Concave Pro-rata Games

Nicholas A. G. Johnson Theo Diamandis Alex Evans

nagj@mit.edu tjdiamand@mit.edu aevans@baincapital.com

Henry de Valence Guillermo Angeris

hdevalence@penumbra.zone gangeris@baincapital.com

October 2022

Abstract

In this paper, we introduce a family of games called concave pro-rata games. In such a game, players place their assets into a pool, and the pool pays out some concave function of all assets placed into it. Each player then receives a pro-rata share of the payout; *i.e.*, each player receives an amount proportional to how much they placed in the pool. Such games appear in a number of practical scenarios, including as a simplified version of batched decentralized exchanges, such as those proposed by Penumbra. We show that this game has a number of interesting properties, including a symmetric pure equilibrium that is the unique equilibrium of this game, and we prove that its price of anarchy is $\Omega(n)$ in the number of players. We also show some numerical results in the iterated setting which suggest that players quickly converge to an equilibrium in iterated play.

Introduction

Existing blockchain systems come to consensus on transactions in batches, called blocks. Yet the economic mechanisms those transactions interact with are generally designed to process each individual transaction sequentially, making their behavior reliant on the ordering of transactions within the batch. This abstraction mismatch is the primary source of miner extractable value (MEV), defined as economic value that can be captured by the block proposer (originally the miner) who selects and sequences the transactions to be included in the batch [DGK+20].

However, rather than trying to blind the block proposer, or choose a "fair" ordering (which is difficult, if not impossible, to construct in any direct sense on current systems) within a batch, we could alternatively attempt to design economic mechanisms which do not depend on the order of transactions within a block, and instead, process each batch of transactions 'all at once'. These mechanisms would then be aligned with the actual ordering

1

provided by the consensus mechanism, stepping from one batch of transactions to the next in the same discrete time steps in which consensus happens.

One such mechanism is a 'pro-rata mechanism'. In this mechanism, there is some known notion of value: for example, every user might want to trade some asset A for another, say B, and everyone 'pitches in' some amount of asset A into a pool. After everyone has placed their amounts, the pool, as a whole, is traded on an exchange for some amount of asset B, and the resulting amount of asset B is distributed back to each player, in proportion to how much of asset A each player placed in the pool. It is not difficult to show that such a mechanism has the desired property: the order in which players placed asset A into the collective pool does not change how much of asset B each player receives. Using some ideas from cryptography, this game can additionally be implemented in a way that does not reveal any one player's contributions or identity [Pen], and so may be considered a simultaneous game.

On the other hand, mechanisms of this form often lead to interesting phenomena as users must now consider the possible actions of other users when planning their own actions. A natural framework to study these kinds of problems, where players must reason about the strategies of other players, recursively, is via game theory and the study of the equilibria of games [VNM07]. This paper serves to cleanly set up the game resulting from a pro-rata mechanism in a simple mathematical framework and derive a number of useful results for such games.

This paper. The paper is organized as follows. We introduce the concave pro-rata game in §1 and show a few interesting properties under mild conditions. Such properties include the existence and uniqueness of a symmetric pure strategy equilibrium and an explicit way of efficiently computing this equilibrium by solving a single variable, unimodal optimization problem. We also show some simple bounds for the price of anarchy. In §2 we then describe how this type of game connects to a recent proposal for a batched decentralized exchange. Finally, in §3, we run a number of simulations illustrating the price of anarchy and showing that in the iterated setting agents appear to converge quickly to the specified equilibrium.

1 The concave pro-rata game

We will define the *pro-rata game* with n players as the game with the following payoff for player $i = 1, \ldots, n$:

$$U_i(x) = \frac{x_i}{\mathbf{1}^T x} f(\mathbf{1}^T x). \tag{1}$$

Here, $f : \mathbf{R}_+ \to \mathbf{R}$ is some function satisfying $f(0) = 0$, while $x \in \mathbf{R}_+^n$ is a nonnegative vector whose ith entry is the action performed by the ith player. We will say the game is a *concave pro-rata game* if the function f is a concave function. This game has a simple interpretation: every player 'pitches in' some amount x_i into a pool, totaling $\mathbf{1}^T x$, and the pool pays out $f(\mathbf{1}^T x)$ depending only on the total amount pitched in by all players. The amount paid out by the pool is then distributed among the players in a pro-rata way; *i.e.*, each player i

receives an amount proportional to how much she put into the pool. For the remainder of this paper, we will assume that the function f is concave. We note that concave pro-rata games consist of a special case of aggregative games in which the payoff of each player is a function of their strategy and the sum of the strategies of all players (*cf.*, [Sel70]).

Concavity.   The payoff U_i is concave in the ith entry, holding the remaining entries constant. To see this, first define $y = \mathbf{1}^T x - x_i$ (*i.e.*, y is the sum of all entries of x except the ith entry). Overloading notation slightly for U_i, we have that

$$U_i(x_i, y) = \frac{x_i}{x_i + y} f(x_i + y).$$

We can write $U_i(\cdot, y)$ as the composition of the following two functions

$$U_i(x_i, y) = g(x_i, h(x_i)),$$

where

$$g(x_i, t) = t f\left(\frac{x_i}{t}\right) \qquad \text{and} \qquad h(x_i) = \frac{x_i}{x_i + y},$$

which are defined for nonnegative real inputs. We will use this rewriting to show that this function is concave in x_i, since, using the basic convex composition rules (*cf.*, [BV04, §3.2.4]) it suffices to show that (a) h is concave and (b) g is concave and nondecreasing in its second argument.

First, note that h is (strictly) concave since

$$h(x_i) = 1 - \frac{y}{x_i + y},$$

which is evidently (strictly) concave in x_i since y is a constant. We can see that g is jointly concave in its arguments as it is the perspective transform of the function f, which preserves concavity (*cf.*, [BV04, §3.2.6]). Finally, we need to show that g is nondecreasing in its second argument. To see this, let $0 \le t \le t'$, then we have

$$
\begin{aligned}
g(x_i, t') = t' f\left(\frac{x_i}{t'}\right) = t' f\left(\frac{t}{t'}\frac{x_i}{t} + \left(1 - \frac{t}{t'}\right) 0\right) \\
\ge t f\left(\frac{x_i}{t}\right) + \left(1 - \frac{t}{t'}\right) f(0) = t f\left(\frac{x_i}{t}\right) = g(x_i, t).
\end{aligned}
\tag{2}
$$

The inequality follows from the definition of concavity, while the second-to-last equality follows from the fact that $f(0) = 0$.

