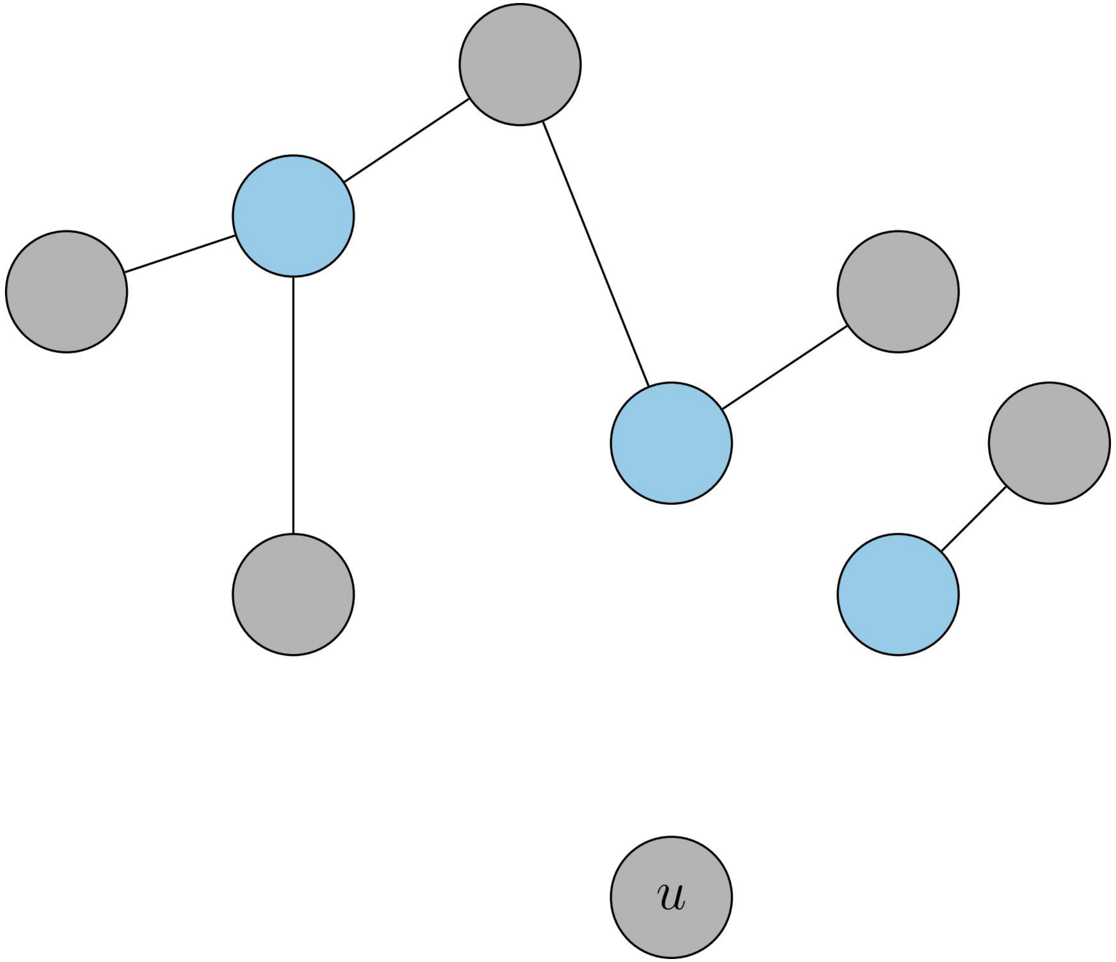
NP-hardness



$b = 0$

$0.5 < c < 1$

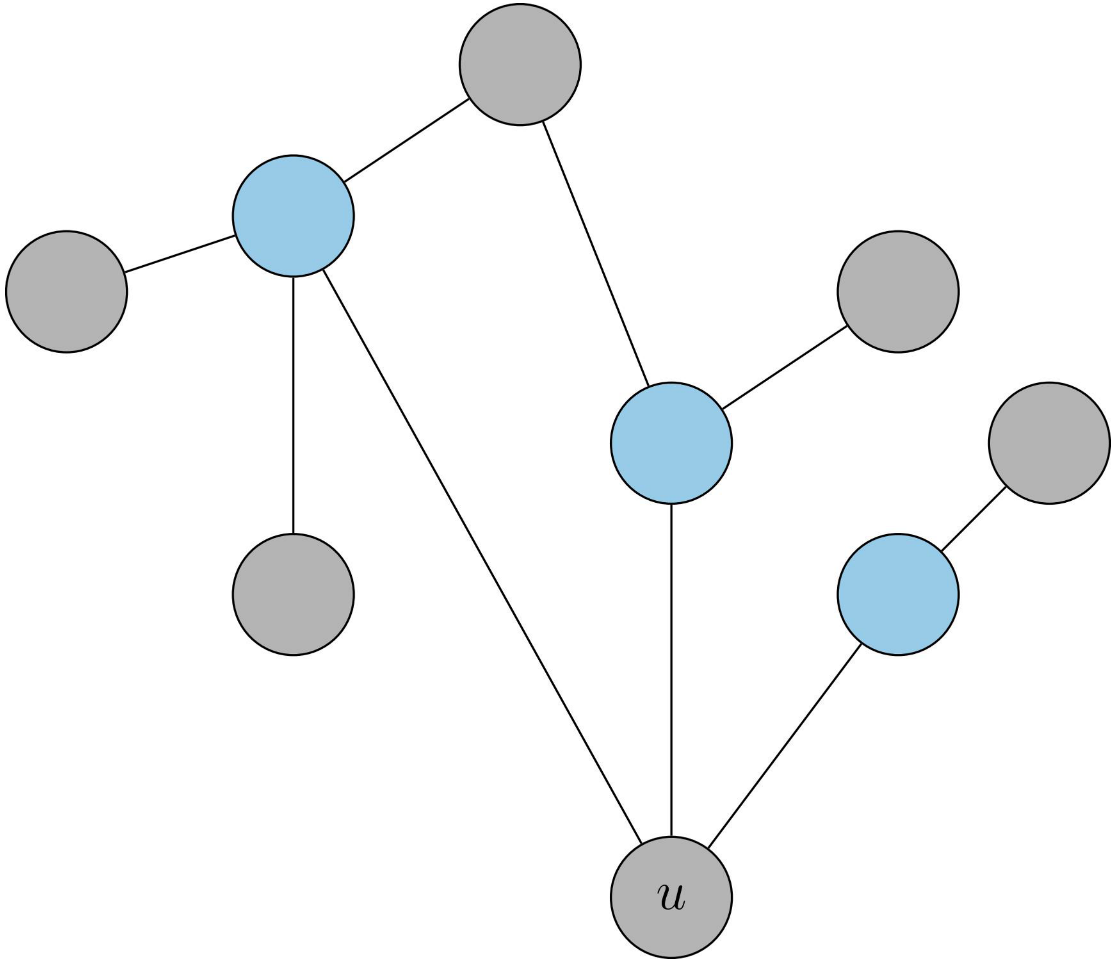
NP-hardness



$b = 0$

$0.5 < c < 1$

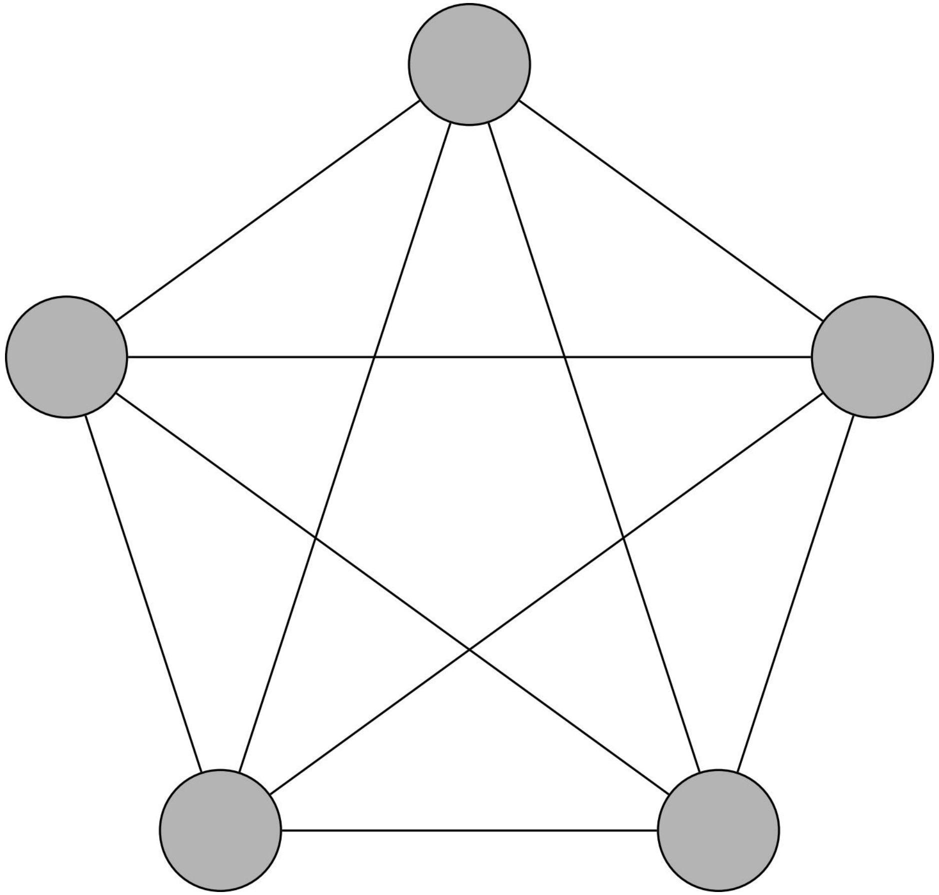
NP-hardness

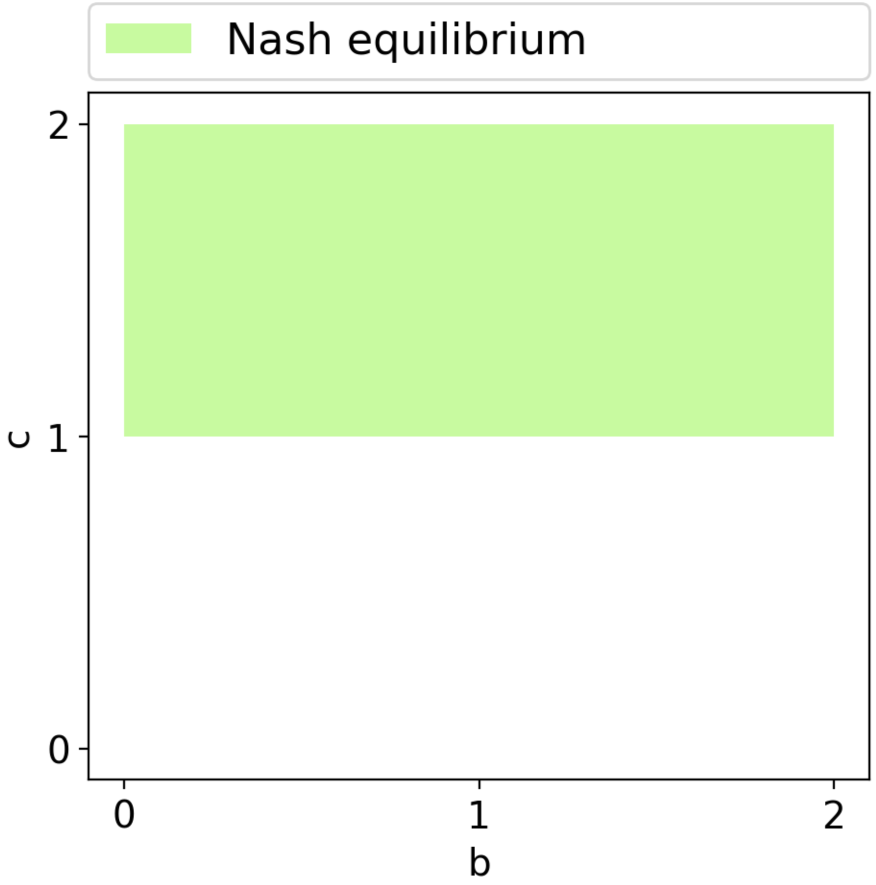


$b = 0$

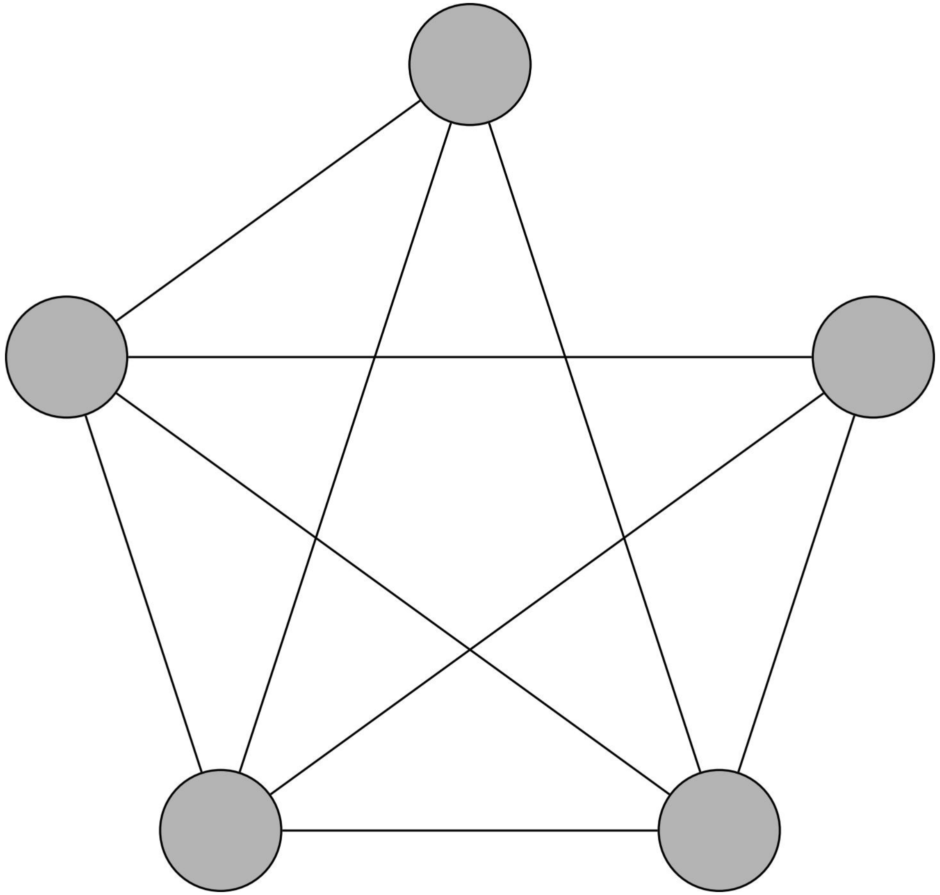
$0.5 < c < 1$

Complete graph



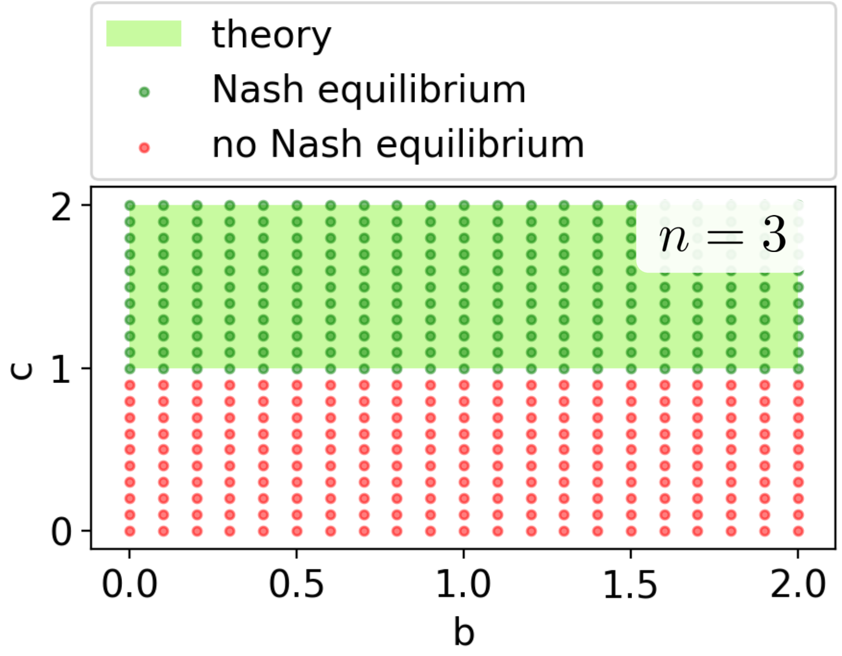


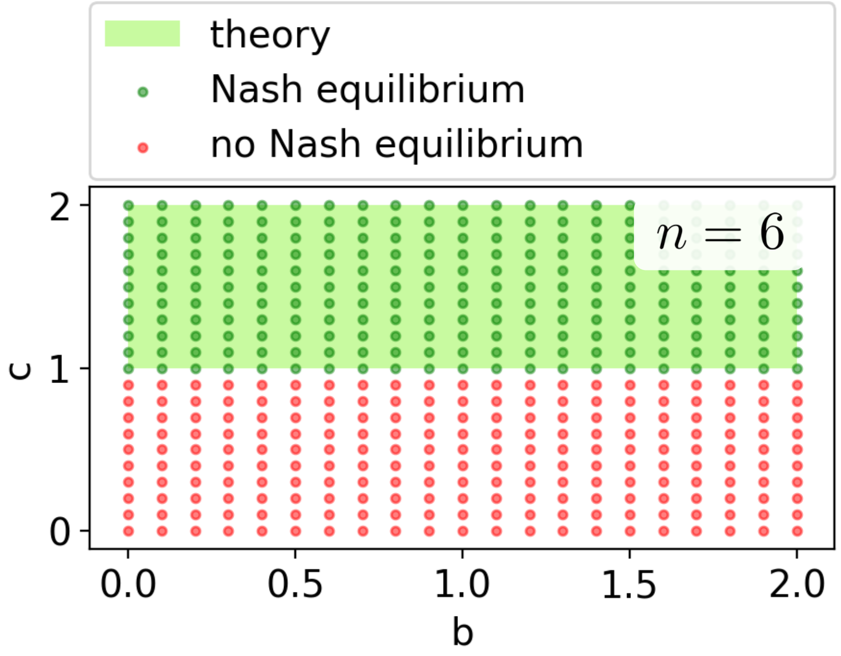
Complete graph



