MS&E 339 Fall 2022-2023
Week 3: Algorithms for Decentralized Finance

Ashish Goel, Thanawat Sornwanee

October 24, 2022

Although we know that a mixed-strategy Nash equilibrium always exists when the number of the admissible actions of each agent is finite, it is possible that there can be multiple equilibria with different characteristics, such as different expected utilities for some agents. In such case, we will not be able to know which equilibrium will occur without more details on the system dynamics, such as the equilibrium iteration algorithm and the initialization condition.

Secondly, Nash equilibrium may not yield high welfare as we would like it to do so. This problem can be seen in the well-known prisoner dilemma. A detailed discussion on prisoner dilemma can be founded in "Lecture 1: Games in Normal Form", Lo [1].

The last implication is that it is often not easy to find or evaluate the equilibrium computationally and analytically, suggesting that there may have to be a simplification for the models. However, it is important to note that this simplification in the modelling process can lead to a qualitatively different result.

In this lecture, we will consider a specific game structure that do not have the three aforementioned implication. In order to do so, we, first, should review a special type of game, **"the complete potential game"**.

1 Complete Potential Game

For all s_i, s_i' be strategies for the agent i and for all s_{-i} be strategies for everyone else. If there exists a function ϕ such that

$$\phi\left(s_i', s_{-i}\right) - \phi\left(s_i, s_{-i}\right) = U_i\left(s_i', s_{-i}\right) - U_i\left(s_i, s_{-i}\right),$$

when $U_i(s_i, s_{-i})$ denotes the (expected) utility that agent i will gain when the agent i plays a strategy s_i and other agents play strategies s_{-i} accordingly, we will call a game as a complete potential game, and call the function ϕ as a potential function.

Note that, for any arbitrary game, a potential function may not exist, and, if a potential function exists, it will not be a unique potential function. Specifically, we can consider that a global translation of a potential function will result in another potential function.

One trivial example of a complete potential game is when the utility of each agent is the same for every state of the world.

1.1 Best Response Dynamics

From the following property of the potential function, we can see that every time an agent in the system optimizes its own utility, the potential function will be weakly increased.

If we know that there exists a finite upper bound for the utility attainable for each agent, then the best response strategy will converge to a pure Nash equilibrium.

Note that the upper bound does not have to be a strict upper bound.

In order to understand this behavior, we can consider an equilibrium searching algorithm when each agent takes turn deciding on the best response, We can see that at each decision, the potential function will be weakly increased. Since there is an upper bound, the sequence of the potential function will converge.

Moreover, if the potential function ϕ has a unique global maximum, then there exists a unique Nash equilibrium.

Can we think of an example when a complete potential game does not have a Nash equilibrium? Consider a game where there are 2 agents, the admissible action space for both of them is $\mathbb{N}$, and the utilities of both of them are the sum of the actions. In this case, there is no finite upper bound, making the best response dynamics not converge; both agents will always have incentives to increase their actions.

1.2 Welfare

It is obvious that an arbitrary game may not have a Nash equilibrium that maximized the (expected) welfare.

However, in a complete potential game, if we specify the welfare to be the sum of the utility of each agent (or a monotone transformation of the sum of the utility of each agent), and if a Nash equilibrium exists, then the welfare will be maximized.

2 Simple Model

2.1 Settings & Assumption

2.1.1 Agents & Actions

The network consists of J agents, denoted as $a_1, a_2, \ldots, a_J$.

Each of them is given a trust budget, which can be thought of a monetary budget for an agent to establish a lightning channel in lightning network formation. These trust budgets are denoted as $B_1, B_2, \ldots, B_J$ respectively.

The action for an agent a_j for $j \in \{1, 2, \ldots, J\}$ is the allocation of initial trust capacity from a_j to a_k with $k \in \{1, 2, \ldots, J\} - \{j\}$. Let denote this by $c_{j,k}$, and let $\mathbf{c}_j$ be a vector representing $c_{j,k}$ for all $k \in \{1, 2, \ldots, J\} - \{j\}$.