Selfish maximum.   The fact that g is nondecreasing in its second argument also has an interesting consequence: a player never does better in the pro-rata game when compared to the 'selfish' version. In other words, for a fixed x_i, player i has the largest payoff when all other players $j \ne i$ have $x_j = 0$. This is easy to see since

$$t = \frac{x_i}{\mathbf{1}^T x} \le 1$$

3

so
$$U_i(x) = g(x_i, t) \leq g(x_i, 1) = f(x_i),$$
where g is as defined above. The inequality follows from the monotonicity of g in its second argument.

Strict concavity. In the important special case where f satisfies
$$f(\alpha t) > \alpha f(t), \tag{3}$$
for every $t > 0$ and $0 < \alpha < 1$, then the function $U_i(\cdot, y)$ is strictly concave in its first argument. (We will show this soon.) Property (3) has the interpretation that any chord of the function, drawn between $(0, 0)$ and any other point on the graph, lies strictly below the function itself. For example, a sufficient condition is that the function f is strictly concave, though this condition is not a necessary one as there are functions which are not strictly concave that satisfy (3). See appendix A for a more general condition.

Since we know that h is a strictly concave function and g is a concave function, we can show that $g(x_i, h(x_i))$ is strictly concave in x_i by showing that g is strictly increasing in its second argument. Strict concavity of g follows from the usual composition rules (see [BV04, §3.2.4]). To show that g is strictly increasing in its second argument, let $0 < t < t'$, then:
$$g(x_i, t') = t'f\left(\frac{x_i}{t'}\right) = t'f\left(\frac{t}{t'}\frac{x_i}{t}\right) > t'\frac{t}{t'}f\left(\frac{x_i}{t}\right) = tf\left(\frac{x_i}{t}\right) = g(x_i, t),$$
where the inequality follows from an application of (3) with $\alpha = t/t'$.

Definitions. For completeness, we state several important definitions [VNM07] from game theory. To each player $i = 1, \ldots, n$, we associate a *strategy*, which is a probability distribution π_i over the possible actions of player i, the nonnegative real numbers. We say a strategy is *pure* if π_i is a deterministic distribution or point mass. In other words, we say a strategy is pure when the probability of choosing a specific action z is always one; *i.e.*, $\pi_i(\{z\}) = 1$ for some $z \geq 0$. Otherwise, we say the strategy is *mixed*.

A *Nash equilibrium* (simply an *equilibrium* from here on out) is a collection of strategies π_i for each player $i = 1, \ldots, n$ such that no individual player can achieve a strictly better outcome by choosing a different strategy. Concretely, let $x_i \sim \pi_i$ be a random variable chosen by player i's strategy (mixed or pure) and let $y_i \sim \pi_{-i}$ be a random variable denoting the sums of random variables from other players' strategies. The collection of strategies (π_i) consists of an equilibrium if, for each player i, we have
$$\mathbf{E}_{x_i \sim \pi_i,\ y_i \sim \pi_{-i}}\left[U_i(x_i, y_i)\right] \geq \mathbf{E}_{x_i \sim \tilde{\pi}_i,\ y_i \sim \pi_{-i}}\left[U_i(x_i, y_i)\right],$$
where $\tilde{\pi}_i$ denotes any strategy. (For the remainder of the paper, we will drop the x_i and y_i in the definition of the expectation to shorten notation.) If the above condition holds with strict inequality for all i except when $\tilde{\pi}_i = \pi_i$, the equilibrium is said to be *strict*. In words, an equilibrium is strict if each player would achieve a strictly worse outcome by choosing a different strategy. In general, we say an equilibrium is pure if all strategies of that equilibrium are pure, and mixed otherwise.

4

Pure equilibria. With those definitions, we note that the strict concavity of $U_i(x_i, y)$ in x_i has an important, direct consequence: every equilibrium of this game is a pure equilibrium. Let $x_i \sim \pi_i$ be any strategy that is not pure, while $y_i \sim \pi_{-i}$ is a random variable denoting the sums of the other players' strategies, then

$$\mathbf{E}_{\pi_i, \pi_{-i}}\left[U_i(x_i, y_i)\right] = \mathbf{E}_{\pi_{-i}}\left[\mathbf{E}_{\pi_i}\left[U_i(x_i, y_i)\right]\right] < \mathbf{E}_{\pi_{-i}}\left[U_i(\mathbf{E}_{\pi_i}[x_i], y_i)\right],$$

where the strict inequality is a result of strict concavity of $U_i(\cdot, y)$ for all y and the fact that π_i is not a point mass. In other words, if $x_i \sim \pi_i$ is a mixed strategy for player i, then this player is always strictly better off playing the pure strategy $\mathbf{E}_{\pi_i}[x_i]$ instead. For the remainder of this paper, we will assume that f is concave and satisfies condition (3), unless otherwise stated. Additionally we will only discuss pure equilibria for the remainder of the paper, as all equilibria must be pure, so talking about a strategy as as a specific action $x_i \in \mathbf{R}_+$ is reasonable.

Extension. A simple immediate extension to the concave pro-rata game is to consider payoff functions of the form:
$$U_i(x) = \frac{c_i x_i}{c^T x} f\left(c^T x\right),$$

for some strictly positive vector $c \in \mathbf{R}_{++}^n$. In this case, all of the same properties given above apply to this slightly more general game, but we will only consider the (often useful) special case where $c = \mathbf{1}$.

1.1   Symmetric pure strict equilibrium

There is a strict, pure equilibrium where all players have equal strategies, given by $x = (q/n)\mathbf{1}$ where q is the optimizer of the following problem:

$$
\begin{aligned}
\text{maximize} \quad & q^{n-1} f(q) \\
\text{subject to} \quad & q \geq 0,
\end{aligned}
\tag{4}
$$

with variable $q \in \mathbf{R}$. We will show some properties of this result first and then show that the pure strategy $x = (q/n)\mathbf{1}$ is, indeed, an equilibrium.

Solution properties. This problem has a (unique) and finite solution $q > 0$ provided $f(z) > 0$ and $f(w) = 0$ for some $0 < z < w$. The fact that $q > 0$ follows by noting that that q must satisfy $q^{n-1} f(q) \geq z^{n-1} f(z) > 0$ since it is optimal. On the other hand, the fact that q is finite follows from the fact that, for any $r \geq w$, we have

$$\frac{w}{r} f(r) + \left(1 - \frac{w}{r}\right) f(0) \leq f(w) = 0,$$

where the first inequality follows from the definition of concavity. Since, by assumption, $f(0) = 0$ and $w/r > 0$, we have that $f(r) \leq 0$ so r cannot be optimal. (In fact, both statements combined prove the stronger fact that $0 < q < w$, but this is not necessary for

what follows.) The uniqueness of the solution to problem (4) follows from observing that the logarithm of the objective function is strictly concave. (This is true since log is strictly increasing and $\log \circ f$ is concave if f is concave.)