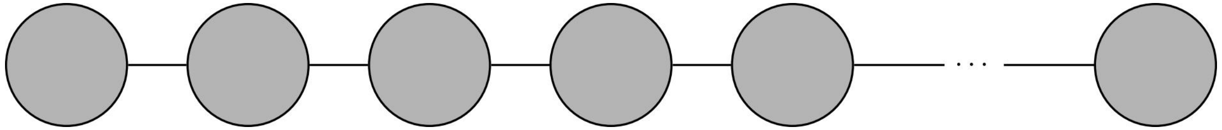
$$\Delta\text{cost} = 1 - c$$

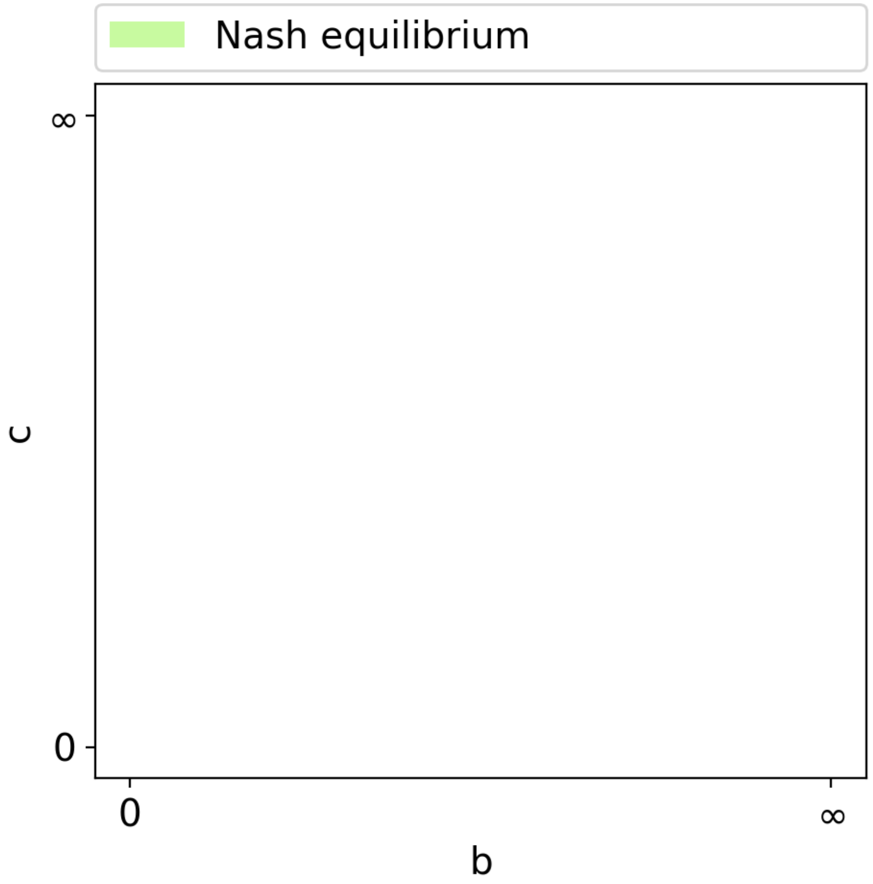
Complete graph



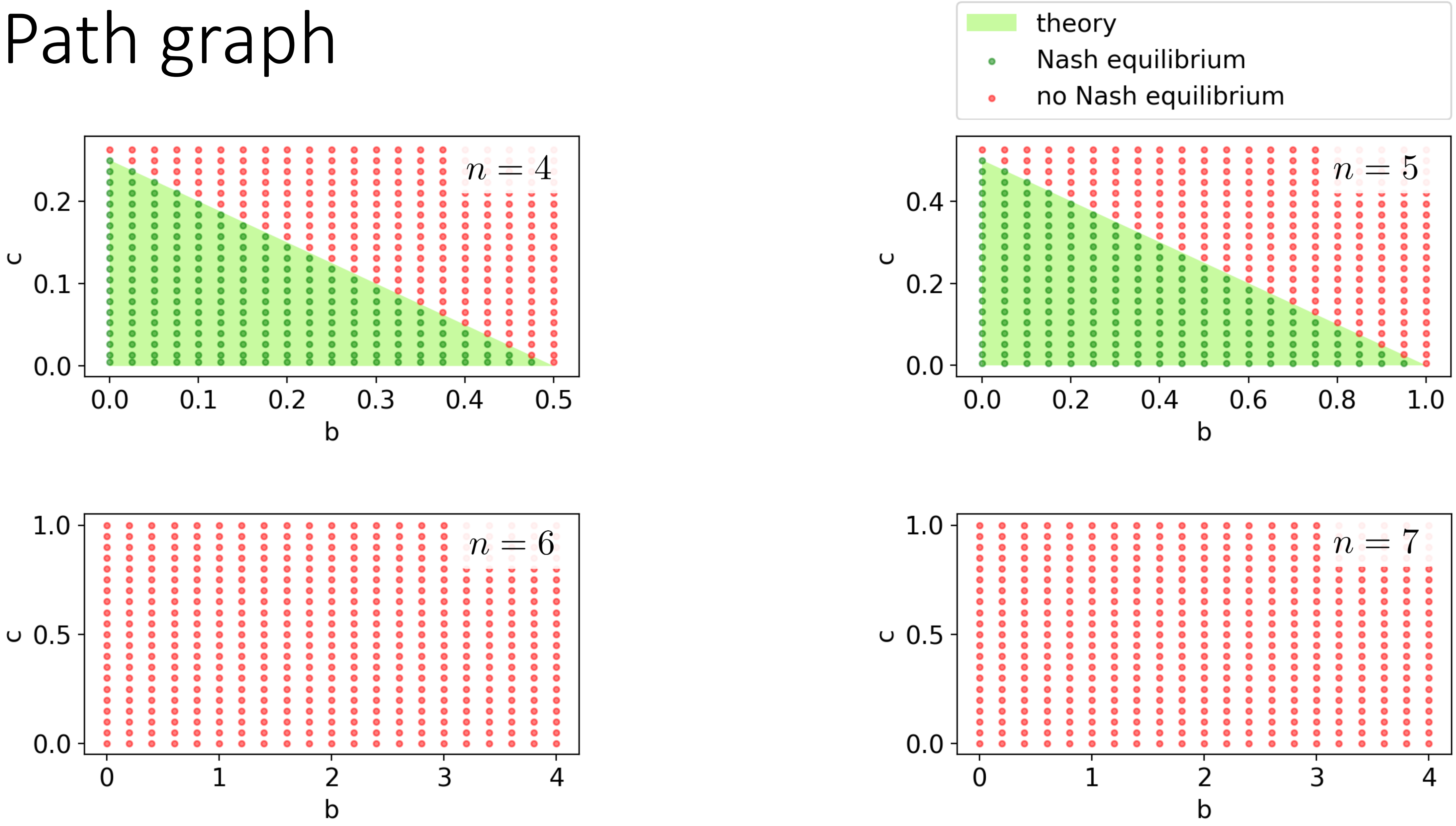


Path graph





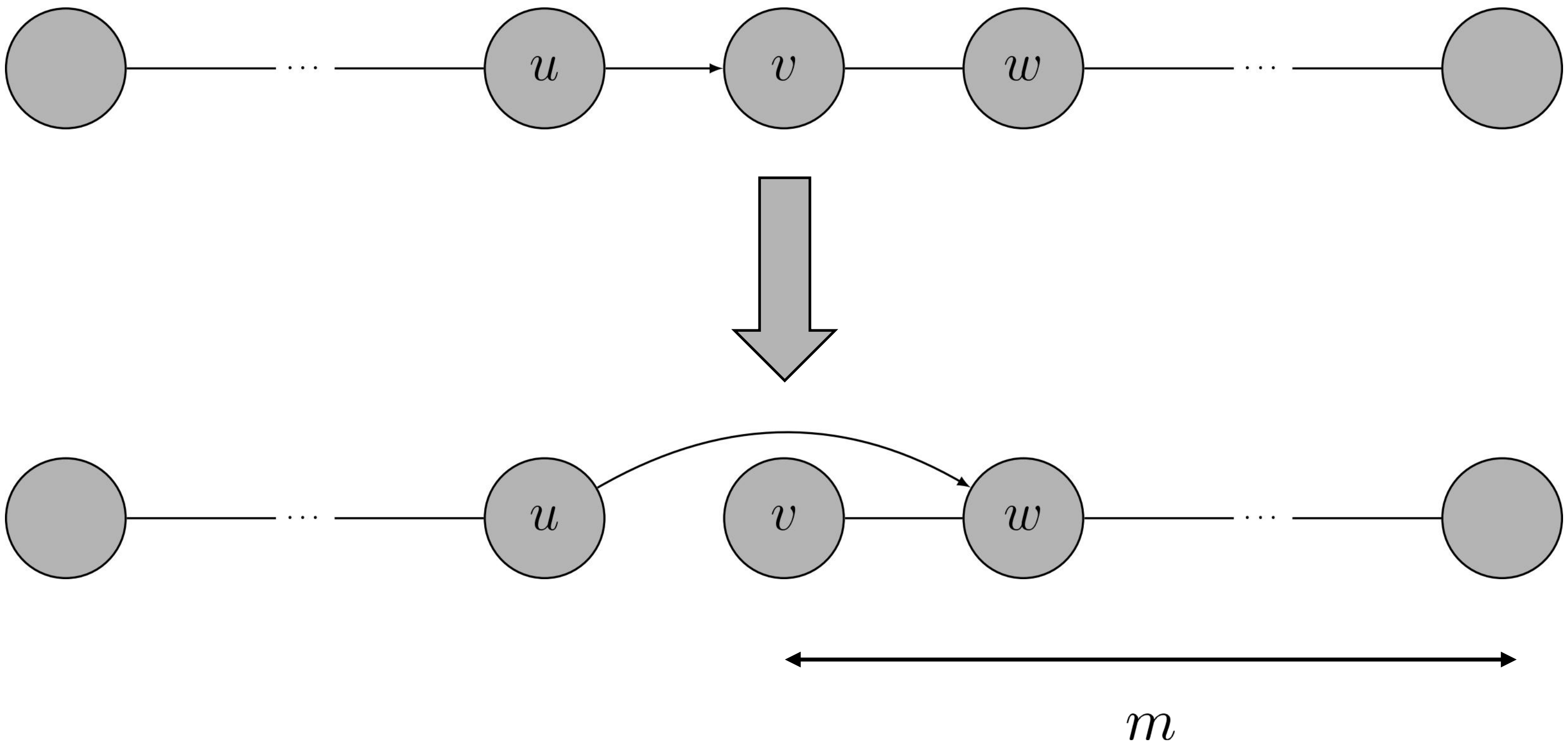
Path graph



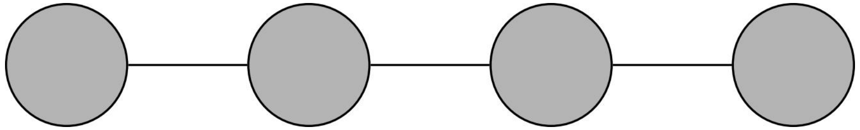
theory
Nash equilibrium
no Nash equilibrium
$n=4$
$n=5$
$n=6$
$n=7$
b
c
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.8
1.0
0
1
2
3
4

