# A Geometric Perspective of CFMMs

## (Based on a WIP monograph)


Guillermo Angeris[1], Tarun Chitra[2], Theo Diamandis[1,3]

[1]Bain Capital Crypto

[2]Gauntlet

[3]MIT


Financial Cryptography 2023

# What's this tutorial about?

- A geometric framework for CFMMs that unifies existing results in the literature
  - Trading sets, reachable sets of reserves, and properties
  - Price definitions (it's convex analysis)
  - No arbitrage problem & 'routing' problem (just 'add em up')
  - Portfolio value function, derivation, and equivalences
  - Link between trading function and portfolio value function (new!!)

# What's this tutorial about?

- A geometric framework for CFMMs that unifies existing results in the literature
  - Trading sets, reachable sets of reserves, and properties
  - Price definitions (it's convex analysis)
  - No arbitrage problem & 'routing' problem (just 'add em up')
  - Portfolio value function, derivation, and equivalences
  - Link between trading function and portfolio value function (new!!)
- Some notes:
  - Many of the results we present are already in the literature in some form or another.
  - Will mostly look at fee-free case, but generalization is easy
  - Will include examples throughout

## Why care about convexity?

All markets that ‘make sense’ (*i.e.,* satisfy the properties we would want/expect) correspond to convex sets with certain properties.

## Why care about convexity?

All markets that ‘make sense’ (*i.e.,* satisfy the properties we would want/expect) correspond to convex sets with certain properties.

These sets give us a unified framework for CFMM theoretical results.

## What does it mean to ‘make sense’?

*Convex duality plays an essential role in many important financial problems. For example, it arises both in the minimization of convex risk measures and in the maximization of concave utility functions. Together with generalized convex duality, they also appear when an optimization is not immediately apparent, for instance in implementing dynamic hedging of contingent claims. Recognizing the role of convex duality in financial problems is crucial for several reasons. First, considering the primal and dual problem together gives the financial modeler the option to tackle the more accessible problem first.*

*(Peter Carr)*

# Outline

# Convex sets

- A set $X$ is convex if for all $x, y \in X$ and $\lambda \in [0, 1]$,

$$\lambda x + (1 - \lambda) y \in X$$

## Convex sets

- A set $X$ is convex if for all $x, y \in X$ and $\lambda \in [0, 1]$,

$$\lambda x + (1 - \lambda) y \in X$$

- For every $x_0 \in \operatorname{bd} X$, there exists a supporting hyperplane, *i.e.*, , there exists an $a$ such that

$$a^T x \le a^T x_0 \quad \forall x \in X$$

- Conversely, $X$ is convex if it is closed, has a nonempty interior, and every point on the boundary has a supporting hyperplane

# Convex functions

- Define the epigraph of a function as 'everything above the function', *i.e.*, , for a function $f : \mathbb{R}^n \to \mathbb{R}$,

$$\operatorname{epi} f = \{(x, w) \in \mathbb{R}^n \times \mathbb{R} : f(x) \leq w\}$$

- A function function is convex if and only if its epigraph is a convex set

## Convex functions

- Define the epigraph of a function as 'everything above the function', *i.e.*, , for a function $f : \mathbb{R}^n \to \mathbb{R}$,

$$\operatorname{epi} f = \{(x, w) \in \mathbb{R}^n \times \mathbb{R} : f(x) \leq w\}$$

- A function function is convex if and only if its epigraph is a convex set
- Of course, there are many other equivalent definitions of convexity as well

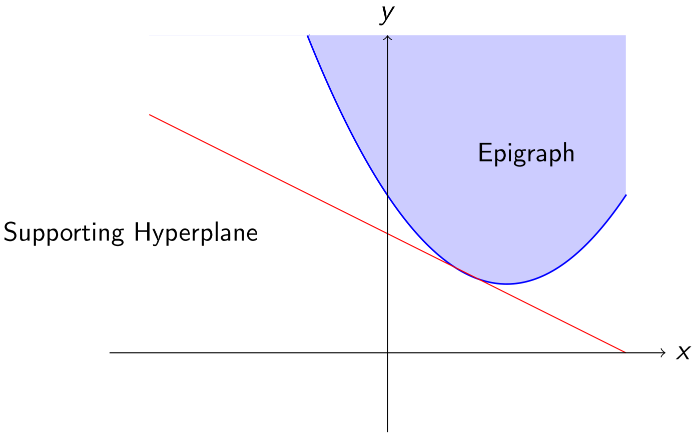
# Convex functions

- Define the epigraph of a function as 'everything above the function', *i.e.*, , for a function $f : \mathbb{R}^n \to \mathbb{R}$,

$$\text{epi}\, f = \{(x, w) \in \mathbb{R}^n \times \mathbb{R} : f(x) \leq w\}$$

- A function function is convex if and only if its epigraph is a convex set
- Of course, there are many other equivalent definitions of convexity as well
- First order condition: $f$ is convex if and only if for all $x, y \in \mathbb{R}^n$,

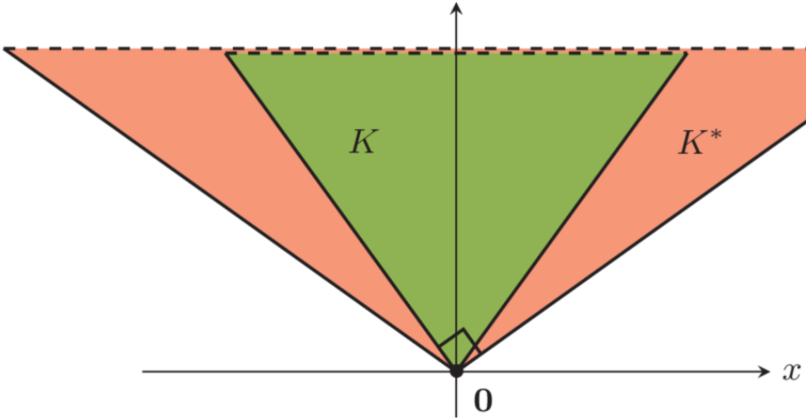
$$f(y) \geq f(x) + \nabla f(x)^T (y - x) \qquad (\textit{cf.}\text{ supporting hyperplane theorem})$$


y
Epigraph
Supporting Hyperplane
x

# Cones & dual cones

- A set $K$ is a cone if
$$x \in K \implies \lambda x \in K \quad \forall \lambda \geq 0$$
- The dual cone of $K$, denoted by $K^*$ is defined as
$$K^* = \{y : x^T y \geq 0 \quad \forall x \in K\}$$