Equilibrium properties. The collection of strategies $x = (q/n)\mathbf{1}$ is clearly pure and symmetric. To see that $x = (q/n)\mathbf{1}$ is a strict equilibrium, note that the best response for any player i, when every other player plays strategy q/n is:

$$
\begin{aligned}
&\text{maximize} \quad \frac{x_i}{x_i + (1 - 1/n)q} f(x_i + (1 - 1/n)q) \\
&\text{subject to} \quad x_i \geq 0,
\end{aligned}
\tag{5}
$$

with variable $x_i \in \mathbf{R}$. We will show that the solution to (5) is $x_i = q/n$ in two steps. First, we will show that any solution must have $x_i > 0$ and therefore that the first order optimality conditions applied to the objective suffice. We will then show that $x_i = q/n$ is a solution to the optimality conditions. This result, combined with the fact that the objective is strictly concave, implies that $x_i = q/n$ is the unique solution to the optimality conditions, which proves the final claim that this equilibrium is strict.

To see that any solution to the best response problem (5) must have $x_i > 0$, note that q/n is feasible and achieves an objective value of $f(q)/n > 0$, which is strictly greater than the objective value of zero achieved by $x_i = 0$.

Next, note that $q > 0$ must satisfy the first order optimality conditions of (4):

$$
(n - 1)f(q) + qf'(q) = 0.
\tag{6}
$$

On the other hand, the first order optimality conditions for the objective of problem (5) are that x_i must satisfy (writing $q' = (1 - 1/n)q$ for convenience)

$$
\frac{q'}{x_i + q'} f(x_i + q') + x_i f'(x_i + q') = 0.
$$

Choosing $x_i = q/n$ clearly satisfies this condition, since plugging this value in gives

$$
\left(1 - \frac{1}{n}\right) f(q) + \frac{qf'(q)}{n} = \frac{1}{n}((n - 1)f(q) + qf'(q)) = 0,
$$

as required. Since the objective is strictly concave, this is the unique x_i satisfying the optimality conditions and is therefore the best response. Additionally, while we have assumed that f is differentiable, a very similar proof using subgradient calculus gives an identical result.

1.2   Uniqueness of equilibrium

In fact, it is not hard to show that the symmetric, pure, strict equilibrium is, surprisingly, the unique equilibrium for this game, under the same conditions as (4); *i.e.*, that $f(z) > 0$

and $f(w) = 0$ for some $0 < z < w$. This proof can be broken down into a few steps. First, we will show that any equilibrium x satisfies $f(\mathbf{1}^T x) > 0$ and $x_i > 0$ for each i. This will then be used to show that there is no non-symmetric equilibrium, and, since we know that any symmetric equilibrium must satisfy equation (4), which has a unique solution, we then know that it is the unique equilibrium of this game.

Positivity of equilibria. First we will show that $f(v) > 0$ for every $0 < v < w$. To see this, note that the function f is bounded from below by all of its chords, as it is a concave function. Note that the chord with endpoints $(0, 0)$ and $(z, f(z))$ lies above the x-axis, except at $(0, 0)$, while the chord with endpoints $(z, f(z))$ and $(w, f(w)) = (w, 0)$ lies above the x-axis, except at $(w, 0)$, which leads to the final result.

Now, suppose a collection of (pure) strategies satisfies $f(\mathbf{1}^T x) < 0$. Since $f(0) = 0$, there is some index i such that $x_i > 0$. This implies that $U_i(x_i, \mathbf{1}^T x - x_i) < 0$. But then player i can achieve a payoff equal to 0 by employing the strategy $\tilde{x}_i = 0$, which is strictly better than a negative payoff, so x cannot be an equilibrium.

On the other hand, if a collection of strategies satisfies $f(\mathbf{1}^T x) = 0$, then, from the previous discussion, we must have either $\mathbf{1}^T x = 0$ or $\mathbf{1}^T x = w$. If $\mathbf{1}^T x = 0$, any player i can obtain a strictly positive payoff by playing the strategy $\tilde{x}_i = z$. If, instead, $\mathbf{1}^T x = w > 0$, there is some index i such that $x_i > 0$. We have that the player's payoff is $U_i(x_i, \mathbf{1}^T x - x_i) = 0$ which means that

$$U_i(x_i - \varepsilon, \mathbf{1}^T x - x_i) = \frac{x_i - \varepsilon}{\mathbf{1}^T x - \varepsilon} f(\mathbf{1}^T x - \varepsilon) > 0,$$

for $\varepsilon > 0$ small enough since $f(w - \varepsilon) > 0$, so x is not an equilibrium.

Putting all of these statements together means that any equilibrium x satisfies $f(\mathbf{1}^T x) > 0$ and $\mathbf{1}^T x < w$. To see that any equilibrium must also satisfy $x > 0$, note that if there exists an index i with $x_i = 0$ for a collection of strategies with $f(\mathbf{1}^T x) > 0$, player i can always achieve a strictly positive payoff by playing $\tilde{x}_i = \varepsilon > 0$, for ε small enough.

Symmetry of equilibria. Next, we will show that if x_i is a best response for player i, then any j for which $x_j > x_i$ is not a best response for player j, and vice versa. This will immediately show that any equilibrium must satisfy $x_i = x_j$ (i.e., it is symmetric). We will show this in the case that f is differentiable, but a similar proof holds in the more general case, using subgradient calculus.

