Lecture 4: (Advanced?) Decentralized Exchanges

Guillermo Angeris

June 2022

Outline

Previous lecture

- Discussed decentralized exchanges (DEXs)
- Focused on a particular implementation: constant function market makers (CFMMs)
- Talked about some basic notions, such as ‘price’ and ‘portfolio value’

This lecture

- Recap the previous lecture with concrete examples
- Discuss some equivalences between portfolio value and trading functions
- Discuss individual-asset payoffs

Notation recap

- The notation used here is now (somewhat?) standard
- $R \in \mathbf{R}_+^n$ are the *reserves*
- $\varphi : \mathbf{R}_+^n \to \mathbf{R}$ is the *trading function*
- $\Delta \in \mathbf{R}_+^n$ is the *tendered basket*
- $\Lambda \in \mathbf{R}_+^n$ is the *received basket*
- $0 < \gamma \leq 1$ is the *trading fee*

Interface recap

- In a CFMM, a `swap(amountIn, amountOut)` accepts if

$$\varphi(R + \gamma\Delta - \Lambda) \geq \varphi(R)$$

where Δ is `amountIn` and Λ is `amountOut`

- When this happens, reserves are updated as

$$R \leftarrow R + \Delta - \Lambda$$

Arbitrage problem

- Given external market with price $c \in \mathbf{R}^n_+$, the arbitrage problem is

$$
\begin{array}{ll}
\text{maximize} & c^T(\Lambda - \Delta) \\
\text{subject to} & \varphi(R + \gamma\Delta - \Lambda) \geq \varphi(R) \\
& \Delta, \Lambda \geq 0
\end{array}
$$

acceptance of a CFMM

with variables $\Delta, \Lambda \in \mathbf{R}^n$

OPT ≥ 0

Arbitrage problem (equiv.)

$$\max.\ c^T(\Lambda - \Delta) \qquad R' = R + \Delta - \Lambda$$
$$\text{s.t.}\ \varphi(R + \Delta - \Lambda) \geq \varphi(R)$$
$$\Delta, \Lambda \geq 0$$

$$R - R' = \Lambda - \Delta$$

$$\cong \max.\ c^T(R - R')$$
$$\text{s.t.}\ \varphi(R') \geq \varphi(R)$$

$$\cong \max.\ -c^T R'$$
$$\text{s.t.}\ \varphi(R') \geq \varphi(R)$$

$$\cong \min.\ c^T R'$$
$$\text{s.t.}\ \varphi(R') \geq \varphi(R).$$

Arbitrage problem (equiv.)

- So the final problem is

$$\begin{array}{ll} \text{minimize} & c^T R' \\ \text{subject to} & \varphi(R') \geq \varphi(R) \\ & R' \geq 0 \end{array}$$

parametrised by c

$V(c)$

with variable $R' \in \mathbf{R}^n$

- Call optimal value $V(c)$, the 'portfolio value function'

No-arbitrage conditions

$$\left.\begin{array}{ll} \min. & c^T R' \\ \text{s.t.} & \varphi(R') \geq \varphi(R) \end{array}\right\} \longrightarrow$$

$$\mathcal{L}(R') = c^T R' + \lambda\big(\varphi(R) - \varphi(R')\big), \quad \lambda \geq 0$$

$$\nabla_{R'} \mathcal{L}(R') = 0 = c - \lambda \nabla \varphi(R') \Rightarrow c = \lambda \nabla \varphi(R')$$

Notes

- For the most part in this lecture, we will consider $\gamma = 1$ for simplicity
- This will simplify a lot of results
- But more general results can be derived