# Cones & dual cones in pictures



# Conic duality

- A conic optimization problem and its dual are

$$\begin{array}{llcll} \text{minimize} & f(x) & \leftrightarrow & \text{minimize} & f^*(y) \\ \text{subject to} & x \in K & & \text{subject to} & y \in K^* \end{array}$$

- $f^*(y)$ is the conjugate function of $f$, defined as

$$f^*(y) = \sup_{x \in \operatorname{dom} f} \{x^T y - f(x)\}$$

- These problems have the same optimal value

# Subgradients

- A subgradient is a generalization of a gradient for non-differentiable functions
- Formally, for a convex function $f : \mathbb{R}^n \to \mathbb{R}$, a vector $g \in \mathbb{R}^n$ is a subgradient if

$$f(y) \geq f(x) + g^T(y - x) \quad \forall x, y \in \mathbb{R}^n$$

- The set of all subgradients of $f$ at $x$ is called the subdifferential, denoted $\partial f(x)$

## Subgradients

- A subgradient is a generalization of a gradient for non-differentiable functions
- Formally, for a convex function $f : \mathbb{R}^n \to \mathbb{R}$, a vector $g \in \mathbb{R}^n$ is a subgradient if

$$f(y) \geq f(x) + g^T(y - x) \quad \forall x, y \in \mathbb{R}^n$$

- The set of all subgradients of $f$ at $x$ is called the subdifferential, denoted $\partial f(x)$
- Compare this with the definition of convexity:

$$f(y) \geq f(x) + \nabla f(x)^T(y - x) \quad \forall x, y \in \mathbb{R}^n$$

- If $f$ is differentiable, then $\partial f(x) = \{\nabla f(x)\}$

# Set addition

- We define the addition between two sets as the Minkowski sum:

$$X + Y = \{x + y \mid x \in X, y \in Y\}$$

- Sometimes we will abuse notation and 'add' a vector to a set:

$$x + Y = \{x + y \mid y \in Y\}$$

# Outline

# Trades with CFMMs

- A *trade* $\Delta \in \mathbb{R}^n$ with a CFMM subtracts transfers $\Delta_i$ units of token $i$ from the CFMM to the trader
  - Positive entries denote tokens received by the trader from the CFMM
  - Negative entries denote tokens tendered by the trader to the CFMM
- The sign does not matter; we take the trader's point of view by convention
- Note the difference with prior work that considered a trade $(\Delta, \Lambda) \in \mathbb{R}^n_+ \times \mathbb{R}^n_+$, where the tendered and received baskets are split.

# The trading set

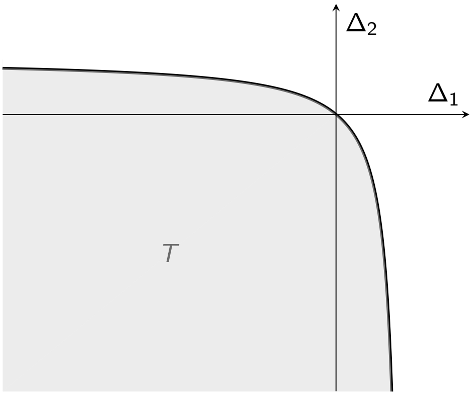
- The *trading set* (set of allowable trades) $T(R) \in \mathbb{R}^n$ at some fixed reserves $R$ has the following properties:
  - $T(R)$ is a closed, convex set
  - $0 \in T(R)$
  - If $\Delta \in T(R)$ then $\Delta' \leq \Delta$ implies $\Delta' \in T(R)$.

# The trading set

- The *trading set* (set of allowable trades) $T(R) \in \mathbb{R}^n$ at some fixed reserves $R$ has the following properties:
  - $T(R)$ is a closed, convex set
  - $0 \in T(R)$
  - If $\Delta \in T(R)$ then $\Delta' \leq \Delta$ implies $\Delta' \in T(R)$.
- Some immediate consequences:
  - Trades on the relative boundary are the 'best' we can do
  - Boundary completely describes the trading set

# Uniswap trading set

- Uniswap's trading set is $T(R) = \{\Delta \mid (R_1 - \Delta_1)(R_2 - \Delta_2) \geq k\}$



# Aggregate CFMMs

- Trading sets are closed under Minkowski addition: if $T_1$ and $T_2$ are trading sets, then $T_1 + T_2$ is also a trading set
  - We can quickly verify this
- Additionally, $\Delta \in T_1 + T_2$ means that there are trades $\Delta_1 \in T_1$ and $\Delta_2 \in T_2$ such that $\Delta = \Delta_1 + \Delta_2$.
- 'Aggregate' CFMMs can be viewed as just one big CFMM

## Adding liquidity

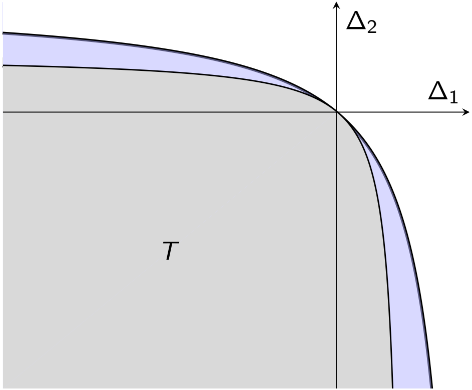
- For $k \geq 0$, we can 'add liquidity' to CFMM $T$ by scaling the trading set:

$$kT = \{k\Delta \mid \Delta \in T\}$$

- Now, trades $k$ times as large are valid

# Adding liquidity to Uniswap

- Assume that $R_1 = R_2 = 1$ initially. Add 1 unit of liquidity to each (blue)t:



# Projections

- Consider a 'selector matrix' $A \in \mathbb{R}^{m \times n}$, which selects a subset of tokens from a trade $\Delta \in \mathbb{R}^n$.
- The set of trades in $T$ with the reduced token set, denoted $AT$ is also a CFMM, where
$$AT = \{A\Delta \mid \Delta \in T\}$$
- Useful for reasoning about things like 3-pools!