Let x be an equilibrium with $x_j > x_i$. Given that x_i is a best response, then the optimality conditions for (5) imply that:

$$\left(\frac{\mathbf{1}^T x - x_i}{(\mathbf{1}^T x)^2} \right) f(\mathbf{1}^T x) + \frac{x_i}{\mathbf{1}^T x} f'(\mathbf{1}^T x) = 0.$$

Since x is an equilibrium, from the previous discussion, we have that $f(\mathbf{1}^T x) > 0$, $x_i > 0$, and $\mathbf{1}^T x > x_i$, so $f'(\mathbf{1}^T x) < 0$. On the other hand, differentiating the objective of the best

response problem (5) for player j gives

$$\left(\frac{\mathbf{1}^T x - x_j}{(\mathbf{1}^T x)^2}\right) f(\mathbf{1}^T x) + \frac{x_j}{\mathbf{1}^T x} f'(\mathbf{1}^T x) < \left(\frac{\mathbf{1}^T x - x_i}{(\mathbf{1}^T x)^2}\right) f(\mathbf{1}^T x) + \frac{x_i}{\mathbf{1}^T x} f'(\mathbf{1}^T x) = 0,$$

where the inequality follows from the fact that, since $x_i < x_j$ we have

$$\frac{\mathbf{1}^T x - x_j}{(\mathbf{1}^T x)^2} < \frac{\mathbf{1}^T x - x_i}{(\mathbf{1}^T x)^2} \quad \text{and} \quad \frac{x_j}{\mathbf{1}^T x} > \frac{x_i}{\mathbf{1}^T x},$$

so x_j cannot be a best response as it is not optimal for (5). The converse case, when $x_j < x_i$ with x_i being a best response, follows from a nearly identical proof. This immediately implies that any equilibrium must be symmetric, so, from the preceding discussion, the unique equilibrium is the one given by the solution to problem (4).

1.3 Equilibrium payoff

Conditioned on each player receiving the same payoff (a fairness condition), the optimal allocation every player would get is

$$\frac{1}{n} \sup f,$$

which is, by definition, at least as good as the equilibrium payoff:

$$\frac{1}{n} f(q),$$

where $q > 0$ is the solution to (4). In fact, we can show that the optimal fair allocation is always strictly better than the equilibrium payoff. To see this, note that, under the assumptions on f introduced above, we know $\sup f$ is achieved by some value $0 < q^\star < w$, satisfying $f'(q^\star) = 0$. Rearranging the first order optimality condition for q in problem (4) gives

$$f'(q) = -(n-1)\frac{f(q)}{q} < 0,$$

for all $n > 1$ since $f(q) > 0$. This means that q does not satisfy the optimality condition for maximizing f, so $f(q) < f(q^\star) = \sup f$. (In fact, this says slightly more: using the concavity of f, we have that $q > q^\star$, i.e., that players 'overpay' at equilibria when $n > 1$.)

Price of anarchy. Given the same assumptions as the beginning of §1.2 on the function f, it is not difficult to show that the price of anarchy satisfies

$$\frac{\sup f}{f(q)} \geq \Omega(n)$$

as the number of players n becomes large. To see this, consider the first order optimality conditions for q (4):

$$(n-1)f(q) + qf'(q) = 0.$$

8

Rearranging and using the fact that f' is nonincreasing and $q \leq w$, we have

$$f(q) = -\frac{qf'(q)}{n-1} \leq -\frac{wf'(w)}{n-1} \leq O\left(\frac{1}{n}\right)$$

whenever $n > 1$. Finally, since we know that $\sup f$ is constant in the number of players, then

$$\frac{\sup f}{f(q)} \geq \Omega(n).$$

(In fact, if the function f' is continuous, it is easy to show that the price of anarchy is actually equal to $\Theta(n)$ by using the fact that $q \uparrow w$ as n becomes large.)

2 Batched decentralized exchanges

In this section, we will show some basic applications of the above properties to a batched decentralized exchange, which we describe below.

Decentralized exchanges. A *decentralized exchange* (or DEX, for short) is a type of exchange that exists on a blockchain. Such exchanges enable any agent to trade currencies without the need for a centralized intermediary. In many cases, these exchanges are organized as constant function market makers (see, *e.g.*, [AAE+22] for a general introduction to this type of exchange), a special type of automated market maker that uses a specific function to price assets.

Batched DEXs. A *batched* decentralized exchange is a DEX where the trades are batched before they are executed. Specifically, the trades are aggregated in some way (depending on the type of batching performed) and then traded 'all together' through the DEX, before being disaggregated and passed back to the users. Though the idea of a batched exchange has been proposed many times in different contexts (see, *e.g.*, [BCS15] and [Wal18]), presently, almost all major decentralized exchanges are not batched. Recent work has suggested that batching is useful for privacy [CAE22] and Penumbra [Pen] has proposed a design for a fully-private decentralized exchange which makes use of batching as a method for avoiding certain information leakage [AEC21]. We describe a very simplified version of this proposal below, which will suffice for our discussion.

Batching design. In this scenario, we have traders $i = 1, \dots, n$ who all wish to trade some amount, say $\Delta_i \in \mathbf{R}$ of asset A for some other asset, which we will call asset B. In this case, negative values of Δ_i denote that trader i wishes to receive some amount of asset A (and will instead tender asset B to the protocol). For convenience, we will assume that $\mathbf{1}^T \Delta > 0$, *i.e.*, on net, traders want more of asset B than asset A. The batching protocol of penumbra first clears all trades to get a nonnegative vector of 'residual' trades $\Delta' \in \mathbf{R}^n_+$ with $\mathbf{1}^T \Delta = \mathbf{1}^T \Delta'$. (In other words, the protocol does not generate debts in any one side.) We can view Δ' as the

9

'excess demand' for asset B over A and leave the mechanism for constructing Δ' otherwise unspecified, requiring only the additional condition that, if $\Delta \geq 0$, then $\Delta' = \Delta$. (This condition can be roughly stated as: if the only trades are due to excess demand, then no clearing happens.) The protocol then pools the residual demand, $\mathbf{1}^T\Delta'$ and trades it against a constant function market maker, represented by some function g, to receive $g(\mathbf{1}^T\Delta')$ of asset B, which it then distributes to each agent i in a pro-rata way, leading to an identical form to that of the pro-rata payoff (1) with $x = \Delta'$. Constant function market makers always have concave g, known sometimes as the *forward exchange function* (*cf.*, [AAE$^+$22, §4]), with $g(0) = 0$, and, in many practical cases, these functions are strictly concave.

2.1 Arbitrage

A common way of analyzing markets is through the lens of *arbitrage*: the ability to exploit price differences in order to make essentially risk-free profit. From before, we will write g for the forward exchange function of a constant function market maker, used by the batching design presented above.

Existence. Assuming g is differentiable at 0, we can interpret $g'(0)$ as the marginal amount of asset B that one would receive for a marginal amount of A. (The function g is often not differentiable at 0, but is one-sided differentiable at 0^+, which suffices.) If $g'(0)$ is larger than the price of an external market, say $c > 0$, then anyone who can directly trade with g can make risk-free profit by trading some (potentially small) amount, $t > 0$ of asset A for $g(t)$ of asset B, and then sell this amount of asset B to get $g(t)/c - t > 0$ of profit. (One simple way to see this is true is to use the definition of a derivative on $g(t)/c$ and send $t \downarrow 0$.)