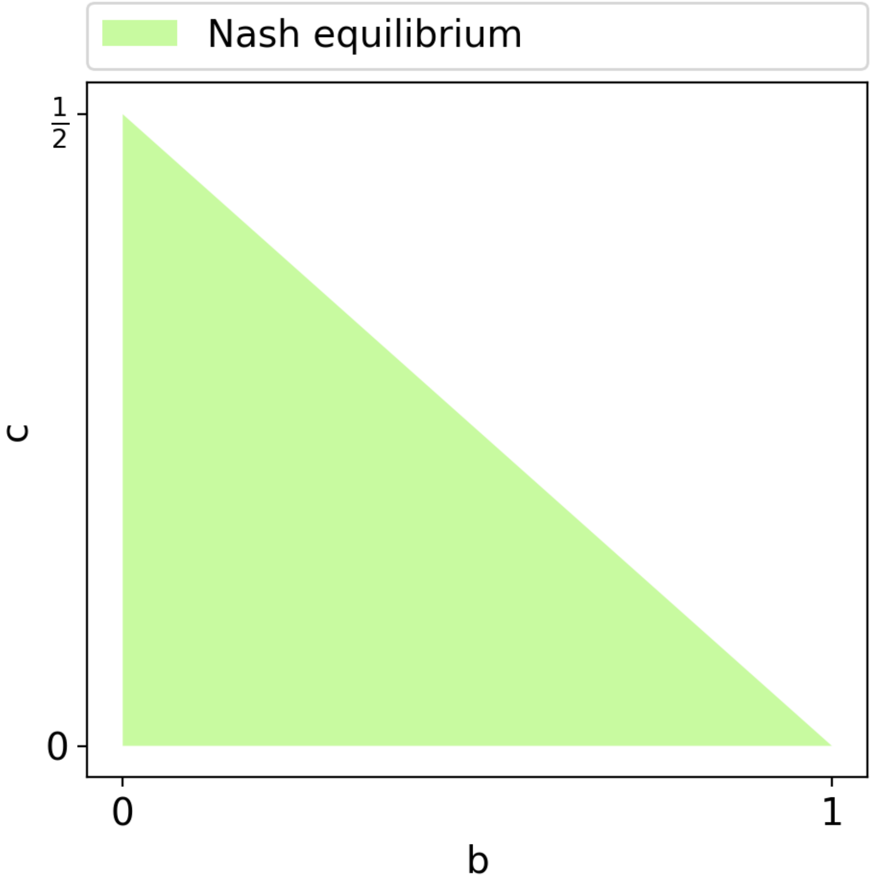
Path graph

$$\Delta\mathrm{cost}_u(s \text{ to } \tilde{s}) = -c \cdot (m-2)$$

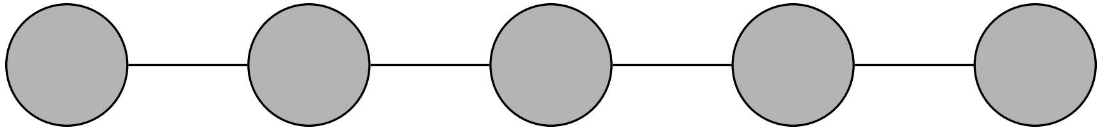


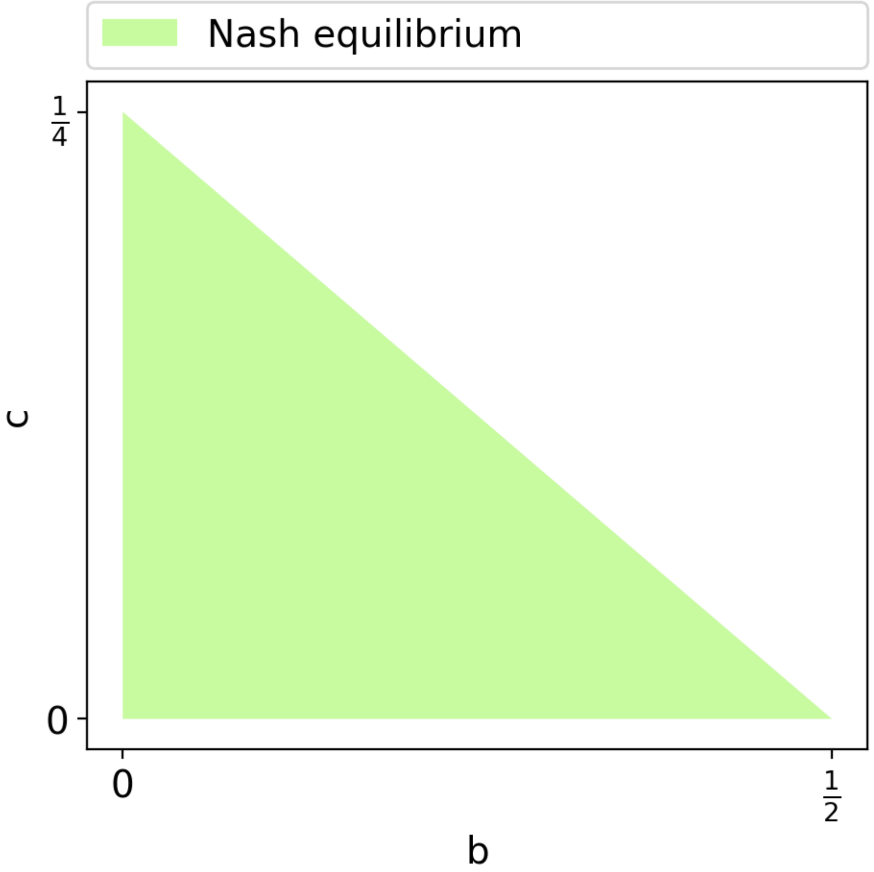
Path graph



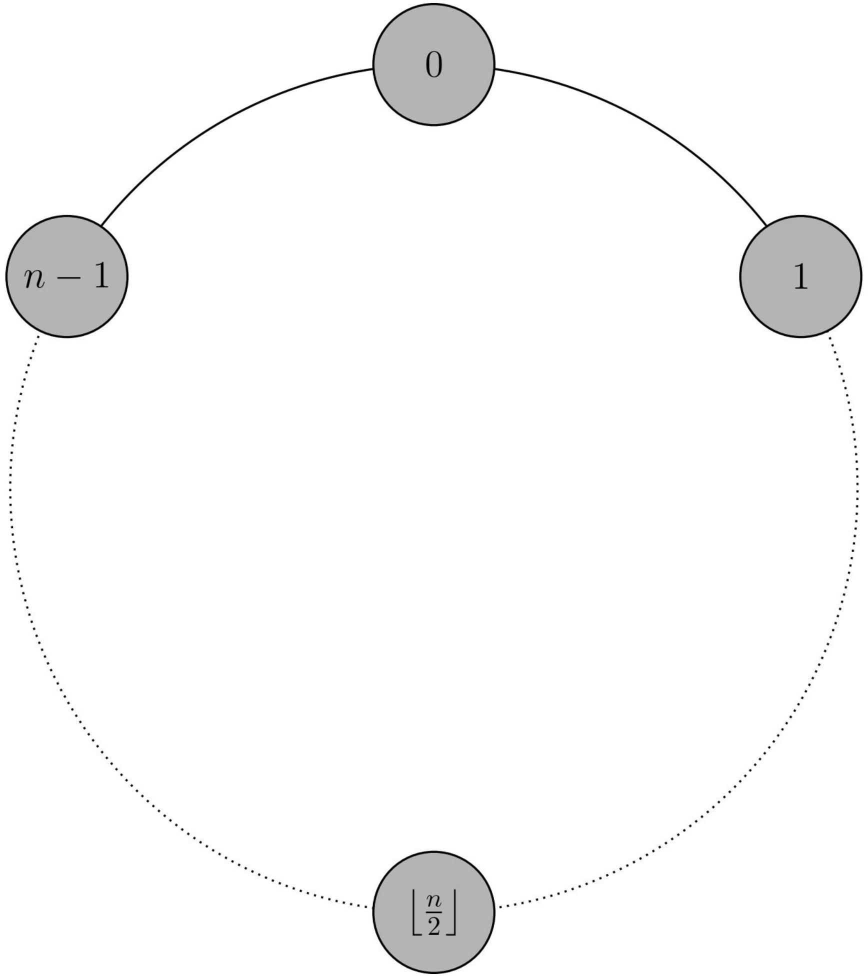


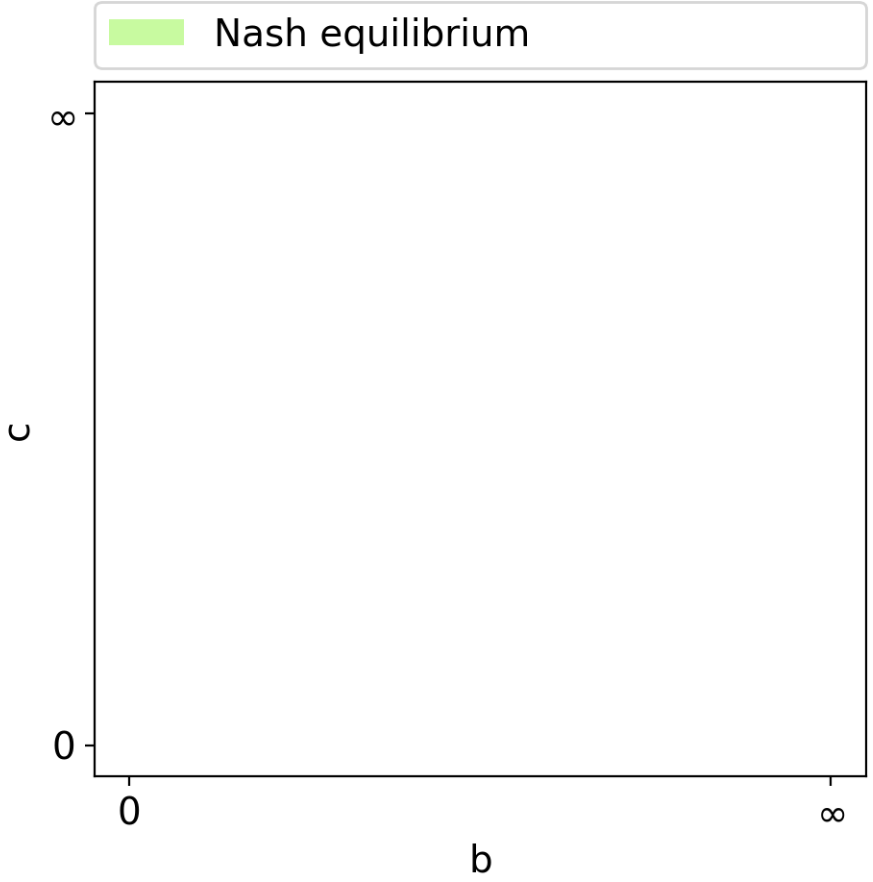
Path graph



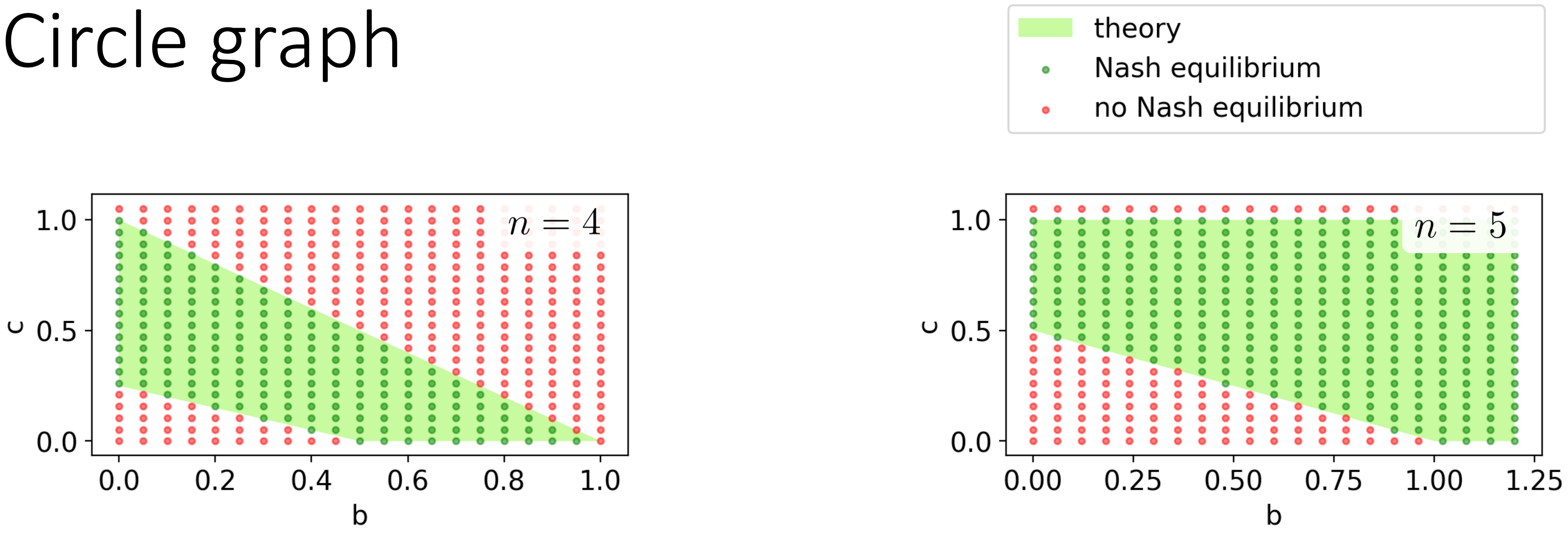


Circle graph