# Outline

# Path independence

- For the remainder of this tutorial, we will assume that the CFMM is *path independent*:

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta + \Delta' \in T(R)$$

# Path independence

- For the remainder of this tutorial, we will assume that the CFMM is *path independent*:

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta + \Delta' \in T(R)$$

- There is no difference between performing the trades sequentially or in aggregate

# Path independence

- For the remainder of this tutorial, we will assume that the CFMM is *path independent*:

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta + \Delta' \in T(R)$$

- There is no difference between performing the trades sequentially or in aggregate
- **Note:** path independence corresponds to the fee-free case and makes proofs easier for the sake of this tutorial
  - In the case with fees, we have 'path deficiency': splitting trades hurts
  - We must consider the 'one step' case and multi-trade cases separately

# Reachable set

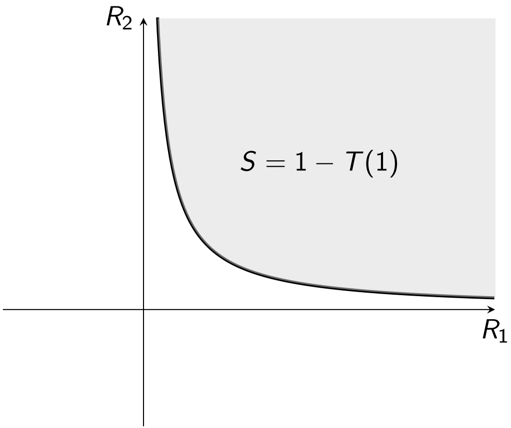
- Define the *reachable set* $S$ as the set of all possible reachable reserves, starting at some initial reserves $R$:
$$S = \{R - \Delta \mid \Delta \in T(R)\}$$
- Note the negative sign in front of $\Delta$ due to CFMM's (LP's) perspective

# Reachable set

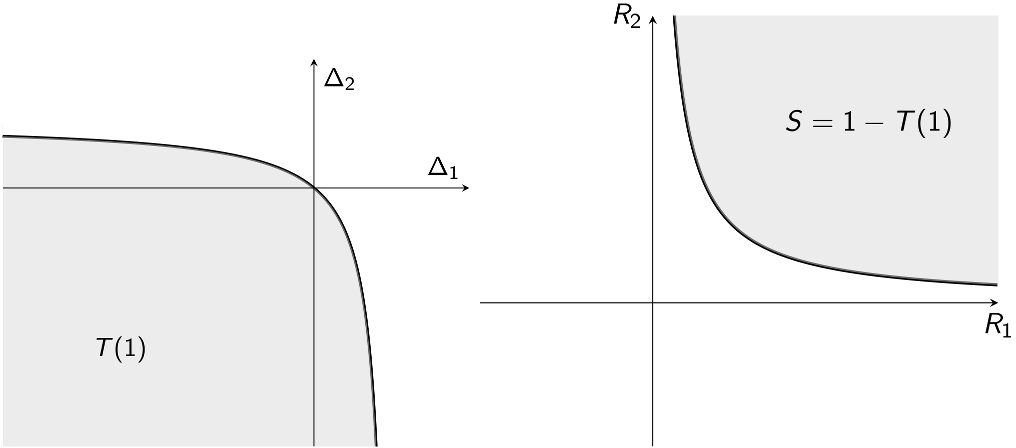
- Define the *reachable set* $S$ as the set of all possible reachable reserves, starting at some initial reserves $R$:
$$S = \{R - \Delta \mid \Delta \in T(R)\}$$
- Note the negative sign in front of $\Delta$ due to CFMM's (LP's) perspective
- More formally, $S$ is such that every trading set $T(R')$ for any reachable $R'$ starting from $R$ can be written as
$$T(R') = R' - S$$
- Path independence means $S$ does not change as trades are performed

# Reachable set

- What does this look like for Uniswap? Familiar $xy \geq 1$ graph!



# Characterizations in terms of $S$ and $T$ are equivalent:



# Importance of path independence

- **Claim:** Whenever the CFMM is path independent, the set of reachable reserves does not depend on $R'$, *i.e.*, we have that for any reachable $R'$, $R - T(R) = R' - T(R')$. We then set $S = R - T(R)$.

- **Proof:**

# Proof

- Only consider $R'$ reachable in 1 step; result follows by induction

# Proof

- Only consider $R'$ reachable in 1 step; result follows by induction
- Rewrite path independence as

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta' \in T(R) - \Delta \iff T(R - \Delta) = T(R) - \Delta$$

# Proof

- Only consider $R'$ reachable in 1 step; result follows by induction
- Rewrite path independence as

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta' \in T(R) - \Delta \iff T(R - \Delta) = T(R) - \Delta$$

- Proof follows from setting $S = R' - T = R - T(R)$ and

$$R' - T(R') = (R - \Delta) - T(R - \Delta) = R - \Delta - T(R) + \Delta = R - T(R).$$

# Reachable set properties

- The set $S$ is a nonempty closed convex set
- Given any $R \in S$, we have that for any $R' \geq R$, we know $R' \in S$.

# Reachable set properties

- The set $S$ is a nonempty closed convex set
- Given any $R \in S$, we have that for any $R' \geq R$, we know $R' \in S$.
- Thus, from the second property, $S + \mathbb{R}^n_+ \subseteq S$

# Outline

## The trading function

- We define the trading function as

$$\phi(R) = \sup\{\lambda > 0 \mid R/\lambda \in S\}$$

# The trading function

- We define the trading function as

$$\phi(R) = \sup\{\lambda > 0 \mid R/\lambda \in S\}$$

- Clearly, $\phi(R) \geq 1$ iff $R \in S$
- The supremum is always achieved since the set is closed

# The trading function

- We define the trading function as

$$\phi(R) = \sup\{\lambda > 0 \mid R/\lambda \in S\}$$

- Clearly, $\phi(R) \geq 1$ iff $R \in S$
- The supremum is always achieved since the set is closed
- $\phi$ is non-decreasing, concave, and 1-homogeneous

# Trading function $\rightarrow$ trading set

- Trading set can be recovered as

$$S = \{R \in \mathbb{R}^n_+ \mid \phi(R) \geq 1\},$$

- Set and function representations are equivalent!
- In fact, $\phi$ is unique up to a scalar constant: any two 1-homogeneous, nondecreasing, concave trading functions that both have feasible set $S$ differ only by a positive scalar constant.