Optimal arbitrage. Since an agent can make risk-free profit in these cases, it is reasonable to ask: what is the maximum amount of profit an agent can make with this strategy? This is known as the *optimal arbitrage problem*, written:

$$\begin{array}{ll} \text{maximize} & g(t) - ct \\ \text{subject to} & t \geq 0, \end{array}$$

with variable $t \in \mathbf{R}$. From before, if we know that $g'(0) > c$, then this problem has an optimal value that is strictly positive. If g is differentiable, the optimal solution $t^\star$ satisfies

$$g'(t^\star) = c,$$

which we can see from the first-order optimality conditions for this problem. This has the interpretation that the marginal price of the CFMM after the trade $t^\star$, given by $g'(t^\star)$ should be equal to the price of the external market, which we defined to be c.

The (aggregated) arbitrage game. In the batched exchange above, arbitrageurs cannot directly trade with the constant function market maker, but must instead go through the

batching process. Assuming there are n arbitrageurs competing to maximize their profit, the next question is: what are the properties of this game? Defining

$$f(t) = g(t) - ct,$$

then this game is a concave pro-rata game with function f, since the payoff (1) for player i is

$$U_i(x_i, y_i) = \frac{x_i}{x_i + y_i} f(x_i + y_i) = \frac{x_i}{x_i + y_i} g(x_i + y_i) - cx_i.$$

Note that this is exactly the amount received from the DEX with forward exchange function g, minus the cost of trading x_i with the external market, for player i. This game inherits all of the properties derived in §1. We show some numerical simulations of iterated behavior for some utility functions of this form in the next section.

3 Numerics

The results of §1 provide insight into the equilibrium behavior of concave pro-rata games. Here we explore the transient behavior of such games through simulation.

Game setup. Suppose that the game is played iteratively, and, at each iteration t, player i chooses some action x_i^t as the best response to the actions chosen by the other players in the previous round (denoted as x_{-i}^{t-1}), possibly subject to additional constraints. We consider the following scenarios:

1. At iteration t, player i takes action equal to the best response to x_{-i}^{t-1}.

2. At iteration t, player i takes action equal to the best response to x_{-i}^{t-1} subject to a budget constraint ($x_i^t \in [0, M_i]$).

Payoff functions. For these simulations, we use functions f of the form $f(t) = g(t) - ct$ where $c > 0$ and $g(t) = \frac{\gamma R_2 t}{R_1 + \gamma t}$ with $0 < \gamma \le 1$, $R_1, R_2 > 0$. The function $g(t)$ is the forward exchange function for a Uniswap V2 swap pool with reserves $R \in \mathbf{R}_+^2$ and fee parameter γ when asset 1 is being tendered and asset 2 is being received. This setting simulates n arbitrageurs competing to maximize their profit, where c denotes the external market price of asset 2. For simulations using a somewhat more simple payoff function, see appendix §C. Note that f is strictly concave and therefore satisfies condition (3), and clearly $f(0) = 0$.

Shared equilibrium. The (unique) symmetric pure equilibrium strategy is the solution to problem (4). This is easy to compute using the first order optimality conditions for problem (4) given in (6). Plugging in this particular form of f, we obtain the following quadratic equation:

$$(cn\gamma^2)q^2 + q(\gamma^2 R_2 + 2cnR_1\gamma - \gamma^2 nR_2) + (cnR_1^2 - \gamma nR_1R_2) = 0. \tag{7}$$

The equilibrium is then given by $x_i = q/n$, for each player $i = 1, \ldots, n$ where q denotes the positive root of (7).
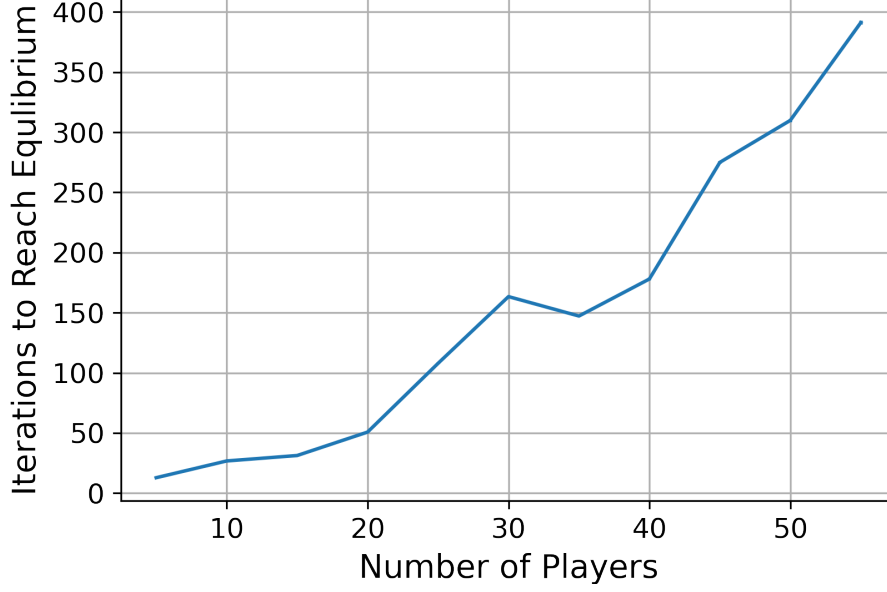
Figure 1: Number of iterations to reach equilibrium versus the number of players in Scenario 1.

Best responses. The best response of player i, given the budget constraint $0 \leq x_i \leq M_i$ and other players' strategies $y_i = \mathbf{1}^T x - x_i$, is given by

$$
\begin{aligned}
\text{maximize} \quad & U(x_i, y_i) \\
\text{subject to} \quad & x_i \in [0, M_i],
\end{aligned} \tag{8}
$$

with variable $x_i \in \mathbf{R}$. This is a single-variable convex optimization problem that is easily solved in practice by any number of off-the-shelf packages [DB16, OCPB16]. When x_i is unconstrained, the optimal value of (8) is given by

$$
x_i = \frac{1}{\gamma} \left(\sqrt{\frac{\gamma R_1 R_2 + \gamma^2 R_2 y}{c}} - R_1 \right) - y
$$