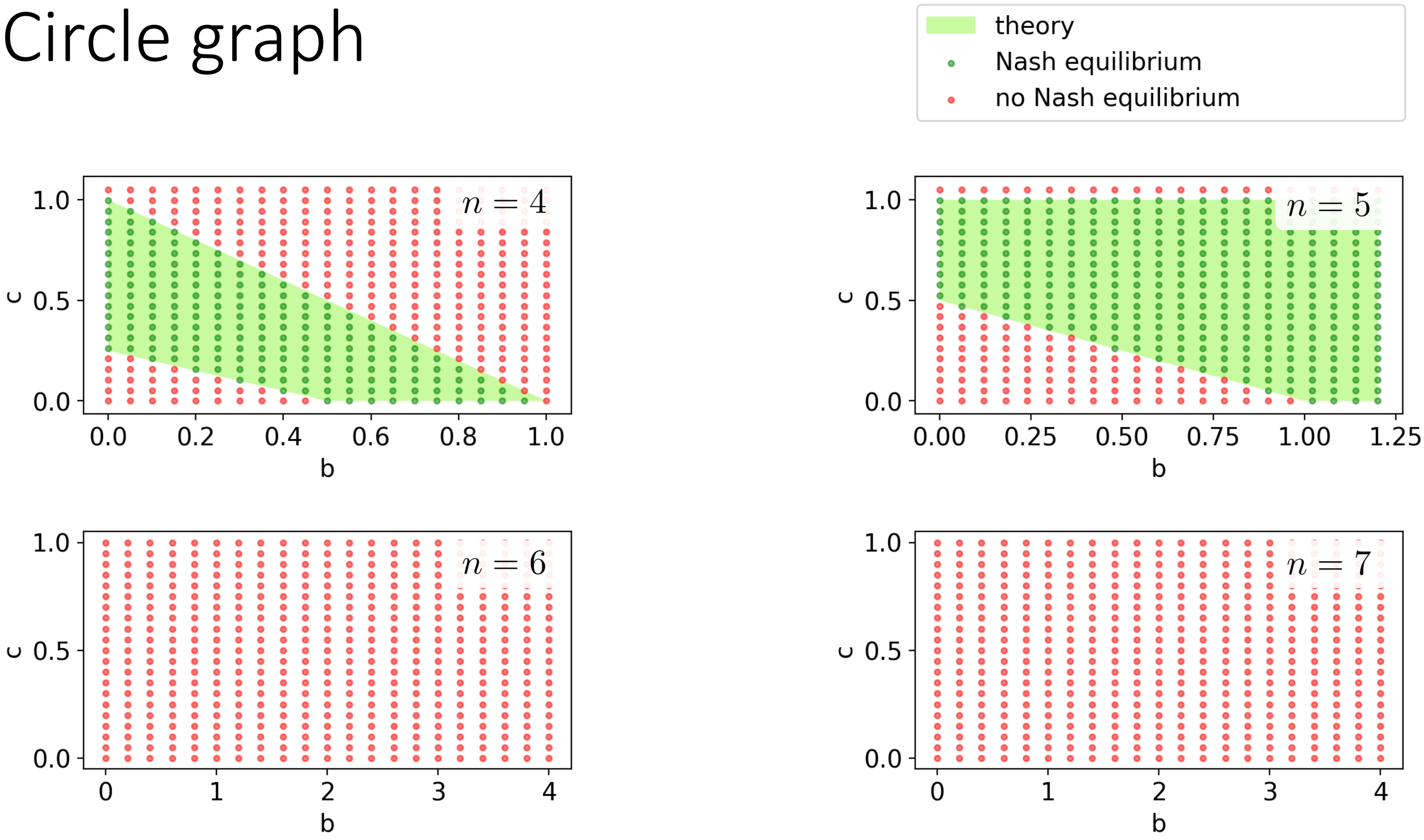




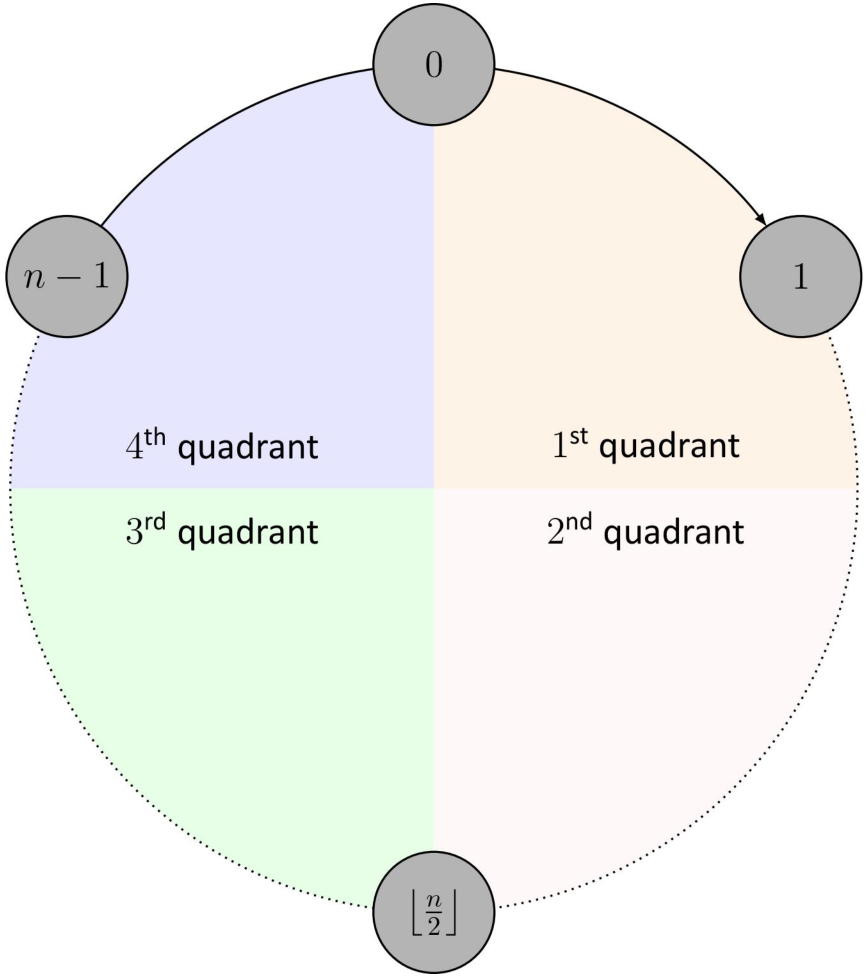
Circle graph



Circle graph



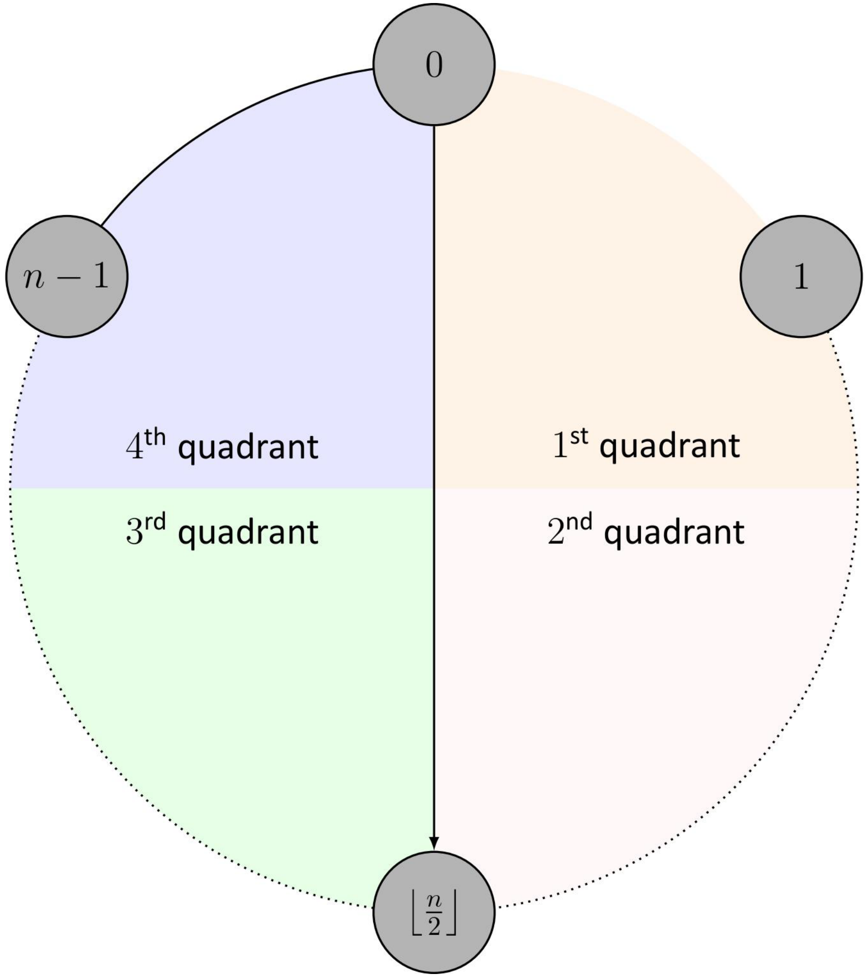
Circle graph



$$\text{betweenness}_0(s) = \frac{3}{4} \cdot n^2 + o\left(n^2\right)$$

$$\text{closeness}_0(s) = \frac{1}{4} \cdot n^2 + o\left(n^2\right)$$

Circle graph

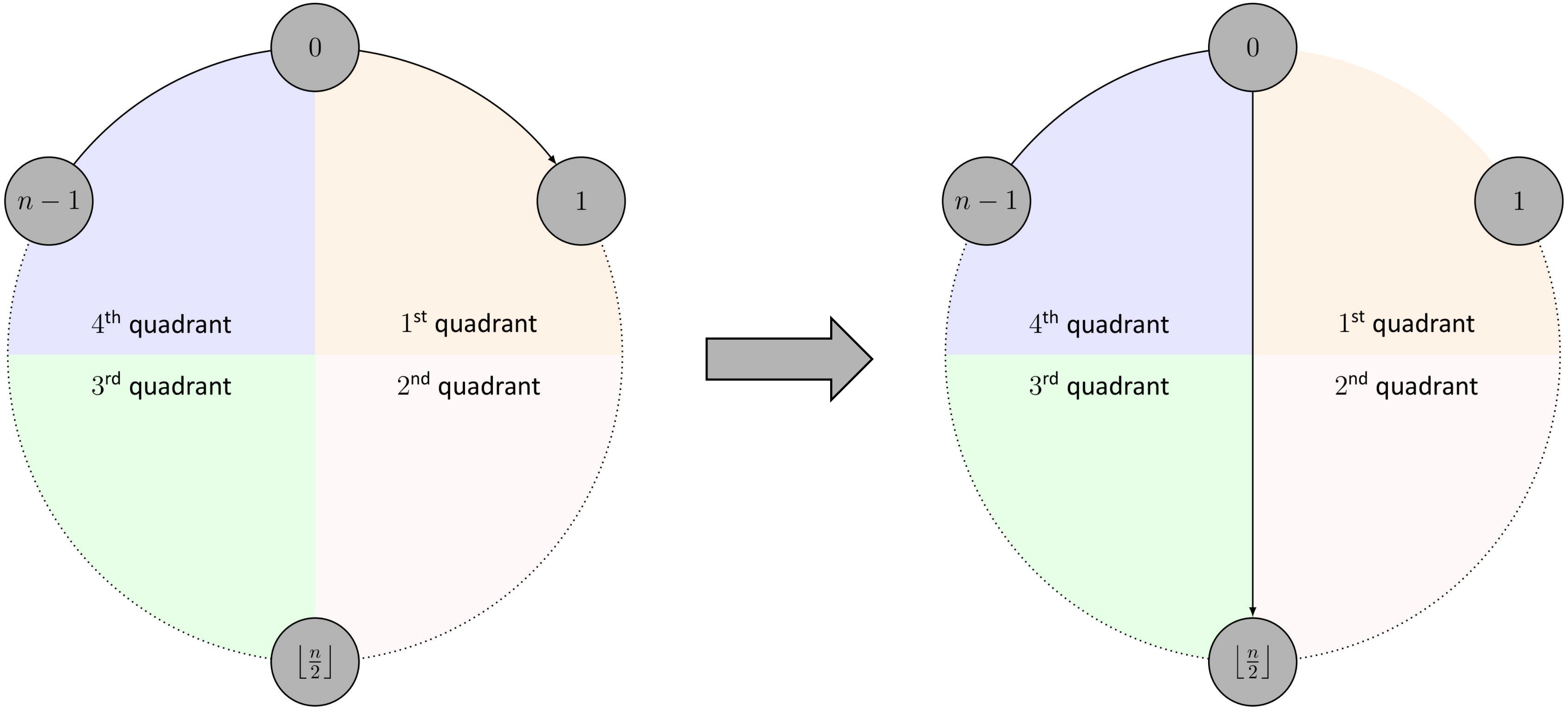


