arXiv:2302.02126v1 [cs.GT] 4 Feb 2023

凹比例分配博弈

Nicholas A. G. Johnson Theo Diamandis AlexEvansnagj@mit.edu
tdiamand@mit.edu aevans@baincapital.comHenryde Valence Guillermo
Angerishdevalence@penumbra.zone gangeris@baincapital.com

2022年10月

摘要

本文介绍了一类称为凹比例分配博弈的博弈。在这类博弈中，玩家将资产投入资金池，资金池根据投入其中的所有资产支付某个凹函数值。随后，每位玩家按比例获得支付额；即，每位玩家获得的金额与其投入资金池的数量成正比。这类博弈出现在许多实际场景中，包括批量去中心化交易所的一种简化版本，例如 Penumbra 提出的方案。我们证明，这类博弈具有若干有趣性质，包括存在一个对称纯策略均衡，且该均衡是此博弈的唯一均衡；我们还证明，其无政府代价随玩家人数为 $\Omega(n)$。此外，我们还展示了迭代情形下的一些数值结果，这些结果表明，玩家在迭代博弈中会迅速收敛至均衡。

引言

现有区块链系统以批次为单位对交易达成共识，这些批次称为区块。然而，这些交易所交互的经济机制通常被设计为按顺序逐笔处理交易，因此其行为取决于批次内交易的排序。这种抽象层面的不匹配是矿工可提取价值（MEV）的主要来源。矿工可提取价值是指区块提议者（最初是矿工）通过选择并排列要纳入批次的交易而获取的经济价值 [6]。

不过，我们也可以尝试设计不依赖区块内交易顺序的经济机制，转而将每个交易批次作为一个整体处理，而不是试图蒙蔽区块提议者，或在一个批次内选择一种“公平”的排序（在现有系统中，要以任何直接的方式构造这种排序都很困难，甚至是不可能的）。这样一来，这些机制就能与实际的排序保持一致

这种排序由共识机制提供，使系统在共识发生的相同离散时间步长内，从一个交易批次推进到下一个交易批次。

这类机制之一是“按比例机制”。在这种机制中，价值的概念是已知的：例如，每位用户可能都想用某种资产 A 交易另一种资产，比如B，而每个人都会拿出一定数量的资产 A 投入资金池。所有人投入各自的资产后，整个资金池会在交易所进行交易，以换取一定数量的资产B，然后按照每位玩家投入资金池的资产 A 数量占比，将所得资产 B 分配给各位玩家。不难证明，这种机制具备所需的性质：玩家将资产 A 投入集体资金池的先后顺序，不会影响各自收到的资产 B 数量。借助密码学中的一些方法，还可以实现这种博弈，使其不会泄露任何一位玩家的投入或身份 [9], ，因此可将其视为同时博弈。

另一方面，这类机制往往会引发有趣的现象，因为用户在规划自己的行动时，必须考虑其他用户可能采取的行动。对于这类问题——玩家必须递归地推演其他玩家的策略——一种自然的研究框架是博弈论，以及对博弈均衡的研究 [12]。本文旨在以简洁的数学框架清晰地构建由按比例机制产生的博弈，并推导出若干适用于这类博弈的实用结果。

本文。 本文的组织结构如下。我们在第 §1 节介绍凹比例分配博弈，并展示其在温和条件下的一些有趣性质。这些性质包括对称纯策略均衡的存在性与唯一性，以及通过求解一个单变量单峰优化问题来高效计算该均衡的明确方法。我们还给出了无政府代价的一些简单界。随后在第 §2 节，我们描述了这类博弈如何与近期提出的一种批量去中心化交易所方案建立联系。我们在第 §A 节和 §B 节进行了多次模拟，说明无政府代价，并展示在迭代情形下，代理人似乎会迅速收敛到指定的均衡。

1 凹比例分配博弈

我们将定义具有 n 名玩家的按比例分配博弈，其定义为：玩家 $i = 1, \ldots, n$的收益如下：

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

这里，f：$\mathbf{R}_+ \to \mathbf{R}$ 是满足 $f(0) = 0$的某个函数，而 $x \in \mathbf{R}_+^n$ 是一个非负向量，其 i 个分量表示第 i 个玩家所采取的行动。如果函数 f 是凹函数，我们就称该博弈为凹比例分配博弈。该博弈有一种简单的解释：每个玩家向资金池投入一定数额 x_i，总额为 $\mathbf{1}^T x$，资金池根据所有玩家投入的总额，仅依据$f(\mathbf{1}^T x)$进行支付。资金池支付的金额随后按照按比例分配的方式分配给玩家；即，每个玩家 i所获得的金额与其投入资金池的数额成比例。在本文余下部分，我们假设函数 f 是凹函数。我们注意到，凹比例分配

博弈是聚合博弈的一种特殊情形，在这类博弈中，每个玩家的收益是其策略以及所有玩家策略之和的函数（参见，[11]）。

凹性。收益 U_i 在固定其余条目为常数的情况下，关于第 i 个条目是凹的。为说明这一点，首先定义 $y = \mathbf{1}^T x - x_i$（即，y 是 x 的所有条目之和，但不包括第 i 个条目）。对 U_i 略作符号重载，我们有

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

我们可以将 $U_i(\cdot, y)$ 写成以下两个函数的复合

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

其中

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

它们的定义域为非负实数。我们将利用这一改写来证明该函数关于 x_i 是凹的，因为根据基本的凸复合规则（参见 [3, §3.2.4]），只需证明：（a）h 是凹的；（b）g 是凹的，且关于其第二个自变量单调不减。

首先，注意到 h 是（严格）凹的，因为

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

显然，由于 y 是常数，该函数关于 x_i 是（严格）凹的。我们可以看到，g 关于其自变量是联合凹的，因为它是函数 f 的透视变换，而透视变换保持凹性（参见 [3, §3.2.6]）。最后，我们需要证明 g 关于其第二个自变量单调不减。为此，令 $0 \le t \le t'$，则有