It is important to note that not all action is admissible. For example, if the agent a_1 has a trust budget $B_1 = 2$, then it cannot establish the initial trust capacities with the agent 2 and the agent 3 such that $c_{1,2} = c_{1,3} = 3$.

Therefore, we have to specify that the set of feasible actions, $\mathcal{A}_j$ is restricted by the (exogenously) allotted trust budget, B_j, of an agent, a_j, such that, for all $j \in \{1, 2, \ldots, J\}$,

$$\mathcal{A}_j = \left\{ \mathbf{c}_j | \sum_{k \neq j} c_{j,k} \leq B_j \right\}.$$

2.1.2 Dynamics & Objective

In the previous subsection, we have seen the basic model of the feasible actions of the model. Next, we have to look into what the objective of each agent will be. To do so, we will first evaluate the dynamics assumption of the model.

Each agent a_j is allowed to transact directly (ie. via direct channel) and will transact to only a small number of nodes. Specifically, a_j will transact to a_k with non-zero transaction rate, $R_{j,k}$, if and only if $k \in T_j \subseteq \{1, 2, \ldots, J\} - \{j\}$.

We assume symmetry of the transaction matrix, so we get that

$$k \in T_j \iff j \in T_k, \text{ and } R_{j,k} = R_{k,j}.$$

The utility for each agent, a_i, is given to be the probability of successful transactions subjected to the dynamics described above. From our steady state analysis of a credit network, we then get that, for each agent a_j, the utility

$$U_j = \sum_{k \in T_j} \left(R_{j,k} \left(1 - \frac{1}{c_{j,k} + c_{k,j} + 1} \right) \right).$$

2.2 Behavior

Let consider the discrepancy of when an agent a_j chooses to deviate from the feasible action $\mathbf{c}_j$ to $\mathbf{c}'_j$ given that other agents still choose the same actions, $\mathbf{c}_{-j}$.

$$
\begin{aligned}
&U_j\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_j\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \\
&= \sum_{k \in T_j} \left(R_{j,k} \left(\frac{1}{c_{j,k} + c_{k,j} + 1} - \frac{1}{c'_{j,k} + c'_{k,j} + 1} \right) \right) \\
&= \frac{1}{2} \sum_{k \in T_j} \left(R_{j,k} \left(\frac{1}{c_{j,k} + c_{k,j} + 1} - \frac{1}{c'_{j,k} + c'_{k,j} + 1} \right) \right) + \frac{1}{2} \sum_{k \in T_j} \left(R_{k,j} \left(\frac{1}{c_{k,j} + c_{j,k} + 1} - \frac{1}{c'_{k,j} + c'_{j,k} + 1} \right) \right) \\
&= \frac{1}{2} \left(U_j\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_j\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \right) + \frac{1}{2} \sum_{k \in T_j} \left(U_k\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_k\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \right) \\
&= \frac{1}{2} \left(U_j\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_j\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \right) + \frac{1}{2} \sum_{k \neq j} \left(U_k\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_k\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \right) \\
&= \frac{1}{2} \sum_{k=1}^{J} \left(U_k\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - U_k\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) \right) \\
&= \frac{1}{2} \sum_{k=1}^{J} U_k\left(\mathbf{c}'_j, \mathbf{c}_{-j}\right) - \frac{1}{2} \sum_{k=1}^{J} U_k\left(\mathbf{c}_j, \mathbf{c}_{-j}\right).
\end{aligned}
$$

Therefore, this is a complete potential game with

$$
\Phi\left(\mathbf{c}_j, \mathbf{c}_{-j}\right) = \frac{1}{2} \sum_{k=1}^{J} U_k\left(\mathbf{c}_j, \mathbf{c}_{-j}\right).
$$

Thus, we can find Nash equilibria by a maximization of the potential. Consider the following problem.