For more details, the code is available at

`github.com/bcc-research/penumbra-arb/experiments/transient_sims.ipynb`

Simulation results. In our simulations, we fix $\gamma = 0.99$, $R_1 = 200$, $R_2 = 250$, and $c = 1$. We average each reported value over 100 trials. In figure 1, the initial strategy of each player is drawn uniformly at random from the interval $(0, w/n)$, where w is a value such that $f(w) = 0$.
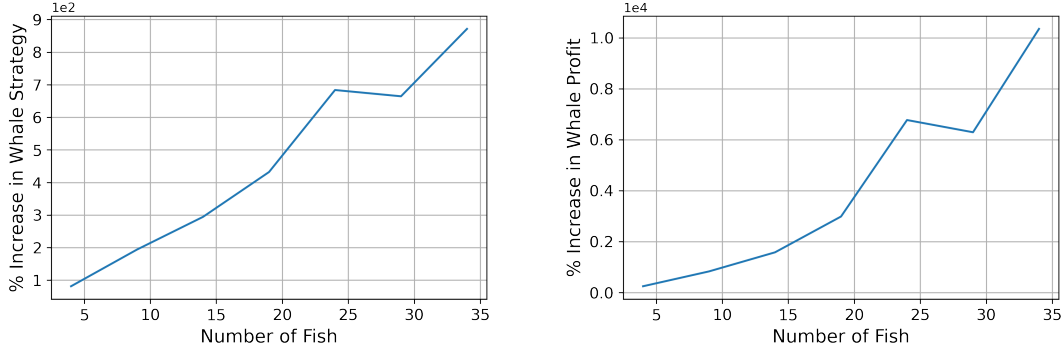
Figure 2: Percent increase in whale strategy and whale profit versus the number of fish when compared to the unconstrained equilibrium strategy and profit.

Figure 1 illustrates that the number of iterations needed to reach the unique equilibrium, in the absence of budget constraints, scales superlinearly in the number of players. We define the number of iterations to reach equilibrium as the number iterations until the strategy of every player is equal to the unique equilibrium up to the first decimal place; *i.e.*, the first round t such that

$$\max_i |x_i^t - x^\star| < 0.1,$$

where $x^\star$ denotes the equilibrium strategy.

In figure 2, we consider the setting where there is one player who has unlimited budget (whom we will call a *whale*) and all remaining players have some budget $M_i < q/n$ (these players are referred to as *fish*). The budgets of the fish are drawn uniformly from the interval $M_i \sim [0, q/n]$ and the initial strategy of each fish is drawn uniformly at random from the interval $[0, M_i]$. The equilibrium strategy chosen by the fish is to use their entire budget, while the whale chooses a strategy in excess of the unconstrained equilibrium strategy and is, as a result, able to extract greater profit. Figure 2 illustrates that the whale chooses an increasingly large strategy and receives an increasing profit as the number of fish increases.

Price of anarchy. In §1 we established the order of growth of the price of anarchy. Here we illustrate the price of anarchy numerically for the specific family of payoff functions introduced previously in this section. We again fix $\gamma = 0.99, R_1 = 200, R_2 = 250$ and $c = 1$. The left plot of figure 3 illustrates the optimal payoff function and the equilibrium payoff function as a function of the number of players n while the right plot of figure 3 illustrates the price of anarchy as function of n.

4   Conclusion

We introduced concave pro-rata games and established several useful properties under relatively mild conditions. In particular, we showed the existence of a unique equilibrium that
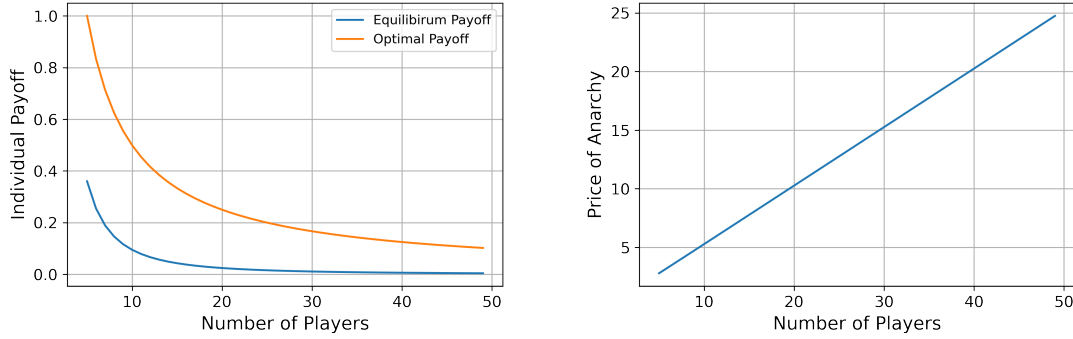
13

Figure 3: (Left) Individual payoff of a player versus the number of players. (Right) Ratio of the optimal payoff divided by the equilibrium payoff versus the number of players.

is symmetric and pure. This equilibrium can be computed efficiently by solving a single variable, unimodal optimization problem. We further established that the price of anarchy is $\Omega(n)$ in the number of players, relative to the optimal 'fair' allocation. We illustrated how concave pro-rata games connect to a recent proposal for a batched decentralized exchange and numerically studied the behavior of agents engaged in such a game in the iterated setting for a specific form of utility function. Future work includes further study of the optimal arbitrage problem for batched decentralized exchanges.

References

[AAE+22]   Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant Function Market Makers: Multi-asset Trades via Convex Optimization. In *Handbook on Blockchain*, page 31. Springer, first edition, 2022.

[AEC21]   Guillermo Angeris, Alex Evans, and Tarun Chitra. A Note on Privacy in Constant Function Market Makers, March 2021.

[BCS15]   Eric Budish, Peter Cramton, and John Shim. The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response. *The Quarterly Journal of Economics*, 130(4):1547–1621, November 2015.

[BV04]   Stephen P. Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, UK; New York, 2004.

[CAE22]   Tarun Chitra, Guillermo Angeris, and Alex Evans. Differential Privacy in Constant Function Market Makers. *Financial Cryptography and Data Security 2022*, 2022.

[DB16]   Steven Diamond and Stephen Boyd. CVXPY: A Python-embedded modeling language for convex optimization. *Journal of Machine Learning Research*, 17(83):1–5, 2016.

[DGK+20] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927, 2020.

[OCPB16] Brendan O'Donoghue, Eric Chu, Neal Parikh, and Stephen Boyd. Conic optimization via operator splitting and homogeneous self-dual embedding. *Journal of Optimization Theory and Applications*, 169(3):1042–1068, June 2016.

[Pen]   Penumbra Labs. ZSwap - The Penumbra Protocol. https://protocol.penumbra.zone/main/zswap.html.

[Ros65]   Jeffrey B. Rosen. Existence and Uniqueness of Equilibrium Points for Concave N-Person Games. *Econometrica*, 33(3):520, July 1965.

[Sel70]   Reinhard Selten. *Preispolitik der Mehrproduktenunternehmung in der statischen Theorie*. 1970.