# Uniswap's trading function

- Recall that Uniswap's feasible set is

$$S = \{(R_1, R_2) \in \mathbb{R}^2_+ \mid R_1 R_2 \geq k\}$$

- We will show that

$$\phi(R) = \sup\{\lambda > 0 \mid R/\lambda \in S\} = \sqrt{\frac{R_1 R_2}{k}}$$

- This function is clearly 1-homogeneous, non-decreasing, and concave

# Derivation: Uniswap's trading function

## Derivation: Uniswap's trading function

# Derivation: Uniswap's trading function

# Liquidity cone

- We will define the *liquidity cone* for a CFMM as

$$\begin{aligned} C &= \mathrm{cl}(\{(R, \lambda) \in \mathbb{R}^{n+1} \mid R/\lambda \in S,\ \lambda > 0\}) \\ &= \{(R, \lambda) \in \mathbb{R}^{n+1} \mid R/\lambda \in S,\ \lambda > 0\} \cup (\mathbb{R}^n_+ \times \{0\}) \end{aligned}$$

- The second line comes from the assumption that $S$ gets arbitrarily close to the axes (*cf.* Uniswap)

# Liquidity cone

- We will define the *liquidity cone* for a CFMM as

$$
\begin{aligned}
C &= \mathrm{cl}(\{(R, \lambda) \in \mathbb{R}^{n+1} \mid R/\lambda \in S,\ \lambda > 0\}) \\
&= \{(R, \lambda) \in \mathbb{R}^{n+1} \mid R/\lambda \in S,\ \lambda > 0\} \cup (\mathbb{R}^n_+ \times \{0\})
\end{aligned}
$$

- The second line comes from the assumption that $S$ gets arbitrarily close to the axes (*cf.* Uniswap)
- We can then write

$$
\phi(R) = \sup\{\lambda \mid (R, \lambda) \in C\}
$$

- The definition of $\phi$ is a particular choice of support function for the cone $C \subseteq \mathbb{R}^{n+1}$

# Uniswap's liquidity cone

- In general, the liquidity cone for a CFMM with trading function $\phi$ is

$$C = \{(R, \lambda) \in \mathbb{R}^n_+ \mid \phi(R) \geq \lambda\},$$

# Uniswap's liquidity cone

- In general, the liquidity cone for a CFMM with trading function $\phi$ is

$$C = \{(R, \lambda) \in \mathbb{R}^n_+ \mid \phi(R) \geq \lambda\},$$

- The liquidity cone for Uniswap is

$$C = \{(R_1, R_2, \lambda) \in \mathbb{R}^2_+ \mid \sqrt{R_1 R_2} \geq \sqrt{k}\lambda\}.$$

# Dual

- Recall that by the definition of the dual cone, we have

$$C^* = \{(c, \eta) \in \mathbb{R}^2_+ \times \mathbb{R} \mid c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in C\},$$

# Dual

- Recall that by the definition of the dual cone, we have

$$C^* = \{(c, \eta) \in \mathbb{R}^2_+ \times \mathbb{R} \mid c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in C\},$$

- Thus, the dual for Uniswap's liquidity cone is then

$$C^* = \{(c, \eta) \in \mathbb{R}^2_+ \times \mathbb{R} \mid 2\sqrt{kc_1 c_2} + \eta \geq 0\}.$$

- We will derive this shortly

# Dual derivation

# Dual derivation

# Dual derivation

# Trading function conjugate

- The 'conjugate' function of $\phi$ is

$$\begin{aligned}\phi^*(c) &= \inf_R \left(c^T R - \phi(R)\right) \\ &= \inf_{(R,\lambda)\in C} (c,-1)^T(R,\lambda)\end{aligned}$$

# Trading function conjugate

- The 'conjugate' function of $\phi$ is

$$\begin{aligned} \phi^*(c) &= \inf_R \left( c^T R - \phi(R) \right) \\ &= \inf_{(R,\lambda) \in C} (c, -1)^T (R, \lambda) \end{aligned}$$

- Since $C$ is a cone, we can also write this as

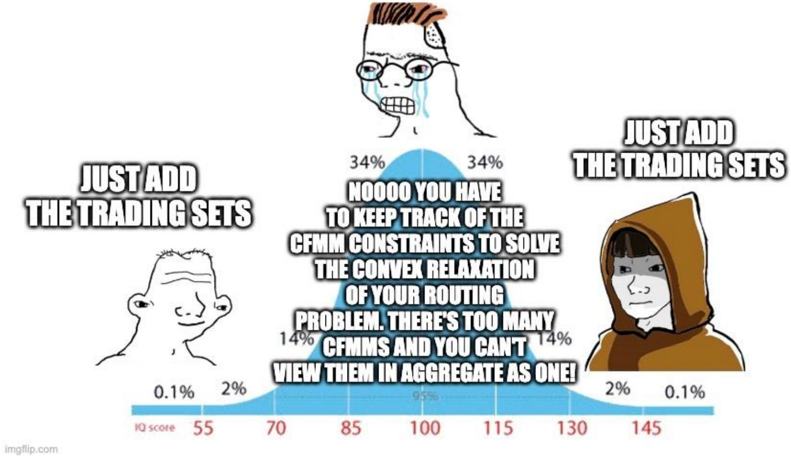
$$\phi^*(c) = I_{C^*}(c, -1)$$

## Aggregate CFMMs

- If $S$ and $S'$ are feasible sets, then the set $S + S'$ will also be a feasible set (nonempty, closed, convex monotonic), *i.e.*, correspond to a CFMM

# Aggregate CFMMs

- If $S$ and $S'$ are feasible sets, then the set $S + S'$ will also be a feasible set (nonempty, closed, convex monotonic), *i.e.*, correspond to a CFMM
- Again, we see that both CFMMs together are just 'one big CFMM'
- And we can recover a trading function from this big CFMM


JUST ADD THE TRADING SETS
34%
34%
NOOOO YOU HAVE TO KEEP TRACK OF THE CFMM CONSTRAINTS TO SOLVE THE CONVEX RELAXATION OF YOUR ROUTING PROBLEM. THERE'S TOO MANY CFMMS AND YOU CAN'T VIEW THEM IN AGGREGATE AS ONE!
JUST ADD THE TRADING SETS
14%
14%
0.1%
2%
2%
0.1%
IQ score
55
70
85
100
115
130
145
imgflip.com

# Outline

# Price cone

- We define the price cone (or just 'prices') at some reserves $R$ as

$$K(R) = \bigcap_{R' \in S} \{\nu \in \mathbb{R}^n \mid \nu^T(R' - R) \geq 0\}$$

# Price cone

- We define the price cone (or just 'prices') at some reserves $R$ as

$$K(R) = \bigcap_{R' \in S} \{\nu \in \mathbb{R}^n \mid \nu^T (R' - R) \geq 0\}$$

- If $S = S_1 + \cdots + S_k$, then

$$K(R) = K_1(R) \cap \cdots \cap K_k(R)$$

- This is related to the no-arbitrage problem

# Arbitrage problem

- Consider the problem of making a trade $\Delta$ with a CFMM that has reserves $R_0$ to maximize profit, with external market prices $c \in \mathbb{R}^n$

$$
\begin{array}{ll}
\text{maximize} & c^T \Delta \\
\text{subject to} & R^0 - \Delta \in S,
\end{array}
$$