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

该不等式由凹性的定义得出，而倒数第二个等式则由以下事实得出：$f(0) = 0$。

自私最大值。g 关于其第二个参数是非递减的，这一事实还带来了一个有趣的结论：与“自私”版本相比，玩家在按比例分配博弈中的表现从不会更好。换句话说，对于固定的 x_i，当所有其他玩家 $j \ne i$ 都具有 $x_j = 0$时，玩家 i 的收益最大。这一点很容易看出，因为

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

so

$$U_i(x) = g(x_i, t) \le g(x_i, 1) = f(x_i),$$

其中， g 的定义如上。不等式源于 g 关于其第二个参数的单调性。

严格凹性。 在满足以下条件的这一重要特例中： f

$$f(\alpha t) > \alpha f(t), \tag{3}$$

对每个 $t > 0$ 和 $0 < \alpha < 1$ 均成立，那么函数 $U_i(\cdot,\ y)$ 关于其第一个自变量严格凹。（我们很快就会证明这一点。）性质 (3) 的含义是：连接函数图像上的点 (0，0) 与任意其他点所作的弦，严格位于函数图像下方。例如，函数 f 严格凹是一个充分条件，但并非必要条件，因为也有一些不严格凹的函数满足 (3)。更一般的条件见附录 C。

由于我们知道 h 是严格凹函数，而 g 是凹函数，因此，只要证明 g 关于其第二个自变量严格递增，就可以说明 $g(x_i,\ h(x_i))$ 关于 x_i 严格凹。根据通常的复合规则， g 严格凹（见 $[3, \S 3.2.4]$）。为证明 g 关于其第二个自变量严格递增，令 $0 < t < t'$，则：

$$g(x_i, t') = t' f\left(\frac{x_i}{t'}\right) = t' f\left(\frac{t}{t'}\frac{x_i}{t}\right) > t'\frac{t}{t'} f\left(\frac{x_i}{t}\right) = t f\left(\frac{x_i}{t}\right) = g(x_i, t),$$

其中，不等式是将 $\alpha = t/t'$ 代入 (3) 得出的。

定义。 为完整起见，我们陈述若干重要的博弈论定义 [12]。对于每位玩家 $i = 1$、.....、 n，我们关联一个策略，它是一个概率分布 π_i，分布在玩家 i可采取的行动（非负实数）上。如果一个策略是确定性分布或点质量，我们就称其为纯策略，即 π_i 。换句话说，如果选择某个特定行动 z 的概率始终为 1，我们就称该策略为纯策略；也就是说， $\pi_i(\{z\}) = 1$ ，其中$z \ge 0$。否则，我们称该策略为混合策略。

纳什均衡（下文简称均衡）是每位玩家 $i = 1$、.....、 n 各自的策略组合π_i，满足任何单个玩家都无法通过选择不同的策略获得严格更好的结果。具体而言，设 $x_i \sim \pi_i$ 为由玩家 i 的策略（混合或纯策略）选取的随机变量，设 $y_i \sim \pi_{-i}$ 为表示其他玩家策略所对应随机变量之和的随机变量。策略组合 (π_i) 构成一个均衡，当且仅当对每位玩家 i，都有

$$\mathbf{E}_{x_i \sim \pi_i,\ y_i \sim \pi_{-i}} \left[U_i(x_i, y_i)\right] \ge \mathbf{E}_{x_i \sim \tilde{\pi}_i,\ y_i \sim \pi_{-i}} \left[U_i(x_i, y_i)\right],$$

其中， $\tilde{\pi}_i$ 表示任意策略。（在本文余下部分，为简化记号，我们将省略期望定义中的 x_i 和y_i 。）如果对于除 $\tilde{\pi}_i = \pi_i$以外的所有 i ，上述条件均以严格不等式成立，则该均衡被称为严格均衡。换言之，如果每个玩家选择不同的策略都会获得严格更差的结果，则该均衡是严格的。一般而言，如果某个均衡的所有策略都是纯策略，我们称其为纯策略均衡；否则称其为混合均衡。

纯策略均衡。根据上述定义，我们注意到，$U_i(x_i,\ y)$ 关于 x_i的严格凹性具有一个重要且直接的推论：该博弈的每个均衡都是纯策略均衡。设 $x_i \sim \pi_i$ 为任意一个非纯策略，而 $y_i \sim \pi_{-i}$ 为表示其他玩家策略之和的随机变量，则

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

其中，严格不等式源于对所有 y ， $U_i(\cdot,\ y)$ 的严格凹性，以及 π_i 不是点质量这一事实。换言之，如果 $x_i \sim \pi_i$ 是玩家 i 的混合策略，那么该玩家选择纯策略 $\mathbf{E}_{\pi_i}[x_i]$ 始终会获得严格更高的收益。在本文余下部分，除非另有说明，我们假设 f 是凹函数并满足条件(3)。此外，由于所有均衡都必须是纯策略均衡，本文余下部分只讨论纯策略均衡，因此将策略视为特定行动$x_i \in \mathbf{R}_+$ 是合理的。

扩展。对凹比例分配博弈的一个简单直接的扩展，是考虑如下形式的收益函数：

$$U_i(x) = \frac{c_i x_i}{c^T x} f\left(c^T x\right),$$

对于某个严格正向量 $c \in \mathbf{R}^n_{++}$。更一般的扩展是考虑一组 n 严格递增函数 $\varphi_i : \mathbf{R}_+ \to \mathbf{R}$，其中 $\varphi_i(0) = 0$ ，且当 $t \to \infty$ 时，对于 $i = 1,\ \ldots\ldots,\ n$，有 $\varphi_i(t) \to \infty$，并且

$$U_i(x) = \left(\frac{\varphi_i(x_i)}{\sum_{i=1}^n \varphi_i(x_i)}\right) f\left(\sum_{i=1}^n \varphi_i(x_i)\right).$$