Outline

Linear trading function

$p \in \mathbb{R}^n_{++}$, $\quad \varphi(R) = p^T R.$

2-asset case

$p_1 \Delta_1 + p_2 \Delta_2 \geq p_1 \Lambda_1 + p_2 \Lambda_2$

$p_1 \Delta_1 = p_2 \Lambda_2$

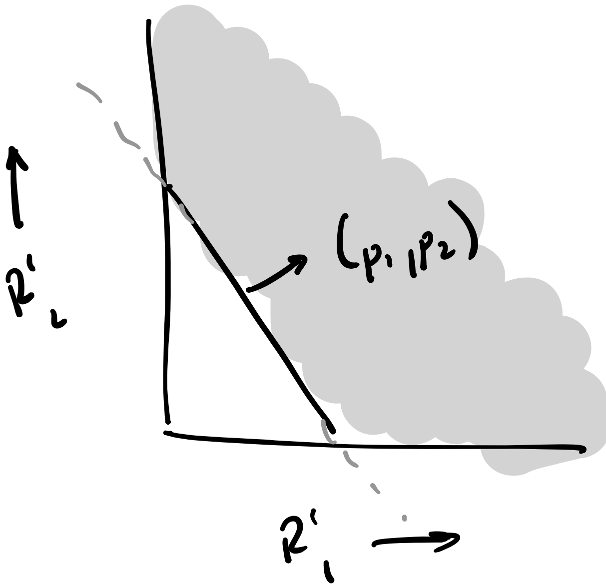
$$\varphi(R + \Delta - \Lambda) \geq \varphi(R)$$

$$\Vert$$

$$p^T(R + \Delta - \Lambda) \geq p^T R$$

$$\boxed{p^T \Delta \geq p^T \Lambda}$$

Linear trading function (reachable set, prices)



$$\{R' \mid \varphi(R') \geq \varphi(R)\}.$$

$$\nabla \varphi(R') = (p_1, p_2)$$

$$\varphi(R') = p^T R'$$

Linear trading function (portfolio value)

$$
\begin{aligned}
\min.\quad & c^T R' \\
\text{s.t.}\quad & p^T R' \geq \overbrace{p^T R}^{k} \\
& R' \geq 0
\end{aligned}
$$

$$\implies q = p_i R'_i$$

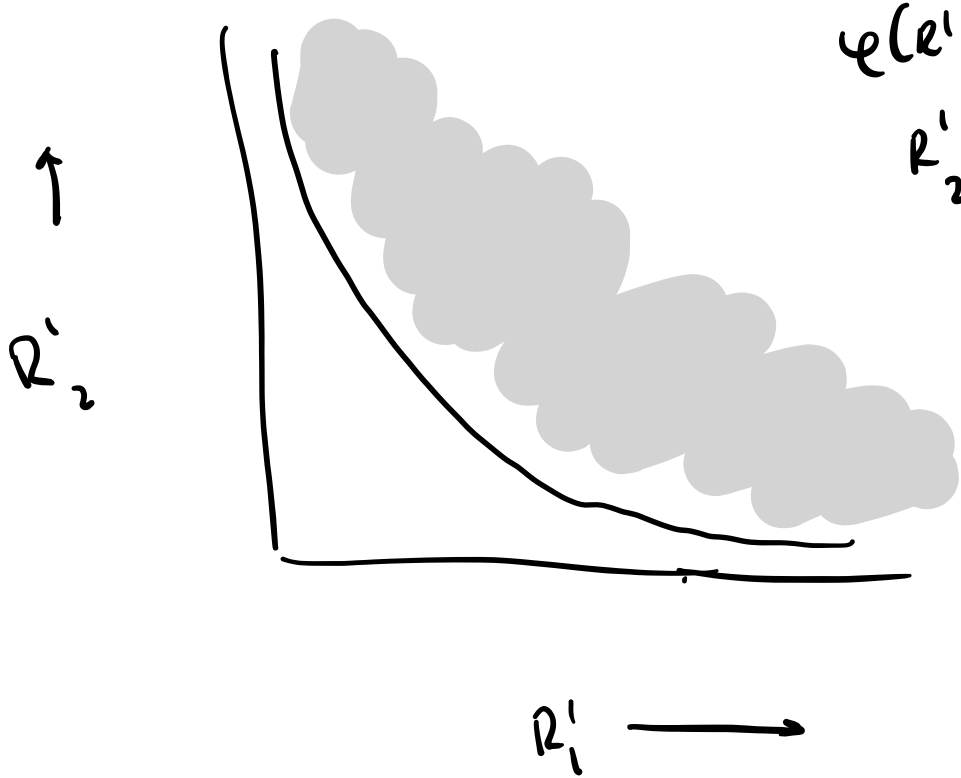
$$
\begin{aligned}
\to \min.\quad & \left(\frac{c}{p}\right)^T q \\
\text{s.t.}\quad & 1^T q \geq k \\
& q \geq 0
\end{aligned}
$$