# Arbitrage problem

- Consider the problem of making a trade $\Delta$ with a CFMM that has reserves $R_0$ to maximize profit, with external market prices $c \in \mathbb{R}^n$

$$\begin{array}{ll}\text{maximize} & c^T \Delta \\ \text{subject to} & R^0 - \Delta \in S,\end{array}$$

- This problem is equivalent to

$$\begin{array}{ll}\text{minimize} & c^T R \\ \text{subject to} & R \in S.\end{array}$$

# Arbitrage problem is an important primitive

- Efficient order routing algorithms use the arbitrage problem as a primitive (come to our talk on Tuesday!)
- From before, we see that we can group CFMMs in useful ways

# Arbitrage problem is an important primitive

- Efficient order routing algorithms use the arbitrage problem as a primitive (come to our talk on Tuesday!)
- From before, we see that we can group CFMMs in useful ways
- Example: Uniswap v3 pools can be viewed as many CFMMs (one for each tick) or one big CFMM (per asset pair) as appropriate

# Arbitrage problem is an important primitive

- Efficient order routing algorithms use the arbitrage problem as a primitive (come to our talk on Tuesday!)
- From before, we see that we can group CFMMs in useful ways
- Example: Uniswap v3 pools can be viewed as many CFMMs (one for each tick) or one big CFMM (per asset pair) as appropriate
- Just choose whatever is easiest to arbitrage over!

## Optimality conditions

- The optimality conditions for the equivalent problem are

$$c \in K(R^\star)$$

- This follows from the fact that an optimal solution $R^\star$ must satisfy

$$c^T R^\star \leq c^T R \iff c \in K(R^\star)$$

- The optimal action is to set the reserves such that the external market price $c$ lies in the price cone $K(R^\star)$, as expected.

## Optimality conditions

- The optimality conditions for the equivalent problem are

$$c \in K(R^\star)$$

- This follows from the fact that an optimal solution $R^\star$ must satisfy

$$c^T R^\star \leq c^T R \iff c \in K(R^\star)$$

- The optimal action is to set the reserves such that the external market price $c$ lies in the price cone $K(R^\star)$, as expected.
- Often (2 asset case), this is a one-dimensional root finding problem

# Outline

# What does bounded liquidity mean?

- All CFMMs so far have placed liquidity on $[0, \infty)$, but what if we only want liquidity when the prices are in a compact set $P \subset [0, \infty)$?

- Formal statement for the condition of placing liquidity on $[0, \infty)$:

$$\forall p \in [0, \infty],\ \exists\ \delta(p) \in \mathbb{R}^n \text{ such that } p \in K(R + \delta(p))$$

- Two equivalent conditions for bounding liquidity to $P$:
  1. Reachability condition:

$$\forall p \in P\ \ \exists \delta(p) \in \mathbb{R}^n \text{ such that } p \in K(R + \delta(p))$$

  2. Boundedness condition: There exists $\Delta_i^\star < \infty$ such that

$$\sup\{\Delta_i \mid \Delta \in T\} = \Delta_i^\star$$

# Uniswap V3

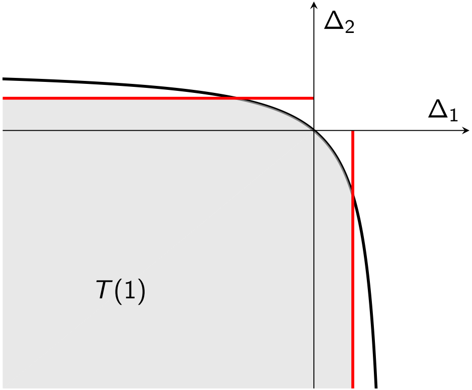
- The first (and most popular by trading volume) bounded liquidity CFMM is Uniswap V3 which has trading function

$$\varphi(R) = \sqrt{(R_1 + \alpha)(R_2 + \beta)}$$

  for $\alpha, \beta \in \mathbb{R}_+$
- We can write the trading function $T(R)$ for this function as the intersection of the Uniswap trading function and two hyperplanes
- We call the hyperplane constraints, *liquidity constraints*

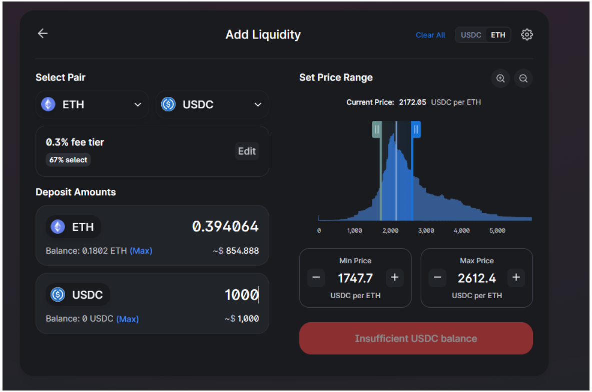
# Trading Set for Uniswap V3

This claim demonstrates that the trading set is a compact set in $\mathbb{R}^2$:



# Sums of Bounded Liquidity CFMMs

- We can take sums of bounded liquidity CFMMs just as we did in the last section — this is how people construct aggregate CFMMs in practice
- Note that this lets users express more complex payoff functions for LPs, *e.g.*, use Uniswap V3 to replicate a generic order book:



## Pushing the limits of Bounded Liquidity

- A natural inverse problem: if I have a payoff $\phi : \mathbb{R}^n \to \mathbb{R}$ how can I construct bounded liquidity CFMMs to replicate it?
- It turns out you need to be able to take the correct limits of bounded liquidity CFMMs (*i.e.,* as the Uniswap V3 tick size goes to zero)
- One way of representing this is via the portfolio value function which represents the value of an LP's stake in a CFMM
- Decomposing a portfolio value function into simpler components will allow one to replicate arbitrary 1-homogeneous, concave payoffs

# Outline

# What is the Portfolio Value Function?

- One way of measuring LP returns is to look at the *portfolio value function*
- This is a way of measuring how much an LP's assets are relative to a numéraire (such as USD, BTC, or ETH)
- Our goal is to define the PV function completely in terms of convex analytic objects and to demonstrate invariance and compositional properties
- Given these properties, we will then demonstrate how they make LP return estimation much easier in a variety of contexts

# Defining the Portfolio value function

- We next define the *portfolio value function* of a set $S$ with some prices $c \in \mathbb{R}^n$ as

$$V(c) = \inf_{R \in S} c^T R$$

## Defining the Portfolio value function

- We next define the *portfolio value function* of a set $S$ with some prices $c \in \mathbb{R}^n$ as

$$V(c) = \inf_{R \in S} c^T R$$

- Interpreted as the minimum possible value of the current reserves
- Alternatively: value of the total reserves when arbitrage is allowed