无论哪种情况，上述所有性质都适用于这个稍微更一般的博弈，证明也几乎完全相同；但我们只考虑这一（通常很有用的）特殊情形：$\varphi_i(t) = t$。

1.1 对称纯策略严格均衡

存在一个严格纯策略均衡，其中所有玩家的策略都相同，表示为 $x = (q/n)\mathbf{1}$，其中 q 是以下问题的最优解：

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

其中变量为 $q \in \mathbf{R}$。我们将先展示这一结果的一些性质，然后证明纯策略 $x = (q/n)\mathbf{1}$ 确实是一个均衡。

解的性质。 该问题有一个有限的（唯一）解 $q > 0$ ，条件是$f(z) > 0$且 $f(w) = 0$对某个 $0 < z < w$成立。注意到 $q > 0$满足 $q^{n-1}f(q) \geq z^{n-1}f(z) > 0$ ，即可得出q 成立，因为它是最优的。另一方面，q 是有限的这一事实，源于对任意 $r \geq w$，我们都有

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

其中，第一个不等式由凹性的定义可得。由于假设 $f(0) = 0$且 $w/r > 0$，因此有 $f(r) \leq 0$，所以 r不可能是最优的。（事实上，这两个陈述结合起来证明了更强的结论：$0 < q < w$，但接下来的推导并不需要这一点。）问题 (4) 的解的唯一性可通过观察到目标函数的对数是严格凹的得出。（这是因为 log 严格递增，且若 f 是凹的，则 $\log \circ f$ 是凹的。）

讨论。 对 f 施加的条件看起来可能非常严格，但事实上，任何不满足上述条件的 f都只有平凡均衡（或没有均衡）。具体而言，由于 f 是凹的，若 f 不满足上述条件，则以下情况必居其一：(a) f 除在 $f(0) = 0$处外处处严格为正；(b) f除在 $f(0) = 0$处外处处严格为负；或 (c) $f = 0$。在第一种情况下，不存在均衡，因为任何玩家都可以通过增加自己的策略来提高收益。在第二种情况下，任何采用非零策略的玩家都会获得负收益（而采用零策略则可获得 0 收益）。第三种情况下，任何策略都是均衡。

均衡的性质。 策略组合 $x = (q/n)\mathbf{1}$ 显然是纯策略且对称的。要证明 $x = (q/n)\mathbf{1}$ 是严格均衡，请注意，当其他每位玩家都采用策略 q/n 时，任意玩家 i的最佳响应为：

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

变量为 $x_i \in \mathbf{R}$。我们将分两步证明 (5) 的解为 $x_i = q/n$ 。首先，我们将证明任何解都必须满足 $x_i > 0$ ，因此对目标函数应用一阶最优性条件就足够了。然后，我们将证明 $x_i = q/n$ 是满足最优性条件的解。结合目标函数严格凹这一事实，这一结果意味着 $x_i = q/n$ 是满足最优性条件的唯一解，从而证明最后的结论：该均衡是严格的。

要证明最佳响应问题 (5) 的任何解都必须满足 $x_i > 0$，请注意，q/n 是可行的，其目标函数值为 $f(q)/n > 0$，严格大于 $x_i = 0$所取得的零目标函数值。

接下来请注意， $q > 0$ 必须满足（4）的一阶最优性条件：

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

另一方面，问题（5）的目标函数的一阶最优性条件要求 x_i 必须满足（为方便起见，记 $q' = (1-1/n)q$）

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

选择 $x_i = q/n$ 显然满足该条件，因为代入此值可得

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

正如所需。由于目标函数严格凹，这是满足最优性条件的唯一 x_i ，因此也是最佳响应。此外，虽然我们假设 f 可微，但使用次梯度演算进行非常类似的证明，也能得到相同的结果。

1.2 均衡的唯一性

事实上，不难证明，在与 (4) 相同的条件下，这个博弈中的对称纯策略严格均衡出人意料地是唯一均衡；也就是说，对于某个 $0 < z < w$， $f(z) > 0$且 $f(w) = 0$ 。该证明可分为几个步骤。首先，我们将证明任何均衡 x都满足 $f(\mathbf{1}^T x) > 0$，且对于每个 i，都有 $x_i > 0$。随后，我们将利用这一点证明不存在非对称均衡；又由于我们知道任何对称均衡都必须满足方程 (4)，而该方程有唯一解，因此可知它就是这个博弈的唯一均衡。

均衡的正性。 首先，我们将证明对于每个 $0 < v < w$，都有 $f(v) > 0$ 。为此，注意到由于 f 是凹函数，因此函数 f 不小于其所有弦。注意，端点为 (0，0) 和 (z， $f(z)$) 的弦位于 x 轴上方，除 (0，0) 点外；而端点为 (z， $f(z)$) 和 (w， $f(w)$) 的弦 =(w，0) 位于 x 轴上方，除 (w，0) 点外，由此可得最终结果。

现在，假设一组纯策略满足 $f(\mathbf{1}^T x) < 0$。由于 $f(0) = 0$，存在某个指标 i，使得 $x_i > 0$。这意味着 $U_i(x_i, \mathbf{1}^T x - x_i) < 0$。但是，玩家$i$ 可以通过采用策略 $\tilde{x}_i = 0$ 获得等于 0 的收益，这严格优于负收益，因此 x 不可能是均衡。

另一方面，如果一个策略组合满足 $f(\mathbf{1}^T x) = 0$，那么，根据前面的讨论，我们必有 $\mathbf{1}^T x = 0$ 或 $\mathbf{1}^T x = w$。如果 $\mathbf{1}^T x = 0$，任何玩家 i 都可以通过采用策略 $\tilde{x}_i = z$ 获得严格为正的收益。反之，如果 $\mathbf{1}^T x = w > 0$，则存在某个指标 i使得 $x_i > 0$。我们知道，该玩家的收益为 $U_i(x_i, \mathbf{1}^T x - x_i) = 0$，这意味着

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

当 $\varepsilon > 0$ 足够小时，因为 $f(w - \varepsilon) > 0$，所以 x 不是均衡。

综合以上所有论述可知，任何均衡 x 都满足 $f(\mathbf{1}^T x) > 0$ 和 $\mathbf{1}^T x < w$。要证明任何均衡还必须满足 $x > 0$，注意到如果存在一个指标 i，使得对于一个满足 $f(\mathbf{1}^T x) > 0$ 的策略组合有 $x_i = 0$，那么玩家 i 总能通过采取 $\tilde{x}_i = \varepsilon > 0$ 获得严格为正的收益，只要 ε 足够小。