$$V(c) = k \cdot \min_i \left\{ \frac{c_i}{p_i} \right\}.$$

Product trading function

$$\varphi(R_1, R_2) = \sqrt{R_1 R_2}$$

Product trading function (reachable set, prices)



$$\varphi(R') \geq \varphi(R) = k$$

$$R'_2 = \frac{k}{R'_1}$$

$$\nabla \varphi(R') = \frac{1}{2}\left(\sqrt{\frac{R'_2}{R'_1}}, \sqrt{\frac{R'_1}{R'_2}}\right)$$

$$\tilde{p} = \left(\frac{R_2}{R_1}, 1\right)$$

Product trading function (output given input)

Product trading function (portfolio value)

$$c = \lambda \nabla \varphi(R)$$

$$= \frac{\lambda}{2}\left(\sqrt{\frac{R'_2}{R'_1}} , \sqrt{\frac{R'_1}{R'_2}} \right)$$

$\uparrow \qquad \uparrow$

$$\frac{c_1}{c_2} = \frac{R'_2}{R'_1} \Rightarrow \boxed{c_1 R'_1 = c_2 R'_2}$$

$$\sqrt{c_1 c_2 k}$$

Outline

Now the question

- Now, where we were last time
- Given any portfolio value, can we recover a trading function?

Now the question

- Not every portfolio value function!
- By definition must be
  - 1-homogeneous
  - Nondecreasing
  - Concave

$$\min \; c^T R'$$
$$\text{s.t.} \quad \varphi(R') \geq \varphi(R)$$

Now the question

- Not every portfolio value function!
- By definition must be
  - 1-homogeneous
  - Nondecreasing
  - Concave
- Call these *consistent* portfolio value functions

Now the question

- Given any consistent portfolio value function, can we recover a trading function?

Now the question

- Given any consistent portfolio value function, can we recover a trading function?
- Yes!

Inverse mapping

$V(c)$

$$\tilde{\varphi}(R) = \inf_{c \geq 0} \left\{ c^T R - V(c) \right\}.$$

Pf. Show that $\tilde{\varphi}(R)$ has payoff V.

Call payoff of $\tilde{\varphi}$, $\tilde{V}$, ① $\tilde{V} \geq V$ ② $\tilde{V}$ "$\leq$" V

① $\left\{ \begin{array}{l} \min \ c^T R' \\ \text{s.t. } \tilde{\varphi}(R') \geq 0 \end{array} \right\}$ if R satisfies this then

$$c^T R' - V(c) \geq \tilde{\varphi}(R') \geq 0$$

$$c^T R' \geq V(c) \Rightarrow \tilde{V} \geq V$$

Inverse mapping (cont.)

(2) $R = \nabla V(c)$

For any g: $V(g) \le \overbrace{\nabla V(c)}^{R}{}^T (g - c) + V(c)$

(a) $c^T R = V(c)$

(b) R is feasible for $\tilde{V}$

$\Rightarrow \tilde{V} \le V \Rightarrow V = \tilde{V}$

What does this give us?

- We can construct complicated, interesting payoffs
- One example: we can construct fully decentralized options !
- These options do not require counterparties
- Only rely on people arbitraging the protocol

Second view on CFMMs

- We can view CFMMs as fully-decentralized portfolio management
- Only requires someone being able to arbitrage portfolio
- Risk-return tradeoff is specified by V
- Can construct a φ which gives this tradeoff

Outline

Final points

- Number of other interesting results in CFMMs
- Including ways of constructing very general payoffs
- Could be a special topic...

Next lecture

- Things that can only be done on the blockchain
- Flashloans, atomic arbitrage, sandwiching...
- And more spicy topics!