# Defining the Portfolio value function

- We next define the *portfolio value function* of a set $S$ with some prices $c \in \mathbb{R}^n$ as
$$V(c) = \inf_{R \in S} c^T R$$
- Interpreted as the minimum possible value of the current reserves
- Alternatively: value of the total reserves when arbitrage is allowed
- Properties:
  - Concave (infimum over a family of affine functions)
  - 1-homogenous
  - nondecreasing
  - nonnegative whenever $c \geq 0$ (and $-\infty$ otherwise)

# Portfolio value function equivalence

- We can show an equivalence between the PV function and the set $S$
- $S \to V$: Clearly for some $S$, a $V$ exists and is unique (by def!)
- $V \to S_V$: We will construct a set $S_V$ from $V$ and see that this is $S$

# Constructing $S$ from portfolio value function

$$S_V = \bigcap_{c \in \mathbb{R}^n_+} \{R \in \mathbb{R}^n_+ \mid c^T R \geq V(c)\}$$

- This set is nonempty, closed, convex (intersection of hyperplanes)

# Constructing $S$ from portfolio value function

$$S_V = \bigcap_{c \in \mathbb{R}^n_+} \{R \in \mathbb{R}^n_+ \mid c^T R \geq V(c)\}$$

- This set is nonempty, closed, convex (intersection of hyperplanes)
- It is the set of supergradients of $V$ at 0 ($V(0) = 0$): $S_V = -\partial(-V)(0)$

# Constructing $S$ from portfolio value function

$$S_V = \bigcap_{c \in \mathbb{R}^n_+} \{R \in \mathbb{R}^n_+ \mid c^T R \geq V(c)\}$$

- This set is nonempty, closed, convex (intersection of hyperplanes)
- It is the set of supergradients of $V$ at 0 ($V(0) = 0$): $S_V = -\partial(-V)(0)$
- The portfolio value function of $S_V$ is

$$\inf\{c^T R \mid R \in \mathbb{R}^n_+ \text{ satisfies } c'^T R \geq V(c') \text{ for all } c' \in \mathbb{R}^n_+\}$$

- We can prove that this is equal to $V(c)$

# Equivalence proof

- Let $-g \in \partial(-V)(c)$ be a subgradient of $-V$ at $c > 0$
- Then for any $c' \in \mathbb{R}^n_+$
$$V(c') \leq V(c) + g^T(c' - c)$$
- **Idea:** we will show that $V(c) = g^T c$ and then that $g \in S'$
- This shows that $g$ is a minimizer of PV of $S_V$, therefore
$$\inf\{c^T R \mid R \in \mathbb{R}^n_+ \text{ satisfies } c'^T R \geq V(c') \text{ for all } c' \in \mathbb{R}^n_+\} = V(c)$$

# Equivalence proof II

- First, note that $V(2c) \leq V(c) + g^T c$.
- By 1-homogeneity, we have that $V(2c) = 2V(c)$ so we get $V(c) \leq g^T c$

# Equivalence proof II

- First, note that $V(2c) \leq V(c) + g^T c$.
- By 1-homogeneity, we have that $V(2c) = 2V(c)$ so we get $V(c) \leq g^T c$
- Similarly, using $c' = 0$, we have that $V(c) \geq g^T c$
- Together, we have $V(c) = g^T c$

# Equivalence proof II

- First, note that $V(2c) \leq V(c) + g^T c$.
- By 1-homogeneity, we have that $V(2c) = 2V(c)$ so we get $V(c) \leq g^T c$
- Similarly, using $c' = 0$, we have that $V(c) \geq g^T c$
- Together, we have $V(c) = g^T c$
- Thus, $g \in S'$ and the set $S_V$ has PV given by $V$
- This shows an equivalence between feasible sets and consistent PV functions

# Summing portfolio value functions

- From this construction we can show that PV's sum!

$$S_{V+V'} = S_V + S_{V'}$$

- In addition, for any $\alpha \geq 0$

$$S_{\alpha V} = \alpha S_V$$

## PV sum proof sketch

- Easy way:

$$S_V + S_{V'} \subseteq S_{V+V'}.$$

# PV sum proof sketch

- Easy way:
$$S_V + S_{V'} \subseteq S_{V+V'}.$$

- Other way: $R \in S_V$ and $R' \in S_{V'}$ will have $c^T R \geq V(c)$

# PV sum proof sketch

- Easy way:
$$S_V + S_{V'} \subseteq S_{V+V'}.$$

- Other way: $R \in S_V$ and $R' \in S_{V'}$ will have $c^T R \geq V(c)$

- So $c^T(R + R') \geq V(c) + V'(c)$

## PV sum proof sketch

- Easy way:
$$S_V + S_{V'} \subseteq S_{V+V'}.$$
- Other way: $R \in S_V$ and $R' \in S_{V'}$ will have $c^T R \geq V(c)$
- So $c^T(R + R') \geq V(c) + V'(c)$
- If $\bar{R} \in S_{V+V'}$, then $c^T \bar{R} \geq V(c) + V'(c)$ for all $c > 0$ by def

# PV sum proof sketch

- Easy way:
$$S_V + S_{V'} \subseteq S_{V+V'}.$$
- Other way: $R \in S_V$ and $R' \in S_{V'}$ will have $c^T R \geq V(c)$
- So $c^T(R + R') \geq V(c) + V'(c)$
- If $\bar{R} \in S_{V+V'}$, then $c^T \bar{R} \geq V(c) + V'(c)$ for all $c > 0$ by def
- Thus,
$$-\bar{R} \in \partial(-V - V')(0) = \partial(-V)(0) + \partial(-V')(0).$$

# Portfolio value $\to$ trading function

- Given a PV, we showed that there is a feasible set $S_V$ that replicates it
- We also know we can construct a 1-homogeneous $\phi$ from any feasible set

# Portfolio value $\rightarrow$ trading function

- Given a PV, we showed that there is a feasible set $S_V$ that replicates it
- We also know we can construct a 1-homogeneous $\phi$ from any feasible set
- Thus, we can construct a 1-homogenous trading function from a PV function:

$$\phi(R) = \inf_{c>0} \left( \frac{c^T R}{V(c)} \right)$$

- And this function is unique up to a scaling constant (and concave, nondecreasing, 1-homogeneous)