均衡的对称性。接下来，我们将证明：如果 x_i 是玩家 i的最佳响应，那么对于任何满足 $x_j > x_i$ 的 j，它都不是玩家 j的最佳响应，反之亦然。这将立即表明，任何均衡都必须满足 $x_i = x_j$（即它是对称的）。我们将在 f 可微的情形下给出证明，但在更一般的情形下，也可以使用次梯度演算得到类似的证明。

设 x 是一个满足 $x_j > x_i$的均衡。鉴于 x_i 是一个最佳响应，问题 (5) 的最优性条件意味着：

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

由于 x 是一个均衡，根据前面的讨论，我们有 $f(\mathbf{1}^T x) > 0$, $x_i > 0$和 $\mathbf{1}^T x > x_i$，因此 $f'(\mathbf{1}^T x) < 0$。另一方面，对玩家 j 的最佳响应问题 (5) 的目标函数求导可得

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

其中，该不等式源于以下事实：由于 $x_i < x_j$，我们有

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

因此，x_j 不可能是最佳响应，因为它不是问题 (5) 的最优解。反过来的情形，即 $x_j < x_i$ 在 x_i 为最佳响应时，也可通过几乎相同的证明得出。这立即意味着，任何均衡都必须是对称的，因此根据前面的讨论，唯一均衡就是问题 (4) 的解。

1.3 均衡收益

在每位玩家获得相同收益（即满足公平性条件）的前提下，每位玩家都能获得的最优分配为

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

根据定义，该分配至少与均衡收益一样好：

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

其中 $q > 0$ 是方程（4）的解。事实上，我们可以证明，最优公平分配始终严格优于均衡收益。为此，请注意，在以下

关于上文引入的 f 的假设下，我们知道 $\sup f$ 由某个值 $0 < q^\star < w$取得，且满足 $f'(q^\star) = 0$。重新整理问题（4）中关于 q 的一阶最优性条件，可得

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

对于所有 $n > 1$，由于 $f(q) > 0$。这意味着 q 不满足最大化 f 的最优性条件，因此 $f(q) < f(q^\star) = \sup f$。（事实上，这说明了更多：利用 f 的凹性，我们有 $q > q^\star$，即，当 $n > 1$ 时，玩家在均衡处"支付过多"。）

无政府代价。在与 §1.2 开头关于函数 f 相同的假设下，不难证明，无政府代价满足

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

当玩家数量 n 增大时，对于某个常数 C，.....。为此，考虑 y (4) 的一阶最优性条件：

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

注意，由于 $q > 0$ 且 $f(q) > 0$，因此 $f'(q) < 0$，所以

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

只要 $n > 1$。由于 f 是凹函数，因此 f' 单调不增；又由于对于每个 n，都有 $q \leq w$，我们得到

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

最后，我们知道 $\sup f$ 是玩家人数的常数，因此

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

2 批量去中心化交易所

本节将展示上述性质在批量去中心化交易所中的一些基本应用，具体介绍如下。

去中心化交易所。去中心化交易所（简称 DEX）是一种存在于区块链上的交易所。这类交易所使任何代理人都能交易货币，而无需中心化中介。在许多情况下，这类交易所采用常函数做市商的形式（参见例如，[1]，了解此类交易所的一般介绍）；这是一种特殊的自动化做市商，使用特定函数为资产定价。

批处理去中心化交易所。批处理去中心化交易所是一种在执行交易前先将交易进行批处理的去中心化交易所。具体来说，交易会以某种方式聚合（具体方式取决于所采用的批处理类型），然后通过去中心化交易所「一起」交易，之后再拆分并返还给用户。批处理交易所这一概念已在不同背景下多次提出（参见例如，[4] 和 [13]），但目前几乎所有主要的去中心化交易所都未采用批处理。近期研究表明，批处理有助于保护隐私 [5]；Penumbra [9] 提出了一种全隐私去中心化交易所设计，利用批处理来避免某些信息泄露 [2]。下面我们将介绍这一提案的一个高度简化版本，足以用于我们的讨论。

批处理设计。 在此情形下，交易者 $i = 1, \ldots, n$ 都希望交易一定数量的资产，比如 $\Delta_i \in \mathbf{R}$ 单位资产 A，以换取另一种资产，我们称之为资产 B。在这种情况下，Δ_i 的负值表示交易者 i 希望收到一定数量的资产 A（并转而向协议交付资产 B）。为方便起见，我们假设 $\mathbf{1}^T\Delta > 0$，即，总体而言，交易者想要的资产 B 多于资产 A。Penumbra 的批处理协议首先对所有交易进行清算，得到一个非负的"剩余"交易向量 $\Delta' \in \mathbf{R}^n_+$，其中 $\mathbf{1}^T\Delta = \mathbf{1}^T\Delta'$。（换言之，协议不会在任何一方产生债务。）我们可以将 Δ' 视为资产 B 相对于 A 的"超额需求"，并且不对构造 Δ' 的机制作其他规定，只要求满足以下附加条件：若 $\Delta \geq 0$，则 $\Delta' = \Delta$。（粗略地说，这一条件可以表述为：如果交易仅由超额需求产生，则不会发生清算。）随后，协议将剩余需求汇集到资金池中，$\mathbf{1}^T\Delta'$ 并与由某个函数 g表示的常函数做市商进行交易，以获得 $g(\mathbf{1}^T\Delta')$ 单位资产 B，再以按比例的方式将其分配给每位代理人 i，从而得到与按比例分配的收益 (1) 相同的形式，其中 $x = \Delta'$。常函数做市商的函数 g总是凹函数，有时称为远期交换函数（参见，[1, §4]），且满足 $g(0) = 0$；在许多实际情形中，这些函数还是严格凹函数。

2.1 套利

分析市场的一种常见方式是从套利的角度出发：利用价格差异获取基本上无风险的利润。根据前文，我们用 g 表示上述批处理设计中使用的常函数做市商的远期交换函数。

存在性。 假设 g 在 0 处可微，我们可以将 $g'(0)$解释为：获得边际数量的资产 B 所需的边际数量 A。（函数 g 通常在 0 处不可微，但在 0^+处单侧可微，这就足够了。）如果 $g'(0)$大于外部市场的价格，例如 $c > 0$，那么任何能够直接与 g 交易的人，都可以通过将一定数量（可能很少）的资产 A，即 $t > 0$，换成 B数量的资产 $g(t)$，再卖出这部分资产 B，获得 $g(t)/c - t > 0$ 的无风险利润。（验证这一点的一个简单方法是对 $g(t)/c$ 使用导数的定义，并令 $t \downarrow 0$。）