$$
\begin{aligned}
\max_{c_{j,k}; \forall j,k \in \{1,2,\ldots,J\}} \quad & \textstyle\sum_{j=1}^{J} \sum_{k \in T_j} \left(R_{j,k} \left(1 - \frac{1}{c_{j,k} + c_{k,j} + 1} \right) \right) \\
\text{subject to} \quad & \textstyle\sum_{k \neq j} c_{j,k} \leq B_j; \forall j \in \{1, 2, \ldots, J\} \quad \text{(Budget Constraint)} \\
& c_{j,k} \in \mathbb{N}_0; \forall j, k \in \{1, 2, \ldots, J\} \quad \text{(Feasibility Constraint)}
\end{aligned}
$$

This is an integer optimization, which is very hard to work with. However, if we relax the feasibility constraint by allowing any trust capacity $c_{j,k}$ to be a non-negative number, then the problem can be reformulated as a convex optimization problem. Consider a new optimization problem, which can be easily computed.

$$
\begin{aligned}
\min_{c_{j,k}; \forall j,k \in \{1,2,\ldots,J\}} \quad & \textstyle\sum_{j,k \in \{1,2,\ldots,J\}} \frac{R_{j,k}}{c_{j,k} + c_{k,j} + 1} \\
\text{subject to} \quad & \textstyle\sum_{k \neq j} c_{j,k} \leq B_j; \forall j \in \{1, 2, \ldots, J\} \quad \text{(Budget Constraint)} \\
& c_{j,k} \geq 0; \forall j, k \in \{1, 2, \ldots, J\} \quad \text{(Feasibility Constraint)}
\end{aligned}
$$

Apart from that Nash equilibrium can be easily found via convex optimization, we should note that, for all $j, k \in \{1, 2, \ldots, J\}$, a function $\frac{R_{j,k}}{c_{j,k}+c_{k,j}+1}$ is strictly concave in $c_{j,k} + c_{k,j}$.

Since there exists an optimal point, we get that the solution will have a unique $c_{j,k} + c_{k,j}$ for each $j, k \in \{1, 2, \ldots, J\}$.

This suggests that, even though there are several Nash equilibria, every one of them will have the same $c_{j,k} + c_{k,j}$ for all $j, k \in \{1, 2, \ldots, J\}$. Thus, all Nash equilibria are cycle reachable!

2.3 Discussion

Note that the simplified model we discussed above (with the integer constraint being relaxed) has several desirable characteristics:

i) The Nash equilibria can be computed efficiently via convex optimization algorithm.

ii) All Nash equilibria are cycle reachable, which facilitate the analysis of the "initiated" credit network. For example, the probability of fail transaction and the probability of bankruptcy (at time ∞) will be the same for each equilibria.

iii) If we define the welfare to be a sum of individual utility, every Nash equilibria will maximize the welfare.

However, the justification for the model may be difficult. For example, in this model, there is no risk from default.

2.4 Example

To provide a better picture on how several equilibria can exist, we cam consider a case when there are 3 agents, denoted as a_1, a_2, a_3 such that $R_{1,2} = R_{1,3} = R_{2,3} = R_{2,1} = R_{3,1} = R_{3,2} = 1$ and $B_1 = B_2 = B_3 = 1$. It is obvious that the Nash equilibria, which maximize the sum of the utility, will have

$$c_{1,2} + c_{2,1} = c_{1,3} + c_{3,1} = c_{3,2} + c_{2,3} = 1.$$

If we constrain ourselves to only consider integer cases, we can get that there exists 2 equilibria. One of them is when $c_{1,2} = c_{2,3} = c_{3,1} = 1$ and $c_{2,1} = c_{3,2} = c_{1,3} = 0$. The other is when $c_{1,2} = c_{2,3} = c_{3,1} = 0$ and $c_{2,1} = c_{3,2} = c_{1,3} = 1$. The visualization is provided at the figure 1.