# Duality

- From strong duality, we have that

$$\begin{aligned} V(c) &= \sup_{\lambda>0} \inf_{R} \left( c^T R - \lambda(\phi(R) - 1) \right) \\ &= \sup_{\lambda>0} \lambda \left( \inf_{R} \left( c^T R/\lambda - \phi(R) \right) - 1 \right) \end{aligned}$$

# Duality

- From strong duality, we have that

$$
\begin{aligned}
V(c) &= \sup_{\lambda > 0} \inf_{R} \left( c^T R - \lambda(\phi(R) - 1) \right) \\
&= \sup_{\lambda > 0} \lambda \left( \inf_{R} \left( c^T R / \lambda - \phi(R) \right) - 1 \right)
\end{aligned}
$$

- The inner inf can be recognized as the dual cone, and we may write

$$
V(c) = \sup_{\lambda > 0} \left( \lambda I_{C^*}(c/\lambda, -1) - \lambda \right)
$$

# Duality II

- Since $\lambda > 0$ then $\lambda I_{C^*} = I_{C^*}$ so
$$V(c) = \sup_{(c/\lambda, -1) \in C^*} \lambda.$$
- Since $x \in C^*$ if and only if $\lambda x \in C^*$ we get
$$V(c) = \sup_{(c, -\eta) \in C^*} \eta.$$

# Duality II

- Since $\lambda > 0$ then $\lambda I_{C^*} = I_{C^*}$ so

$$V(c) = \sup_{(c/\lambda, -1) \in C^*} \lambda.$$

- Since $x \in C^*$ if and only if $\lambda x \in C^*$ we get

$$V(c) = \sup_{(c, -\eta) \in C^*} \eta.$$

- There is a clear duality between $V$ and $\phi$:

$$\phi(R) = \sup\{\lambda \mid (R, \lambda) \in C\}$$

## Duality: Proof

- Note that the value of the PV function $V(c) = \inf\{c^T R \mid (R, 1) \in C\}$ is the same as finding the largest $\eta$ such that

$$\eta \leq c^T R \qquad \text{for all } (R, 1) \in C.$$

## Duality: Proof

- Note that the value of the PV function $V(c) = \inf\{c^T R \mid (R, 1) \in C\}$ is the same as finding the largest $\eta$ such that

$$\eta \leq c^T R \qquad \text{for all } (R, 1) \in C.$$

- Multiplying both sides by $\lambda > 0$ and using the fact that $C$ is a cone

$$\lambda\eta \leq c^T R' \iff (R', \lambda)^T (c, -\eta) \geq 0 \qquad \text{for all } (R', \lambda) \in C$$

# Duality: Proof

- Note that the value of the PV function $V(c) = \inf\{c^T R \mid (R, 1) \in C\}$ is the same as finding the largest $\eta$ such that

$$\eta \leq c^T R \qquad \text{for all } (R, 1) \in C.$$

- Multiplying both sides by $\lambda > 0$ and using the fact that $C$ is a cone

$$\lambda\eta \leq c^T R' \iff (R', \lambda)^T (c, -\eta) \geq 0 \qquad \text{for all } (R', \lambda) \in C$$

- This happens iff $(c, -\eta) \in C^*$, by definition of the dual cone

## Duality: Proof

- Note that the value of the PV function $V(c) = \inf\{c^T R \mid (R, 1) \in C\}$ is the same as finding the largest $\eta$ such that

$$\eta \leq c^T R \qquad \text{for all } (R, 1) \in C.$$

- Multiplying both sides by $\lambda > 0$ and using the fact that $C$ is a cone

$$\lambda\eta \leq c^T R' \iff (R', \lambda)^T (c, -\eta) \geq 0 \qquad \text{for all } (R', \lambda) \in C$$

- This happens iff $(c, -\eta) \in C^*$, by definition of the dual cone
- $V(c)$ is given by the largest possible $\eta$ satisfying $(c, -\eta) \in C^*$, so

$$V(c) = \sup\{\eta \mid (c, -\eta) \in C^*\}$$

## Summming trading functions

- **Question:** What does adding feasible sets mean for trading functions?

# Summing trading functions

- **Question:** What does adding feasible sets mean for trading functions?
- **Answer:** infimal convolution: given $S$ and $S'$ with $\phi$ and $\phi'$, then the trading function corresponding to $S + S'$ is

$$(\phi \square \phi')(R) = \sup_x \left(\phi(x) + \phi'(R - x)\right)$$

## Summing trading functions

- **Question:** What does adding feasible sets mean for trading functions?
- **Answer:** infimal convolution: given $S$ and $S'$ with $\phi$ and $\phi'$, then the trading function corresponding to $S + S'$ is

$$(\phi \square \phi')(R) = \sup_x \left(\phi(x) + \phi'(R - x)\right)$$

- This operation is associative and commutative
- But harder to reason able than the feasible sets or portfolio value functions

# Outline

# Putting it all together

- Geometry of the last section was to show how to solve the inverse problem of going from a payoff function to a trading function and/or trading set
- We'll explore a few non-trivial (*i.e.,* non-Uniswap, compact support) examples of payoff functions and how to perform the replication
- These examples will demonstrate the power of the geometric lens of CFMMs versus the analytic lens often found in the literature
- We note that RMMs were first introduced in [AEC23]

## Two token case: replicating market makers (RMMs)

- In the $n = 2$ case, the set $S$ can be characterized by its boundary (a 2d curve):

$$S = \{(u, v) \mid u \geq \eta(t),\ v \geq t \geq 0\}$$

where

$$\eta(t) = \inf\{v \mid (v, t) \in S\}$$

## Two token case: replicating market makers (RMMs)

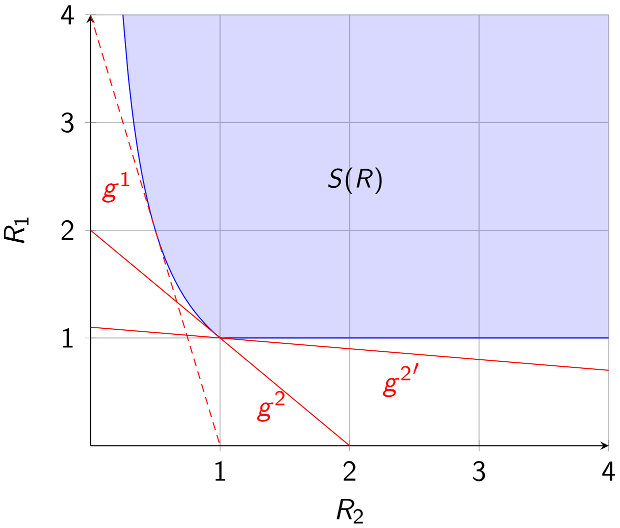
- In the $n = 2$ case, the set $S$ can be characterized by its boundary (a 2d curve):

$$S = \{(u, v) \mid u \geq \eta(t),\ v \geq t \geq 0\}$$

  where

$$\eta(t) = \inf\{v \mid (v, t) \in S\}$$

- When $S$ is strictly convex, then $\eta'(t)$ is strictly monotonic, and $\eta'(t) \geq 0$, which can be interpreted as the marginal price of $S$ when the reserves are $(t, u) \in \mathbf{bd}\, S$.
- Instead of parameterizing by $t$, we often want to parameterized by the price $p = \eta'(t)$ s.t. $t = (\eta')^{-1}(p)$