最优套利。 由于代理人在这些情况下可以获得无风险利润，因此可以合理地提出这样的问题：代理人通过这种策略最多能获得多少利润？这就是所谓的最优套利问题，写作：

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

变量为 $t \in \mathbf{R}$。根据前文，若已知 $g'(0) > c$，则该问题的最优值严格为正。若 g 可微，则最优解 $t^\star$ 满足

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

这一点可由该问题的一阶最优性条件看出。这意味着，交易 $t^\star$ 后恒定函数做市商的边际价格 $g'(t^\star)$ 应等于外部市场的价格，我们将其定义为 c。

（汇总后的）套利博弈。在上述批处理交易所中，套利者无法直接与常数函数做市商交易，而必须通过批处理流程。假设有 n 名套利者竞相最大化利润，接下来的问题是：这个博弈有哪些性质？定义

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

那么该博弈是一个以函数 f 为特征的凹比例分配博弈，因为玩家 i 的收益 (1) 为

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

请注意，这恰好是玩家 i 从具有远期交换函数g的去中心化交易所获得的金额，减去其与外部市场进行交易 x_i 的成本。该博弈继承了 §1 中推导出的所有性质。我们在附录 A 和 B 中展示了这种形式的效用函数下迭代行为的一些数值模拟。

3 结论

我们介绍了凹比例分配博弈，并在相对温和的条件下确立了若干有用性质。特别是，我们证明了存在一个唯一的、对称的纯策略均衡。通过求解一个单变量单峰优化问题，可以高效地计算出该均衡。我们还证明，相对于最优的“公平”分配，无政府代价随玩家人数呈 $\Omega(n)$ 级增长。我们说明了凹比例分配博弈与近期提出的一种批量去中心化交易所方案之间的联系，并针对某种特定形式的效用函数，以数值方法研究了代理人在迭代情形下参与此类博弈的行为。未来的研究方向包括进一步探讨批量去中心化交易所的最优套利问题。

参考文献

[1] Angeris, G., Agrawal, A., Evans, A., Chitra, T., Boyd, S.：常函数做市商：通过凸优化进行多资产交易。载于：《区块链手册》，第 31 页。施普林格，第一版。（2022）[2] Angeris, G., Evans, A., Chitra, T.：关于常函数做市商中隐私的一则短论（2021年3月）[3] Boyd, S.P., Vandenberghe, L.：凸优化。剑桥大学出版社，英国剑桥；纽约（2004）[4] Budish, E., Cramton, P., Shim, J.：高频交易军备竞赛：频繁批量拍卖作为市场设计的应对方案。《经济学季刊》**130(4)**，1547–1621（2015年11月）。https://doi.org/10.1093/qje/qjv027[5] Chitra, T., Angeris, G., Evans, A.：常函数做市商中的差分隐私。《金融密码学与数据安全》2022（2022）[6] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.：Flash Boys 2.0：去中心化交易所中的抢跑交易、矿工可提取价值与共识不稳定性。载于：2020 IEEE安全与隐私研讨会（SP）。第 910–927 页（2020）。https://doi.org/10.1109/SP40000.2020.00040[7] Diamond, S., Boyd, S.：CVXPY：一种嵌入 Python 的凸优化建模语言。《机器学习研究杂志》**17(83)**，1–5（2016）[8] O’Donoghue, B., Chu, E., Parikh, N., Boyd, S.：通过算子分裂和齐次自对偶嵌入进行锥优化。《优化理论与应用杂志》**169(3)**，1042–1068（2016年6月），`http://stanford.edu/~boyd/papers/scs.html`[9]Penumbra Labs：ZSwap——Penumbra协议。https://protocol.penumbra.zone/main/zswap.html[10] Rosen, J.B.：凹N人博弈均衡点的存在性与唯一性。《计量经济学》**33(3)**，520（1965年7月）。https://doi.org/10.2307/1911749[11]Selten, R.：静态理论中的多产品企业价格政策（1970）[12] 冯·诺伊曼, J., Morgenstern, O.：博弈论与经济行为。载于：《博弈论与经济行为》。普林斯顿大学出版社（2007）[13] Walther, T.：采用统一清算价格的多代币批量拍卖（2018年7月）

数值计算

第 §1 节的结果揭示了凹比例分配博弈中的均衡行为。在此，我们通过模拟探究此类博弈的瞬态行为。

博弈设定。 假设博弈以迭代方式进行，并且在每次迭代中， t玩家 i根据上一轮中其他玩家所选择的行动（记为 x_{-i}^{t-1} ）选择某个行动 x_i^t 作为最佳响应，也可能需要满足其他约束。我们考虑以下情形：

1. 在第 t 次迭代中，玩家 i 采取等于对 x_{-i}^{t-1} 的最佳响应的行动。
2. 在第 t 次迭代中，玩家 i 采取等于对 x_{-i}^{t-1} 的最佳响应且满足预算约束（ $x_i^t \in [0, M_i]$）的行动。

收益函数。 对于这些模拟，我们使用形如 $f(t) = g(t) - ct$ 的函数 f，其中 $c > 0$，并且 $g(t) = \frac{\gamma R_2 t}{R_1 + \gamma t}$，其中 $0 < \gamma \leq 1$、 R_1， $R_2 > 0$。函数 $g(t)$ 是 Uniswap V2 兑换池在资产 1 被投入、资产 2 被接收时的远期交换函数，其储备量为 $R \in \mathbf{R}_+^2$，费用参数为γ。该设定模拟了 n 个套利者竞相最大化其利润的情形，其中 c 表示资产 2 的外部市场价格。关于使用较为简单的收益函数进行的模拟，请参见附录 B。注意， f 是严格凹的，因此满足条件 (3)，并且显然 $f(0) = 0$。