$$\text{betweenness}_0(\tilde{s}) = \frac{11}{16} \cdot n^2 + o\left(n^2\right)$$

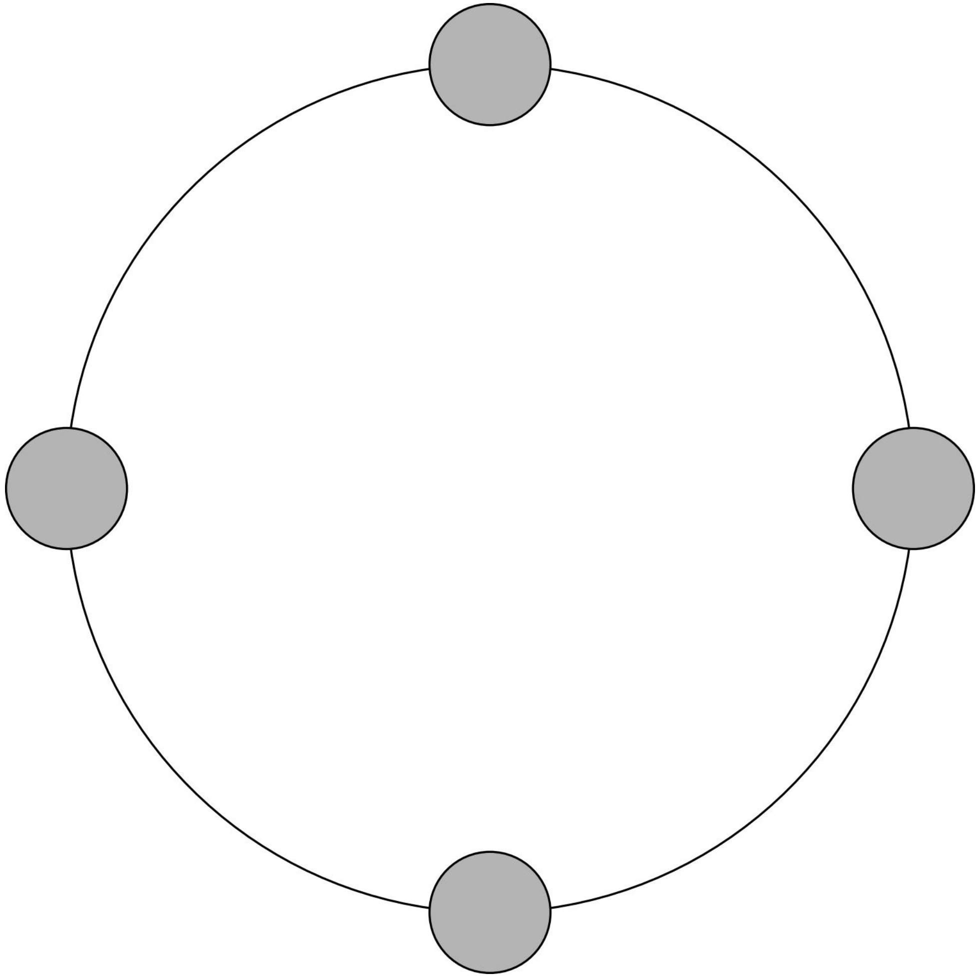
$$\text{closeness}_0(\tilde{s}) = \frac{3}{16} \cdot n^2 + o\left(n^2\right)$$

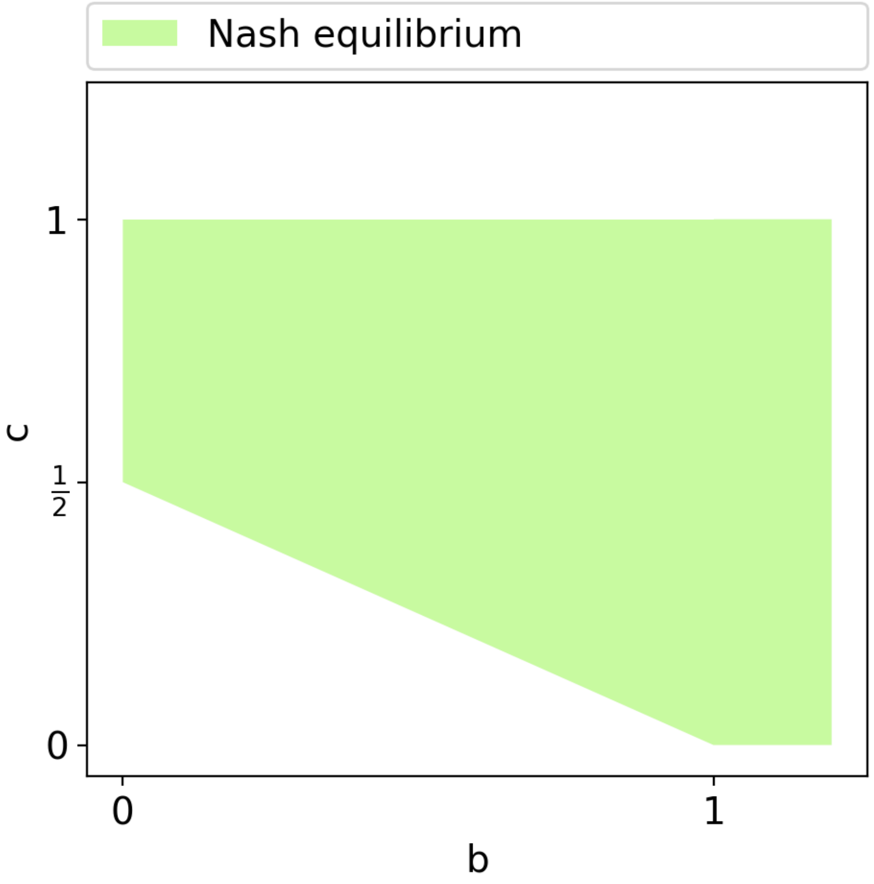
Circle graph

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}) = -\left(\frac{1}{16}n^2 + o\left(n^2\right)\right)(b+c)$$