3 More Realistic Model

For a more "realistic" model, we can consider the case when each agent a_j carries a risk of default r_j, and these risks are globally known with certainty to everyone in the system. In this specification, we will get that Nash equilibria tend to result in hubs, where everyone should trust the agent with the least risk. This is not a great network topology, since decentralization is lost.

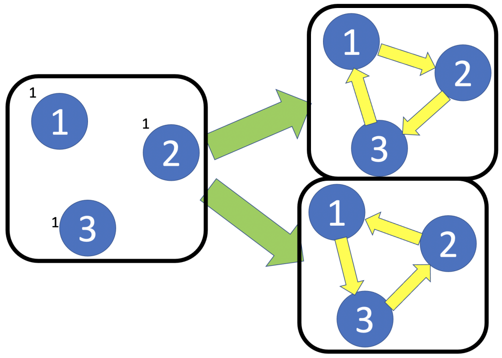

Figure 1: Example of multiple Nash equilibria in a simple system.

One possible research direction is to come up with a model on how the credit network formation is done, and test the hypothesis with the empirical observation of credit networks. For example, the risk default may not be directly known to everyone in the system, but each agent gets a different noisy signal about the default risk of one another.

4 Mechanism Design

As we have seen in the previous section, with some assumptions, the end result of a strategic formation may not yield a "healthy" network (i.e. low liquidity, high centralization, etc.). If we are endowed with a regulatory power, can we enforce some rules of reward and penalty to incentivize the system to create a "healthier" network than that when there is no intervention. For example, can we charge some additional cost of allocating trust with a highly connected node in order to demotivate an agent from choosing to only establish a connection with a "central" node.

However, we have to keep in mind that the power we have is usually limited. In most case, we will assume **"Individual Rationality"**[1], meaning that, although we can force an agent that has already decided to join the system to follow our rules, we **cannot** force it to join in the first place. In other words, if the rules we impose will adversely affect its individual utility such that it is better to stay out of the system. This means that we may not be able to make every agent fully internalize the healthiness of the network, since it may go against individual rationality constraint we have. We will explore more on this concept in the next set of lectures on exchanges.

One possible research direction is then to quantify the healthiness of a network, and to design a regulatory mechanism to nudge the agents within the system to reach a healthy network as desired.

[1]For some application, we may even allow an agent to exit the system after the initialization has been done. The choice of what level of individual rationality to be imposed or whether to impose individual rationality or not is highly dependent on the problem model itself. For example, many taxation designs will not consider individual rationality, since most agents will be better off staying out of the taxation system.

5 Stable Coin

A stable coin is a digital currency whose value is pegged to a fiat currency, such as a national currency. There are primarily 4 potential types of stable coin.

0) **Trust Us:** This system requires other people to trust the value of a stable coin. This is then not often used in a practical setting when people have heterogeneous beliefs.

1) **Partial or Complete Reserve in a Fiat Currency:** In this system, more reserve is required for more stable coin to be issued. The collateral can be in a form of assets with low liquidity but can still back the value of the issued stable coin, which has high liquidity. The provider of a stable coin does direct the redemption and sales for the coin (e.g. Tether). One possible risk of this system is that an inadequate collateral can not only cause runs but also result in inflated value. This is because the circulated amount cannot be adjusted according to the demand-supply, the shift in the demand-supply will then result in a higher change in the equilibrium price.

2) **Partial or Complete Reserve in a Basket of other Crypto-Assets:** In this system, the collateral that back the issuance of new coin will be in a form of a portfolio of other crypto-assets instead.

3) **Algorithmic Stable Coin:** The value of a coin will be maintained by an automated burning or issuing of the basket of crypto-assets when the price is too low or too high. Sometimes, the basket can consist merely a single cryptocurrency issued by the same entity. In such case, the burning process can be successful only when a great portion of the cryptocurrency is owned by the provider.

Open Question 1 Design a stable coin with a credit network.

References

[1] Irene Lo. Lecture 1: Games in normal form, 01 2021.