[VNM07]   John Von Neumann and Oskar Morgenstern. Theory of games and economic behavior. In *Theory of games and economic behavior*. Princeton university press, 2007.

[Wal18]   Tom Walther. Multi-token Batch Auctions with Uniform Clearing Prices, July 2018.

A   Relaxing strict concavity

We do not, in fact, need strict concavity in the proofs above. Instead, we only need that f has 'some curvature' at 0. Specifically, it suffices that for all t and t' such that $0 < t < t'$, we have

$$f(t) > \frac{f(t')}{t'}t.$$

Written in English, this is the condition that the chord from 0 to t always lies strictly below the function. This condition is sometimes difficult to confirm for general functions f, so we will show that this is equivalent to the (potentially simpler-to-handle) property that all supergradients at 0 lie strictly above the function at all points. We will show that, for any concave function $f : \mathbf{R}_+ \to \mathbf{R}$ with $f(0) = 0$, the following two statements are equivalent: (a) there is some $s' > 0$ and $\alpha \in \mathbf{R}$ such that for every s with $0 \le s \le s'$ we have

$$f(s) = \alpha s,$$

and (b) there exists some $0 < t < t'$ such that

$$\frac{f(t)}{t} = \frac{f(t')}{t'}.$$
(9)

The statement above follows from the negation of both (a) and (b). This equivalence has a simple interpretation: if the point $(0, 0)$ is collinear with any other two points on the graph of f, $\{(s, f(s)) \mid s > 0\}$, then the function f is a piecewise function with a linear segment starting at 0. The converse of this is that if the function f has no linear segment around 0 (*i.e.*, every linear overestimator around 0 lies strictly above f) then any chord must lie strictly below the function.

Proof. The forward implication is very easy: pick $t' = s'$ and let t be any $0 < t < s'$, then we have

$$\frac{f(t')}{t'} = \alpha = \frac{f(t)}{t}.$$

Now we'll consider the reverse implication. Given $0 < t < t'$ satisfying (9), we will show that, for any $0 \le s \le t$ we have

$$f(s) = \frac{f(t)}{t} s,$$

which satisfies the original claim with $\alpha = f(t)/t$. First, it is easy to show that

$$f(s) \ge \frac{f(t)}{t} s,$$
(10)

since

$$f(s) = f\left(\frac{s}{t} t + \left(1 - \frac{s}{t}\right) 0\right) \ge \frac{s}{t} f(t),$$

where the inequality follows from the concavity of f and the fact that $f(0) = 0$. We will now show that any function f satisfying (10) strictly, *i.e.*,

$$f(s) > \frac{f(t)}{t} s,$$
(11)

for some $0 < s < t$ cannot be concave. The result follows from the contrapositive. To see this, let $0 < \gamma \le 1$ such that $t = \gamma s + (1 - \gamma)t'$, then

$$\gamma f(s) + (1 - \gamma)f(t') > \gamma \frac{f(t)}{t} s + (1 - \gamma)\frac{f(t)}{t} t' = f(t) = f(\gamma s + (1 - \gamma)t'),$$

so f cannot be concave. The inequality follows directly from conditions (9) and (11), and both the first and second equalities follow from the definition of γ.

B Rosen condition

Pro-rata games, even concave ones, do not satisfy the Rosen condition [Ros65] for the uniqueness of equilibria in concave games. The Rosen condition for uniqueness is that if, there exists some $z \geq 0$ with $z \neq 0$ such that

$$\Phi(x) = \begin{bmatrix} z_1 \partial_1 U_1(x) \\ \vdots \\ z_n \partial_n U_n(x) \end{bmatrix}$$

is a strictly monotone operator; *i.e.*, for any $x \neq y$ we have

$$(y - x)^T (\Phi(y) - \Phi(x)) > 0,$$

then there is a unique equilibrium that is also pure. (Here, ∂_i denotes the ith partial derivative.) This is a common condition used to prove the uniqueness of pure equilibria in games. We will show that this condition does not hold in general for concave pro-rata games, even under most 'niceness' assumptions such as strict concavity or even strong concavity and differentiability.

Setting $2x = y = \mathbf{1}$ then the condition can be written as (using the definition of U)

$$(\mathbf{1}^T z/2)((1/n)(f'(n) - f'(n/2)) + (1 - 1/n)(f(n) - 2f(n/2))) > 0,$$

but this can be rewritten (since $\mathbf{1}^T z > 0$)

$$(1/n)(f'(n) - f'(n/2)) + (1 - 1/n)(f(n) - 2f(n/2)) > 0,$$

which is clearly not true for all concave functions f, since picking $f(t) = \min\{t, 3n\}$ suffices. (A mollifying argument would show that this also gives a reasonable counterexample even in the case that f is strictly concave and differentiable.) A more direct counterexample that is differentiable and strictly concave is $f(t) = (4n)^2 - (4n - t)^2$, which is slightly more difficult to verify.

C Additional Numerics

Here we expand on the simulations introduced in §3 using a class of utility function that allows us to express many quantities of interest in closed form.

Game setup. We consider the following three scenarios:

1. At iteration t, player i takes action equal to the best response to x_{-i}^{t-1}.

2. At iteration t, player i takes action equal to the best response to x_{-i}^{t-1} subject to a bounded update constraint ($|x_i^t - x_i^{t-1}| \leq \delta$).

3. At iteration t, player i takes action equal to the best response to x_{-i}^{t-1} subject to a budget constraint ($x_i^t \in [0, M_i]$).
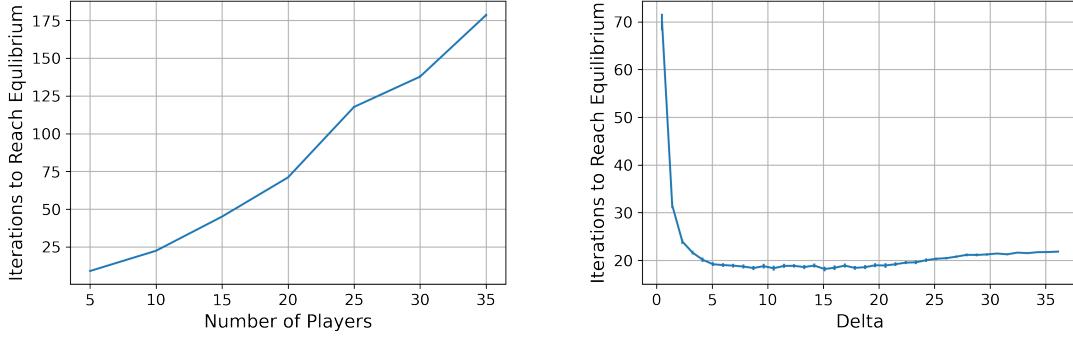
Figure 4: (Left) Number of iterations to reach equilibrium versus the number of players in Scenario 1. (Right) Number of iterations to reach equilibrium versus δ in Scenario 2 (with $n = 10$ players).