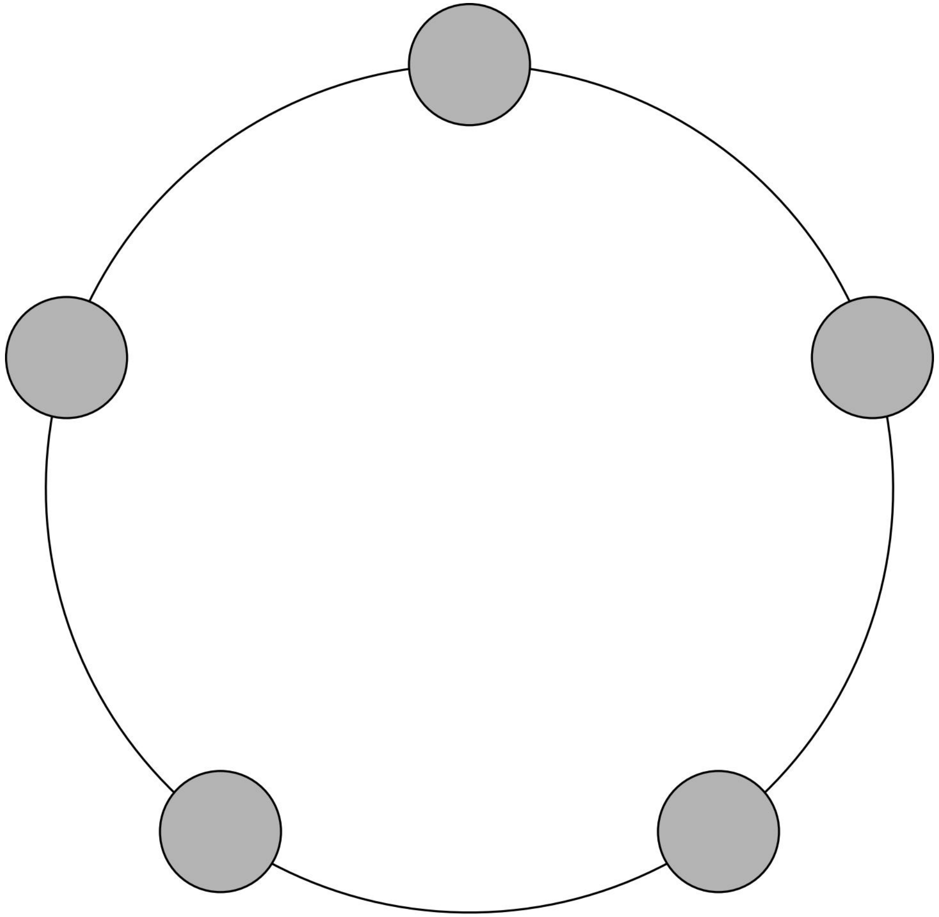


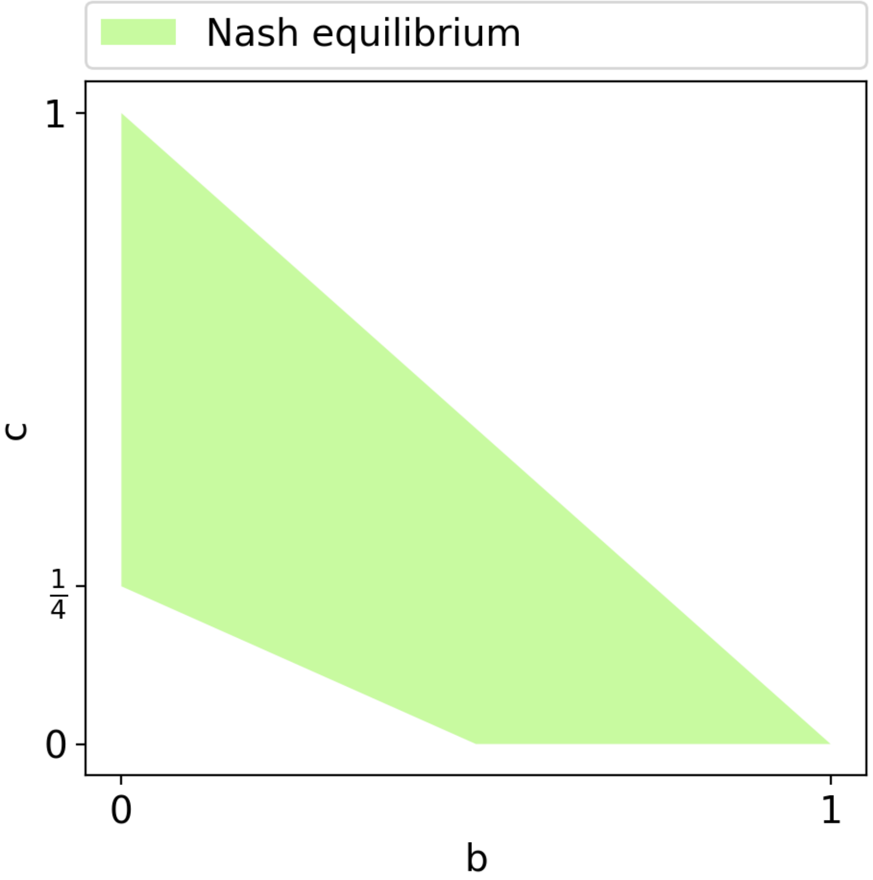
Circle graph



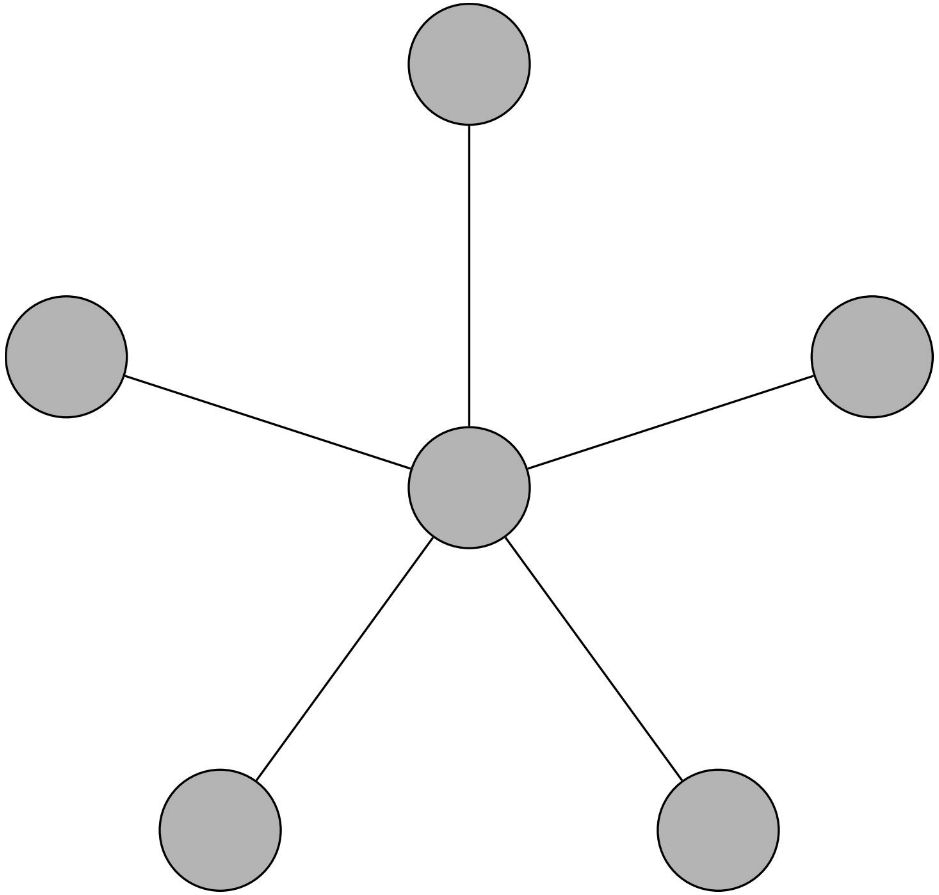


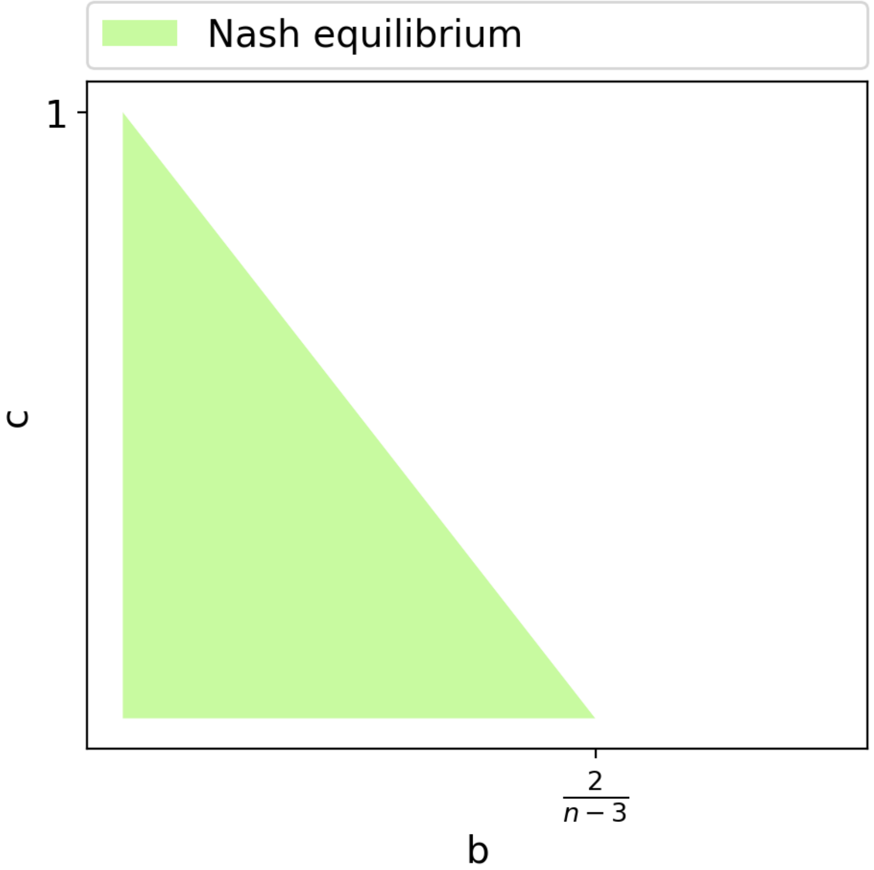
Circle graph



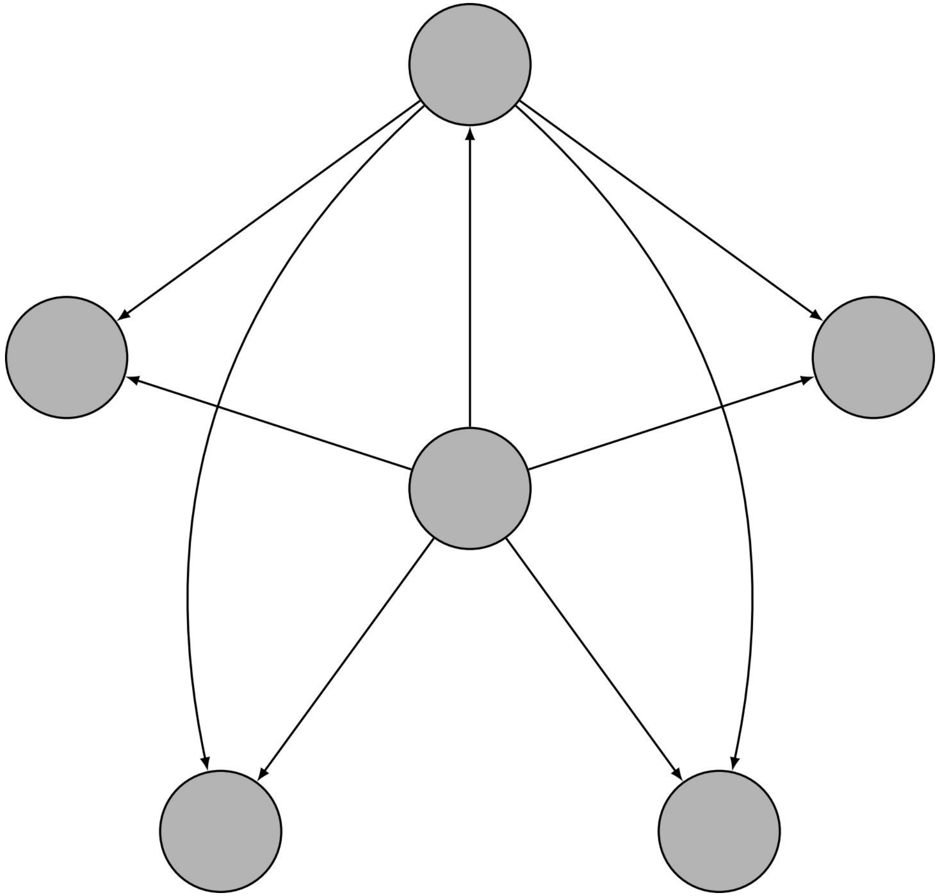


Star graph





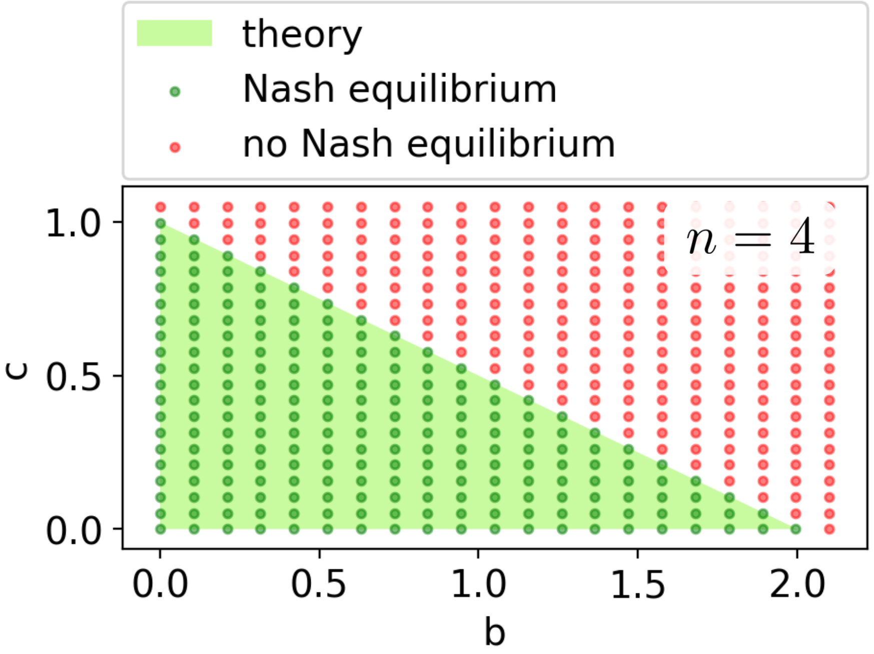
Star graph



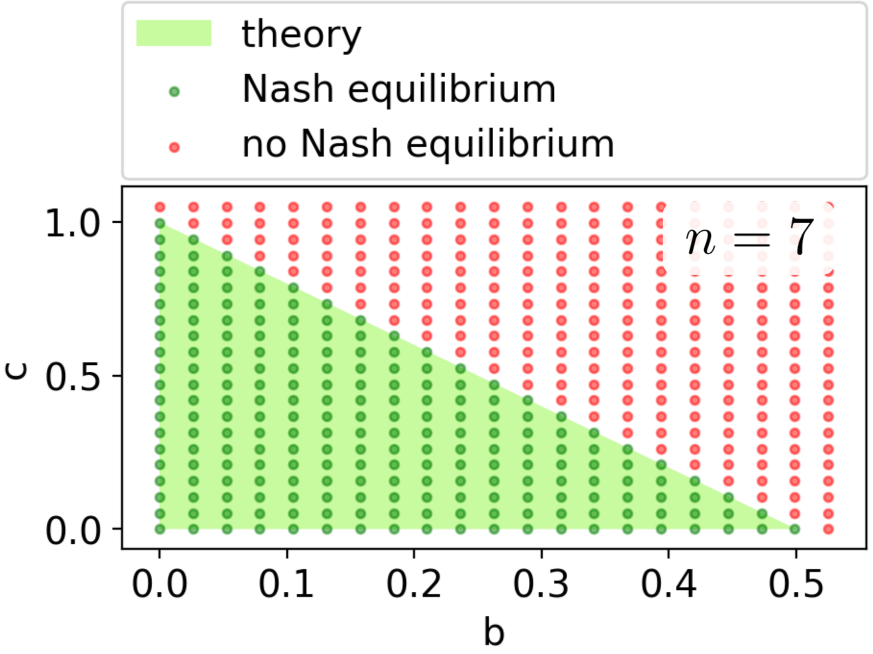
$$\Delta\text{cost} = n - 2 - \frac{(n-2)\cdot(n-3)}{2}b - (n-2)\cdot c$$

$$0 \leq 1 - \frac{n-3}{2}b - c$$

Star graph

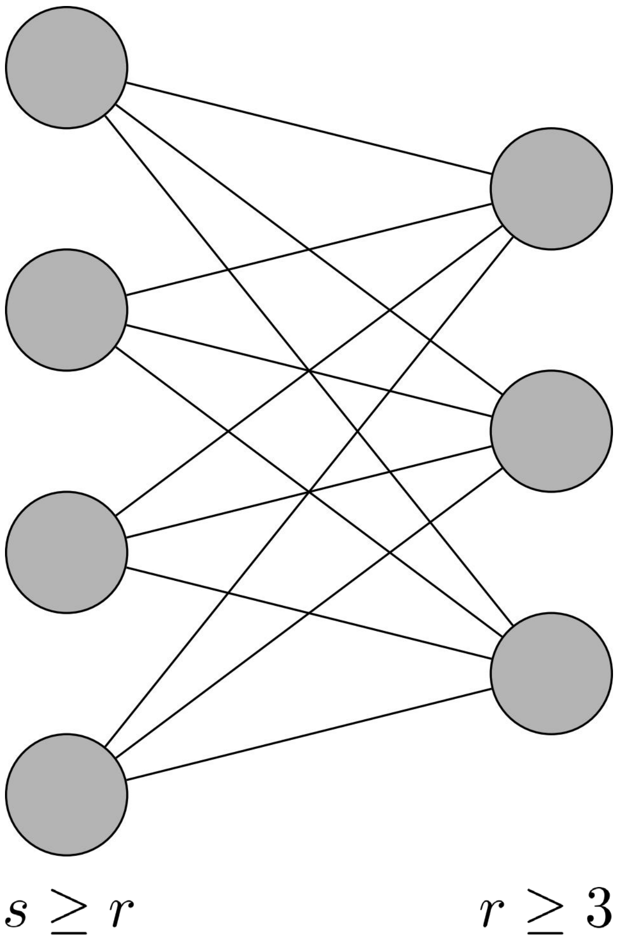


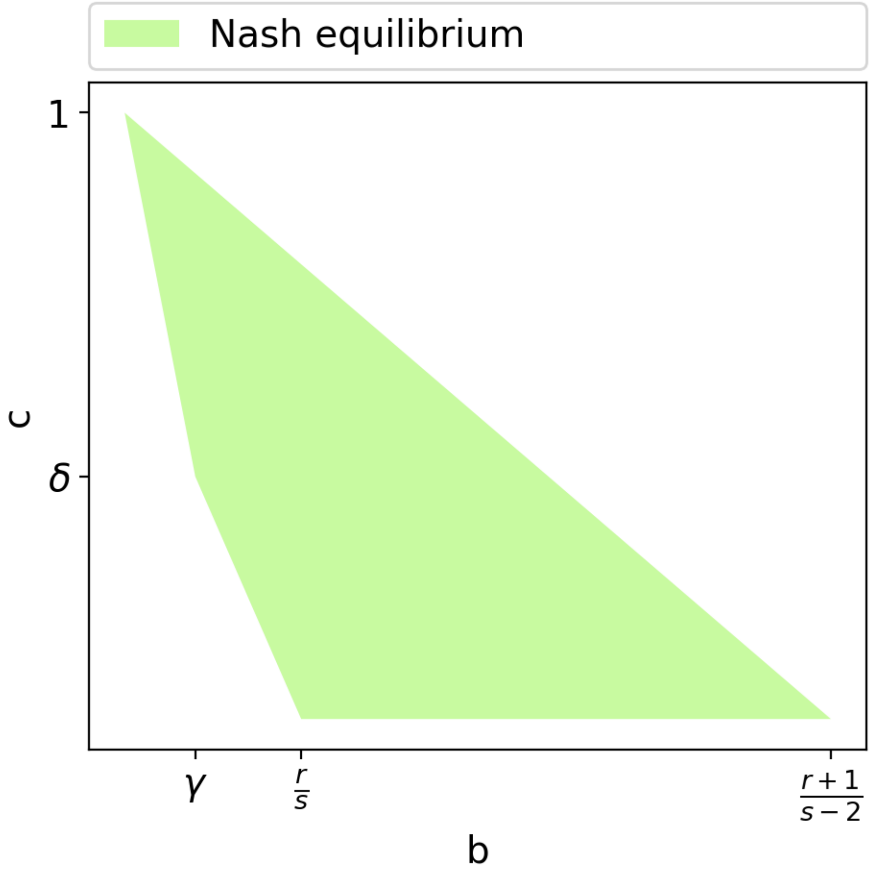