共享均衡。 （唯一的）对称纯均衡策略是问题 (4) 的解。利用问题 (4) 在 (6) 中给出的一阶最优性条件，可以很容易地求出该解。将 f 的这一特定形式代入后，我们得到以下二次方程：

$$(cn\gamma^2)q^2 + q(\gamma^2 R_2 + 2cnR_1\gamma - \gamma^2 nR_2) + (cnR_1^2 - \gamma nR_1 R_2) = 0. \tag{7}$$

于是，对每个玩家 $i = 1, \ldots, n$，均衡为 $x_i = q/n$，其中 q 表示 (7) 的正根。

最佳响应。 给定预算约束 $0 \leq x_i \leq M_i$ 和其他玩家的策略 $y_i = \mathbf{1}^T x - x_i$，玩家 i 的最佳响应为

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

变量为 $x_i \in \mathbf{R}$。这是一个单变量凸优化问题，在实际中可以轻松地通过各种现成软件包 [7, 8] 求解。当 x_i 不受约束时，(8) 的最优值为

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

更多详情请参阅代码（评审期间已匿名处理）。

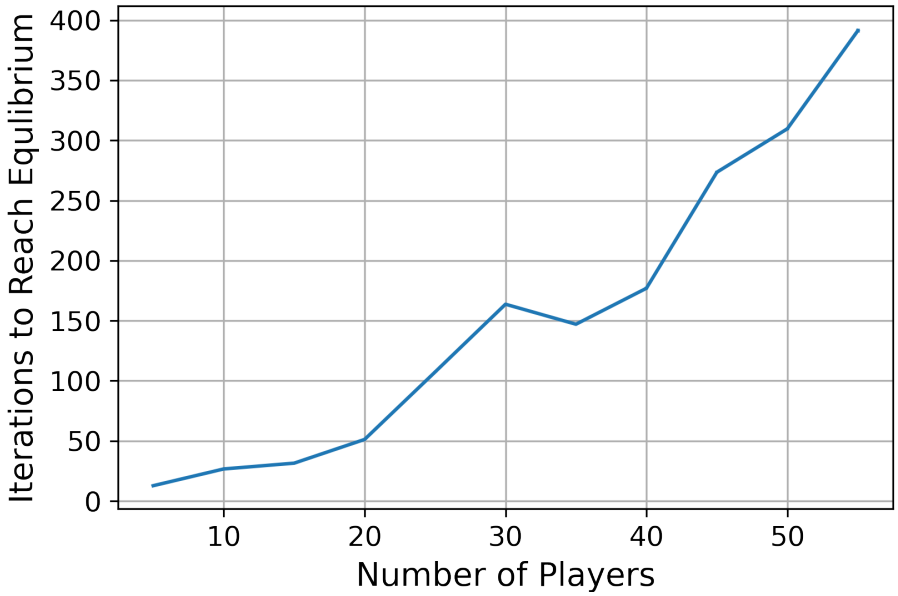

图1：场景1中达到均衡所需的迭代次数与玩家数量的关系。

模拟结果。 在我们的模拟中，我们固定 $\gamma = 0.99$, $R_1 = 200$, $R_2 = 250$ 和 $c = 1$。每个报告值均取 100 次试验的平均值。在图1中，每位玩家的初始策略均从区间 $(0, w/n)$ 中均匀随机抽取，其中 w 是一个满足$f(w) = 0$的值。

图1显示，在没有预算约束的情况下，达到唯一均衡所需的迭代次数随玩家数量超线性增长。我们将达到均衡所需的迭代次数定义为：直到每个玩家的策略在小数点后第一位上都与唯一均衡相等时所经历的迭代次数；即，满足以下条件的第一轮 t

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

其中， $x^\star$ 表示均衡策略。

在图2中，我们考虑这样一种情形：一名玩家拥有无限预算（我们称其为巨鲸），其余玩家都有一定预算 $M_i < q/n$ （这些玩家称为小鱼）。小鱼的预算在区间 $M_i \sim [0, q/n]$ 上均匀抽取，每条小鱼的初始策略则从区间 $[0, M_i]$中均匀随机抽取。小鱼选择的均衡策略是用尽全部预算，而巨鲸选择高于无约束均衡策略的策略，因此能够获取更多利润。图2表明，随着小鱼数量增加，巨鲸会选择越来越大的策略，并获得越来越多的利润。