Payoff functions. For these simulations, we use functions f of the form $f(t) = t^\beta - \gamma t$ where $0 < \beta < 1$ and $\gamma > 0$. Note that f is concave as it is the sum of two concave functions and $f(0) = 0$. These functions also satisfy the strict concavity property (3) since

$$f(\alpha t) = \alpha^\beta t^\beta - \alpha \gamma t > \alpha t^\beta - \alpha \gamma t = \alpha f(t),$$

for $0 < \alpha < 1$.

Shared equilibrium. The (unique) symmetric pure equilibrium strategy is the solution to problem (4). This is easy to compute using the first order optimality conditions for problem (4) given in (6). Plugging in this particular form of f, we have:

$$(n - 1)(q^\beta - \gamma q) + q(\beta q^{\beta - 1} - \gamma) = 0,$$

which has a solution

$$q = \left(\frac{\beta + n - 1}{n\gamma} \right)^{1/(1-\beta)}.$$

The equilibrium is then given by $x_i = q/n$, for each player $i = 1, \ldots, n$.

Simulation results. In our simulations, we fix $\beta = 0.5$ and $\gamma = 0.05$. We average each reported value over 100 trials. In figure 4, the initial strategy of each player is drawn uniformly at random from the interval $(0, w/n)$, where w is a value such that $f(w) = 0$.

The left plot of figure 4 illustrates that the number of iterations needed to reach the unique equilibrium, in the absence of budget constraints, scales superlinearly in the number of players. The right plot demonstrates that in the scenario of bounded strategy updates, for small values of δ, the number of iterations required to reach equilibrium increases significantly when compared to the unbounded strategy update scenario.
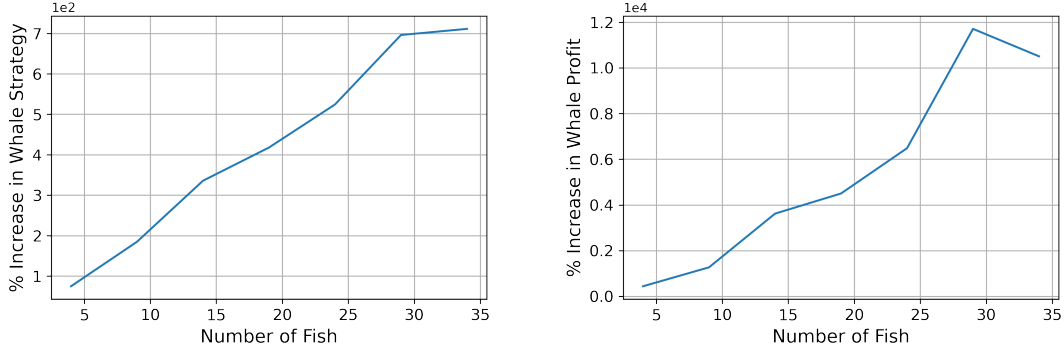
18

Figure 5: Percent increase in whale strategy and whale profit versus the number of fish when compared to the unconstrained equilibrium strategy and profit.

In figure 5, we consider the setting where there is one player who has unlimited budget (whom we will call a *whale*) and all remaining players have some budget $M_i < q/n$ (these players are referred to as *fish*). The budgets of the fish are drawn uniformly from the interval $M_i \sim [0, q/n]$ and the initial strategy of each fish is drawn uniformly at random from the interval $[0, M_i]$. The equilibrium strategy chosen by the fish is to use their entire budget, while the whale chooses a strategy in excess of the unconstrained equilibrium strategy and is, as a result, able to extract greater profit. Figure 5 illustrates that the whale chooses an increasingly large strategy and receives an increasing profit as the number of fish increases.

Price of Anarchy   The equilibrium payoff can easily be found to be

$$\frac{1}{n} f(q) = \left(\frac{n + \beta - 1}{\gamma n} \right)^{\beta/(1-\beta)} \left(\frac{1 - \beta}{n^2} \right).$$

Similarly, it can be show that the optimal payoff conditioned on every agent receiving the same payoff is given by

$$\frac{1}{n} \sup f = \left(\frac{\beta}{\gamma} \right)^{\beta/(1-\beta)} \left(\frac{1 - \beta}{n} \right).$$

We obtain the price of anarchy by taking the ratio of the equilibrium payoff and the optimal payoff:

$$\frac{\sup f}{f(q)} = n \left(\frac{\beta n}{n + \beta - 1} \right)^{\beta/(1-\beta)}.$$

We again fix $\beta = 0.5$ and $\gamma = 0.05$. The left plot of figure 6 illustrates the optimal payoff function and the equilibrium payoff function as a function of the number of players n while the right plot of figure 6 illustrates the price of anarchy as function of n.
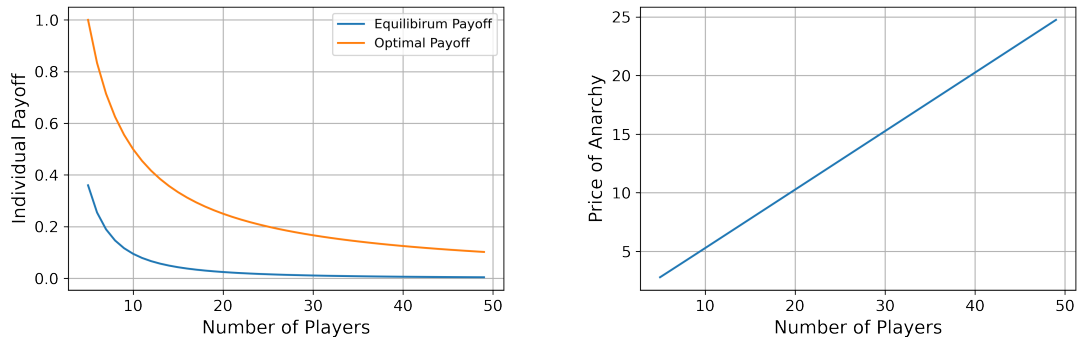
19

Figure 6: (Left) Individual payoff of a player versus the number of players. (Right) Ratio of the optimal payoff divided by the equilibrium payoff versus the number of players.