theory
Nash equilibrium
no Nash equilibrium
$n = 4$
1.0
0.5
0.0
c
0.0
0.5
1.0
1.5
2.0
b



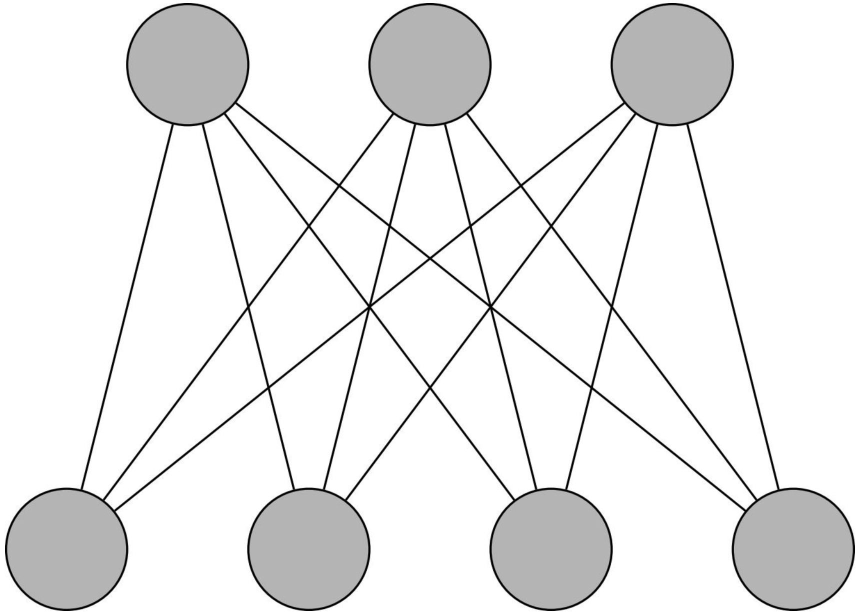
theory
Nash equilibrium
no Nash equilibrium
$n = 7$
1.0
0.5
0.0
c
0.0
0.1
0.2
0.3
0.4
0.5
b

Complete bipartite graph





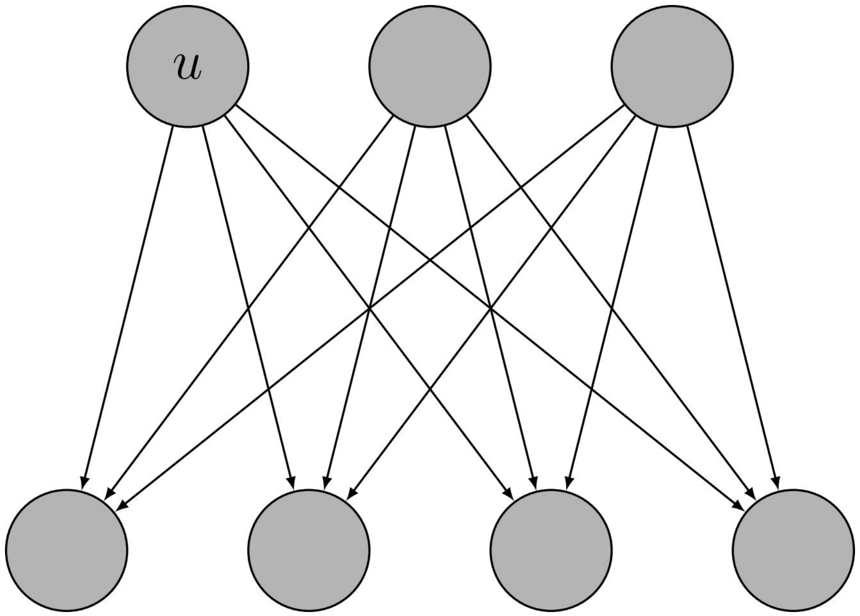
Complete bipartite graph



$r \geq 3$

$s \geq r$

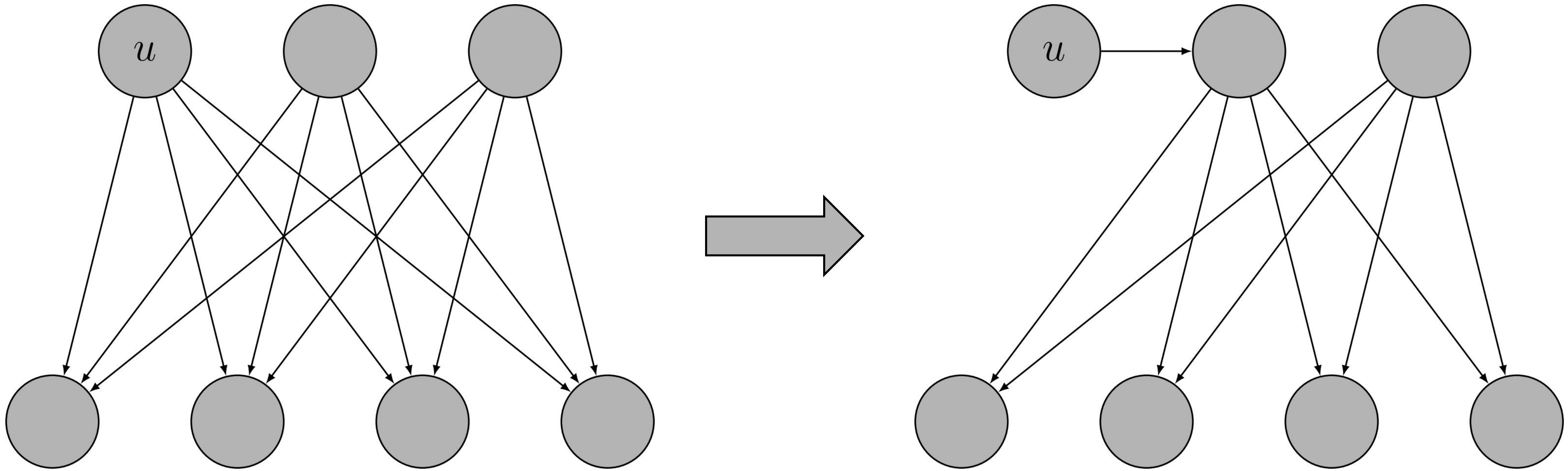
Complete bipartite graph



Complete bipartite graph

$$\Delta\mathrm{cost}_u(s \text{ to } \tilde{s}_1) = -(s-1) + \frac{s\cdot(s-1)}{r}b + (s+r-3)\cdot c$$