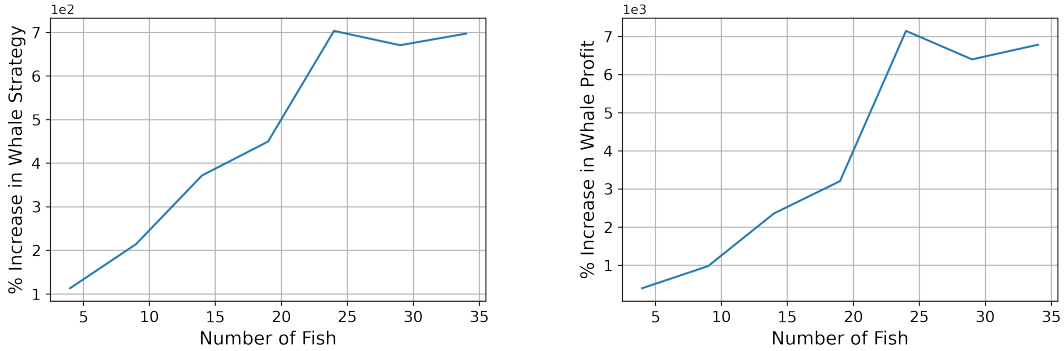

图2：与无约束均衡策略和利润相比，巨鲸策略和巨鲸利润随小鱼数量变化的百分比增幅。

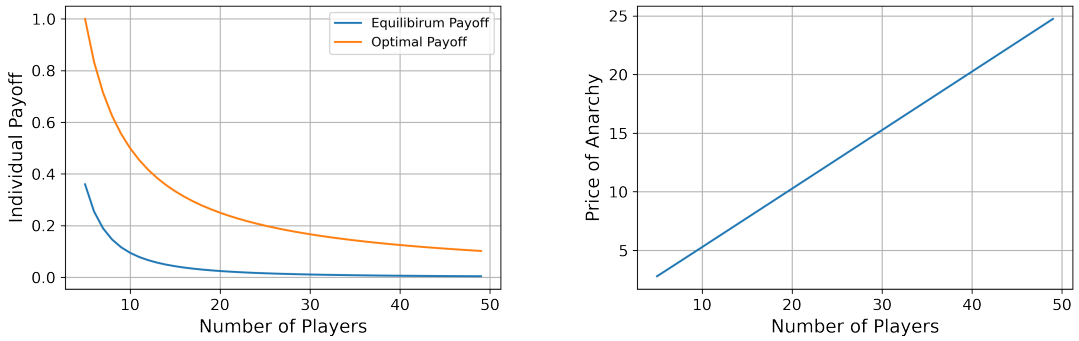

图3：（左）玩家的个体收益随玩家数量的变化。（右）最优收益与均衡收益之比随玩家数量的变化。

无政府代价。在§1中，我们确定了无政府代价的增长阶。这里，我们针对本节前文介绍的特定收益函数族，以数值方式展示无政府代价。我们再次固定 $\gamma = 0.99$，$R_1 = 200$，$R_2 = 250$ 和 $c = 1$。图3左侧的图展示了最优收益函数和均衡收益函数如何随玩家数量 n 变化；右侧的图则展示了无政府代价如何随 n变化。

B 补充数值计算

这里我们通过一类效用函数对附录 A 中介绍的模拟作进一步探讨，该函数使我们能够以闭式形式表示许多感兴趣的量。

博弈设定。 我们考虑以下三种情形：

1. 在第 t次迭代中，玩家 i 采取针对x_{-i}^{t-1} 的最佳响应。

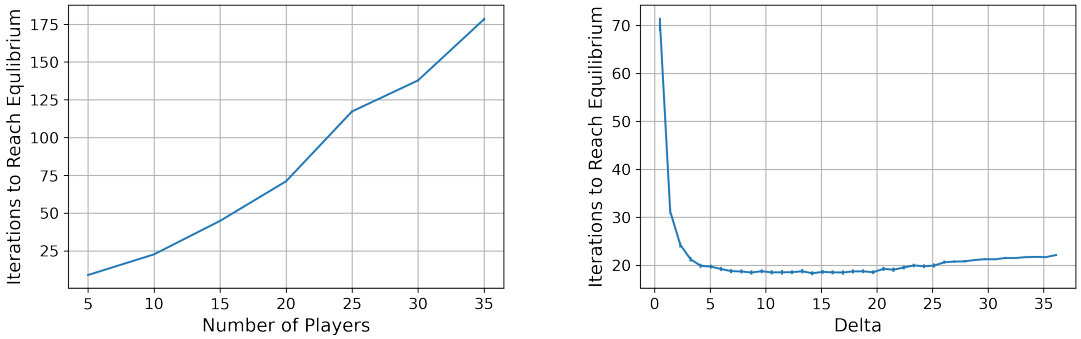

图4：（左）场景1中达到均衡所需的迭代次数与玩家人数的关系。（右）场景2中达到均衡所需的迭代次数与 δ 的关系（有$n = 10$ 名玩家）。

2. 在第 t次迭代中，玩家 i 在有界更新约束（$|x_i^t - x_i^{t-1}| \leq \delta$）下，采取针对 x_{-i}^{t-1} 的最佳响应。

3. 在第 t次迭代时，玩家 i 采取对 x_{-i}^{t-1} 的最佳响应，同时满足预算约束（$x_i^t \in [0, M_i]$）。

收益函数。对于这些模拟，我们使用形式为 $f(t) = t^\beta - \gamma t$的函数 f，其中 $0 < \beta < 1$ 且 $\gamma > 0$。注意，f 是凹函数，因为它是两个凹函数之和，并且 $f(0) = 0$。这些函数还满足严格凹性条件（3），因为

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

对于 $0 < \alpha < 1$。

共享均衡。</style}（唯一的）对称纯均衡策略是问题（4）的解。利用问题（4）的一阶最优性条件（见（6）），很容易计算出该解。代入 f的这一特定形式，我们得到：

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

该方程有解

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

那么，均衡由 $x_i = q/n$ 给出，对每位玩家 $i = 1, \ldots\ldots, n$。

模拟结果。在我们的模拟中，我们固定 $\beta = 0.5$ 和 $\gamma = 0.05$。每个报告值均取自100次试验的平均值。在图4中，每个玩家的初始策略均从区间 (0，w/n) 中均匀随机抽取，其中 w 是一个满足 $f(w) = 0$ 的值。

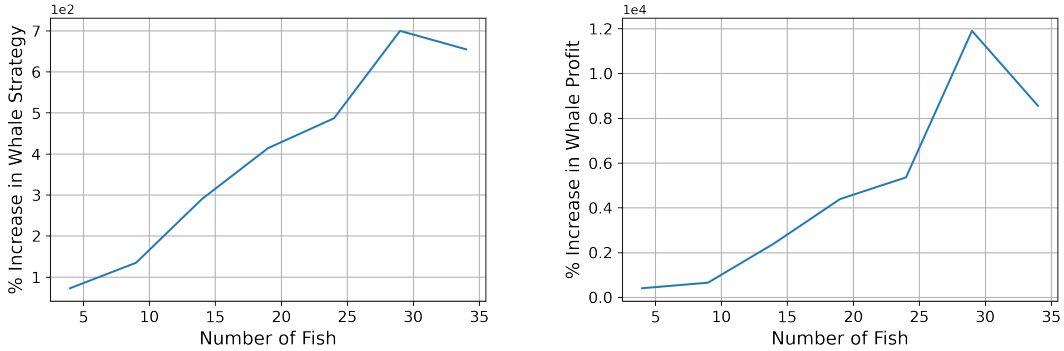

图5：与无约束均衡策略和利润相比，巨鲸策略和巨鲸利润的百分比增幅随小鱼数量的变化。

图4左侧的图表表明，在没有预算约束的情况下，达到唯一均衡所需的迭代次数会随着玩家数量的增加而超线性增长。右侧的图表显示，在有界策略更新的情形下，当 δ的值较小时，与无界策略更新的情形相比，达到均衡所需的迭代次数会显著增加。