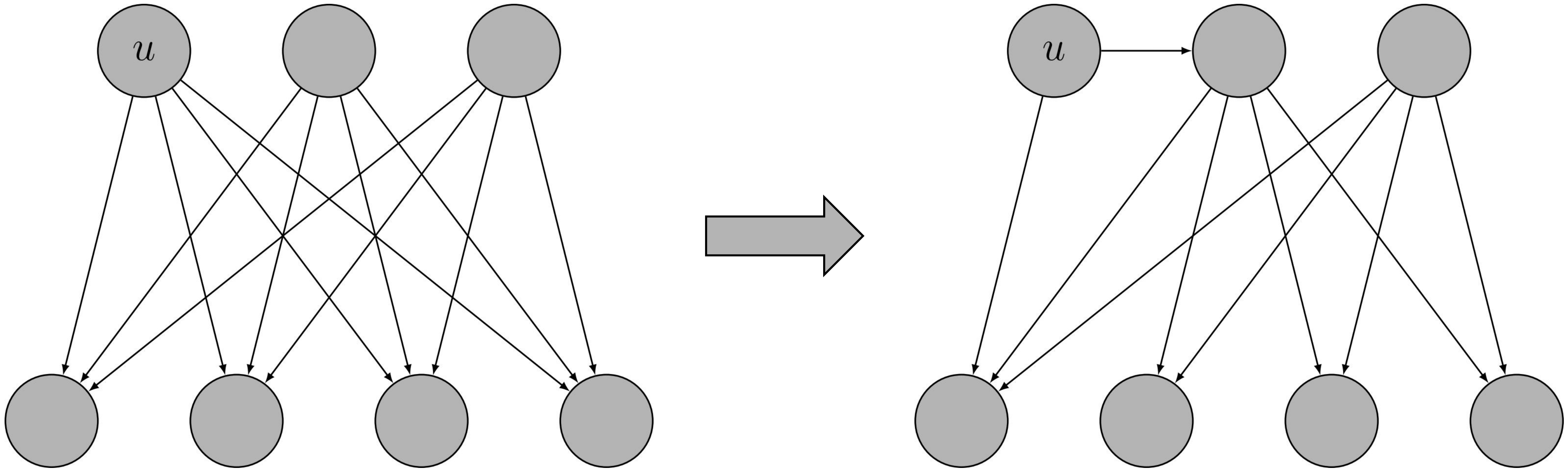
$$1 \le \frac{s}{r}b + \frac{s+r-3}{s-1}c$$



Complete bipartite graph

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}_2) = 2 - s + \left(\frac{s \cdot (s-1)}{r}\right) b + (s-2) \cdot c$$

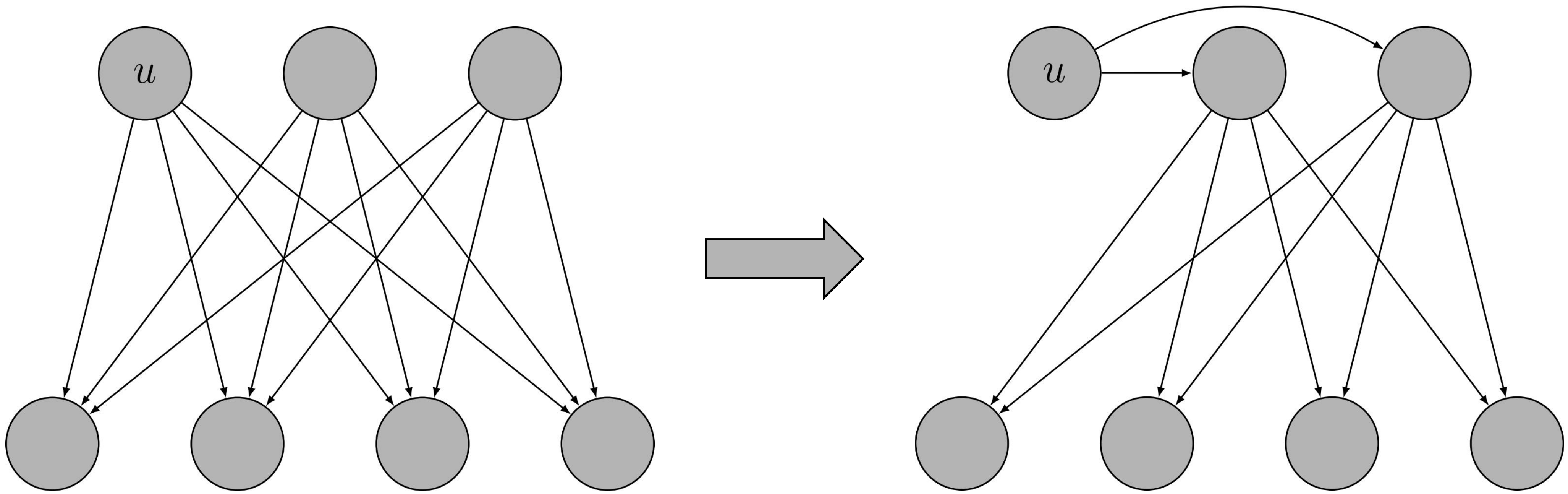
$$1 \leq \left(\frac{s \cdot (s-1)}{r \cdot (s-2)}\right) b + c$$



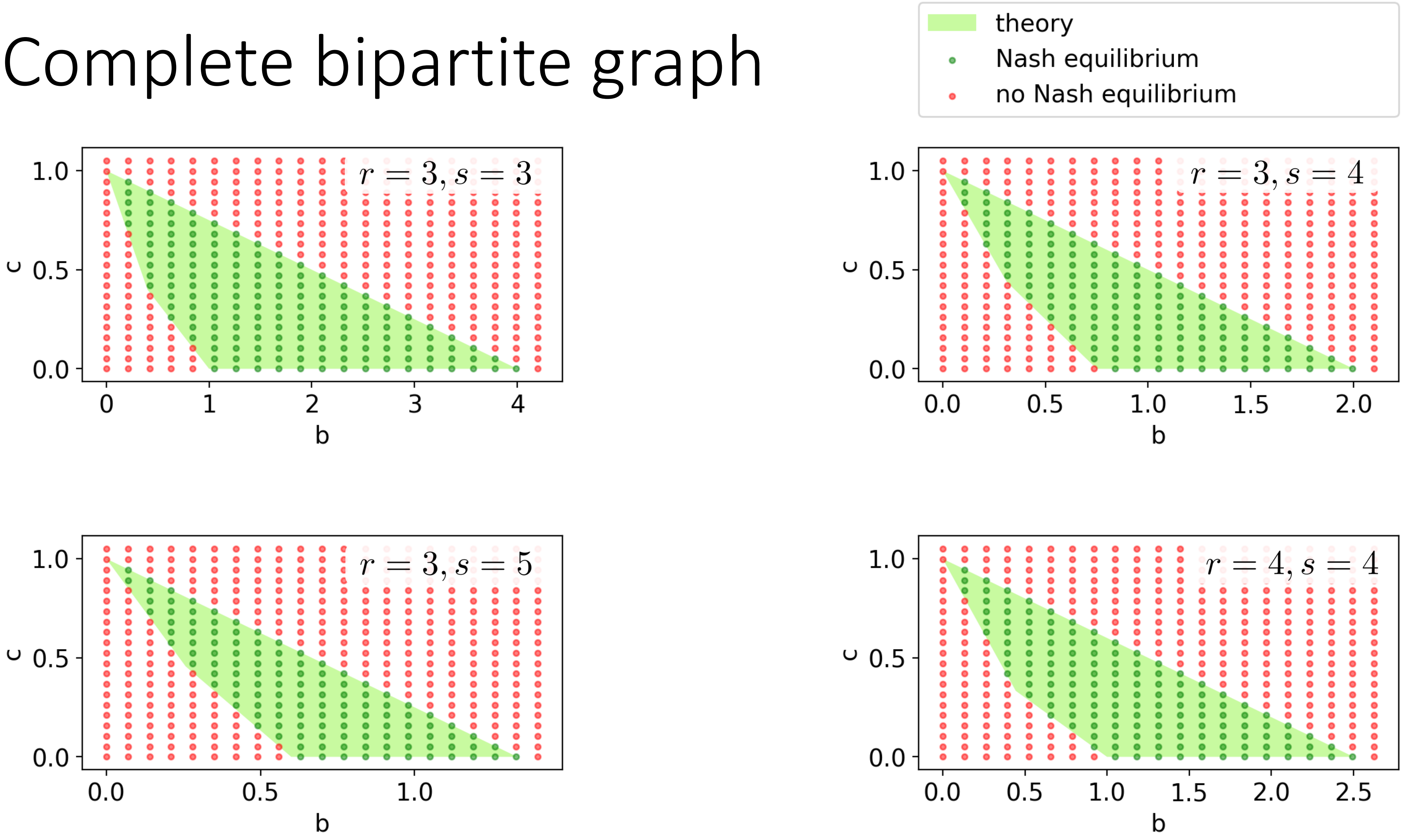
Complete bipartite graph

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}_3) = r - s + 1 + \left(\frac{s\cdot(s-1)}{r} - \frac{(r-1)(r-2)}{s+1}\right)b + (s-r+1)\cdot c$$

$$1 \leq \frac{1}{(s-r+1)}\left(\frac{s\cdot(s-1)}{r} - \frac{(r-1)(r-2)}{s+1}\right)b + c$$



Complete bipartite graph



Price of anarchy ($\mathbf{c} > 1$)

$$c > \frac{1}{2} + b$$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(complete graph)}} = \mathcal{O}(1)$$

Price of anarchy ($\mathbf{c} > 1$)

$c > \frac{1}{2} + b$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(complete graph)}} = \mathcal{O}(1)$$

$b \leq c \leq \frac{1}{2} + b$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(star graph)}} = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + (c + b \cdot (n-1))(n-2)} = \mathcal{O}(1)$$

Price of anarchy ($\mathbf{c > 1}$)

$c > \frac{1}{2} + b$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(complete graph)}} = \mathcal{O}(1)$$

$b \leq c \leq \frac{1}{2} + b$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(star graph)}} = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + (c + b \cdot (n-1))(n-2)} = \mathcal{O}(1)$$

$c < b$

$$\rho(G) = \frac{\text{cost(complete graph)}}{\text{cost(path graph)}} = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + \left(\frac{2}{3}b - \frac{1}{3}c\right) \cdot n \cdot (n-2)} = \mathcal{O}(1)$$

Price of anarchy ($c + b \leq 1/n^2$)

$$\Delta\text{cost}_u(s) > -n^2 \cdot c - n^2 \cdot b + 1$$

spanning trees

$$\text{cost}(s) = \Theta(n)$$

$$\rho(G) = \mathcal{O}(1)$$

Price of anarchy ($\mathbf{c} \leq 1$ & $c + b \geq 1/n^2$)

$$\rho(G) = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + (c - b) \cdot \sum_{u \in [n]} \sum_{r \in [n] - u} (d_G(u, r) - 1)}{n^3 \cdot b + n}\right)$$

Price of anarchy ($\mathbf{c} \leq 1$ & $c + b \geq 1/n^2$)

$$\rho(G) = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + (c-b) \cdot \sum_{u \in [n]} \sum_{r \in [n]-u} (d_G(u,r) - 1)}{n^3 \cdot b + n}\right)$$

$$d_G(u,r) < \Theta\left(\frac{2}{\sqrt{c+b}}\right) \quad \Longrightarrow \quad \rho(G) = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + n^2 \frac{c-b}{\sqrt{b+c}}}{b \cdot n^3 + n}\right)$$

Price of anarchy ($c \leq 1$ & $c + b \geq 1/n^2$)

$$\rho(G) = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + (c-b) \cdot \sum_{u\in[n]} \sum_{r\in[n]-u} (d_G(u,r) - 1)}{n^3 \cdot b + n}\right)$$

$$\mathcal{O}\left(\frac{n^3 \cdot b}{n^3 \cdot b + n}\right) = \mathcal{O}(1)$$

$$\mathcal{O}\left(\frac{n^2 \frac{c-b}{\sqrt{b+c}}}{n^3 \cdot b + n}\right) = \mathcal{O}\left(\frac{c-b}{n^2 \cdot b + 1}\right) = \mathcal{O}(1)$$

⇒

$$\rho(G) = \mathcal{O}(n)$$

$$\mathcal{O}\left(\frac{|E(G)|}{b \cdot n^3 + n}\right) = \mathcal{O}(n)$$