在图5中，我们考虑这样一种情形：一名玩家拥有无限预算（我们称其为巨鲸），其余玩家均有一定预算 $M_i < q/n$ （这些玩家称为小鱼）。小鱼的预算从区间 $M_i \sim [0, q/n]$ 中均匀抽取，每条小鱼的初始策略则从区间 $[0, M_i]$中均匀随机抽取。小鱼选择的均衡策略是用尽全部预算，而巨鲸选择高于无约束均衡策略的策略，因此能够获得更高的利润。图5表明，随着小鱼数量增加，巨鲸选择的策略越来越大，获得的利润也越来越高。

无政府代价 均衡收益很容易求得为

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

类似地，可以证明，在每个代理人获得相同收益的条件下，最优收益为

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

无政府代价是通过均衡收益与最优收益之比得出的：

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

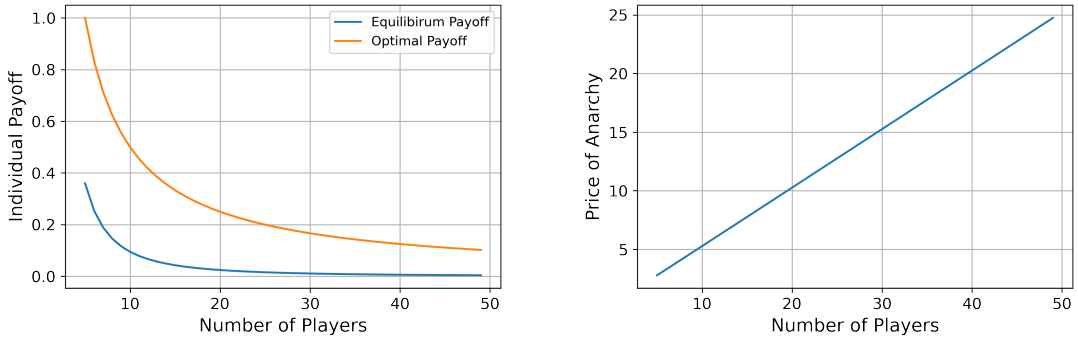

图 6: （左）玩家的个体收益与玩家数量的关系。（右）最优收益与均衡收益之比与玩家数量的关系。

我们再次固定 $\beta = 0.5$ 和 $\gamma = 0.05$。图 6 左侧的图展示了最优收益函数和均衡收益函数随玩家数量 n 的变化情况，而图 6 右侧的图展示了无政府代价随 n的变化情况。

C 放宽严格凹性

事实上，上述证明并不需要严格凹性。我们只需要 f在 0 处具有“某种曲率”。具体而言，只要对于所有满足 $0 < t < t'$的 t 和 t'，都有

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

用英文来说，这个条件是指从 0 到 t 的弦始终严格位于函数下方。对于一般函数 f，有时很难验证这一条件，因此我们将证明，这等价于一个（可能更容易处理的）性质：0 处的所有超梯度在所有点都严格高于函数。我们将证明，对于任意凹函数 $f : \mathbf{R}_+ \to \mathbf{R}$，且满足 $f(0) = 0$，以下两个陈述等价：（a）存在某个 $s' > 0$ 和 $\alpha \in \mathbf{R}$，使得对于每个满足 $0 \leq s \leq s'$ 的 s，都有

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

且 (b) 存在某个 $0 < t < t'$，使得

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

上述陈述可由 (a) 和 (b) 的否定推出。这个等价关系有一个简单的解释：如果点 (0，0) 与图像 f, $\{(s,\ f(s)) \mid s > 0\}$上的任意另外两点共线，那么函数 f 是一个分段函数，且从 0 开始有一个线性段。反过来说，如果函数 f 在 0 附近没有线性段（即，0 附近的每个线性上估计函数都严格位于 f 上方），那么任意一条弦都必须严格位于该函数下方。

证明。 正向蕴含非常简单：取 $t' = s'$，并令 t 为任意一个 $0 < t < s'$，则有

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

现在我们来考虑逆向蕴含。给定满足 (9) 的 $0 < t < t'$，我们将证明，对于任意 $0 \leq s \leq t$，都有

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

which 满足原命题，且 $\alpha = f(t)/t$。首先，容易证明

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

因为

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

其中，不等式由 f 的凹性以及 $f(0) = 0$ 这一事实得出。现在我们将证明，任何严格满足 (10) 的函数 f，即，

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

对于某个 $0 < s < t$，都不可能是凹函数。结论由逆否命题得出。为此，令 $0 < \gamma \leq 1$ 满足 $t = \gamma s + (1 - \gamma)t'$，则

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

因此 f 不可能是凹函数。不等式直接由条件 (9) 和 (11) 得出，第一个和第二个等式都由 γ 的定义得出。

D Rosen 条件

按比例分配博弈，即使是凹博弈，也不满足凹博弈均衡唯一性的 Rosen 条件 [10]。唯一性的 Rosen 条件是：如果存在某个 $z \geq 0$，满足 $z \neq 0$，那么

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

是一个严格单调算子；即，对于任意 $x \neq y$，我们有

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

那么就存在一个唯一的纯策略均衡。（这里， ∂_i 表示第 i个偏导数。）这是用于证明博弈中纯策略均衡唯一性的一个常见条件。我们将证明，对于凹比例分配博弈，即使在严格凹性，甚至强凹性和可微性等大多数“良好”假设下，这个条件通常也不成立。

设定 2　$x = y = \mathbf{1}$ 那么，利用 U 的定义，该条件可以写为)

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

但由于 $\mathbf{1}^T z > 0$，这可以改写为

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

显然，这并不适用于所有凹函数 f，因为只需取 $f(t) = \min\{t, 3n\}$ 即可。（磨光论证表明，即使在 f 严格凹且可微的情况下，这也构成一个合理的反例。）另一个更直接的反例是可微且严格凹的函数 $f(t) = (4n)^2 - (4n - t)^2,$，不过验证起来稍微困难一些。