4
3
2
1
$R_1$
$g^1$
$S(R)$
$g^2$
$g^{2\prime}$
1
2
3
4
$R_2$

# RMMs II

- We define
$$f(p) = \eta((\eta')^{-1}(p)) \quad \text{and} \quad g(p) = (\eta')^{-1}(p),$$
to get
$$\mathrm{bd}(S) = \{(f(p), g(p)) \mid p \geq 0\}.$$
- Interpretation: $f(p)$ is te quantity of asset 1 in the pool assuming an external market price of $p$ and similarly for $g(p)$, where
$$f'(p) = pg'(p) \qquad \text{or} \qquad g(p) = \int_p^\infty \frac{df(q)}{q}$$

# Example: Replicating Black–Scholes covered call option

- The payoff function of a covered call option is

$$V(p, 1) = p\Phi(d_1) + K\Phi(d_2)$$

where

$$d_1 = \frac{\log(p/K) - (\sigma^2/2)\tau}{\sigma\sqrt{\tau}}, \qquad d_2 = d_1 + \sigma\sqrt{\tau}$$

and $\Phi$ is the Gaussian density function

- Using the variable substitution $p/K \mapsto p$ can show via F.O. conditions that

$$\inf_{p>0} \left(V(p, 1) - pR_1/\lambda\right)$$

is minimized whenever $1 - \Phi(d_1) - \bar{R}_1 = 0$, where $\bar{R}_1 = R_1/\lambda$

,

# Example: Replicating Black–Scholes covered call option II

- (Continued) this means that this infimum is minimized at

$$p^\star = \exp\left(\sigma\sqrt{\tau}\Phi^{-1}(1 - \bar{R}_1) + (\sigma^2/2)\tau\right).$$

# Example: Replicating Black–Scholes covered call option II

- (Continued) this means that this infimum is minimized at

$$p^\star = \exp\left(\sigma\sqrt{\tau}\Phi^{-1}(1 - \bar{R}_1) + (\sigma^2/2)\tau\right).$$

- When $\sigma^2\tau = 1$, we recover

$$\exp(\Phi^{-1}(1 - \bar{R}_1) + 1/2)(1 - \bar{R}_1) + \Phi(\Phi^{-1}(1 - \bar{R}_1) + 1).$$

# Example: Replicating Black–Scholes covered call option III

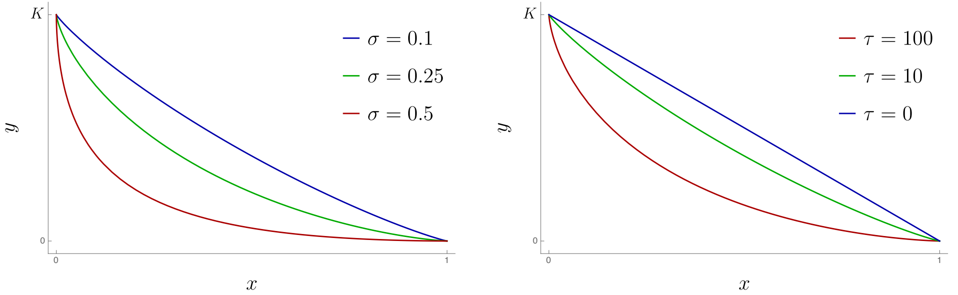


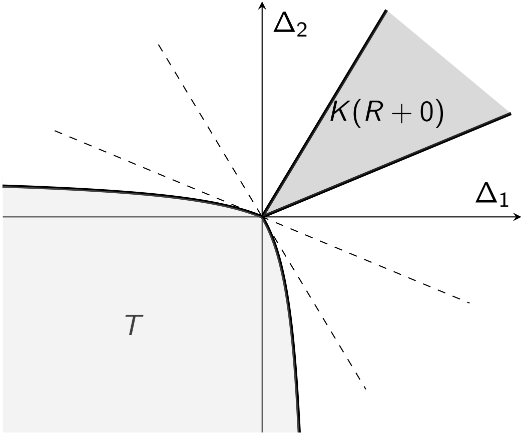

Figure: The left figure plots the trading function of the replicating CFMM for a covered call with $\tau = 10$ for different values of implied volatility. The right figure shows how the trading function changes with time to maturity for $\sigma = 0.1$.

# Outline

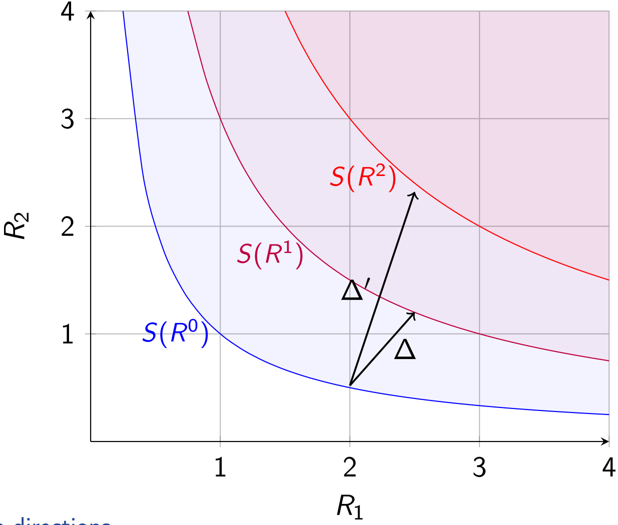
# Adding fees

- In the free free case, no-arbitrage almost completely specifies the behavior of the system
- Many important functions, like the portfolio value, are easy to derive in this case
- Fees introduce some complexities...

# For example, the no-trade cone is nontrivial



# Path Deficiency means the trading set depends on trades



# Connections to Prediction Markets

- [AC20] first remarked upon the connection between classical prediction markets and CFMMs
- [FPW23] demonstrate that by using the perspective transform, one can turn any smooth CFMM trading function into a proper scoring rule

## Connections to Prediction Markets

- [AC20] first remarked upon the connection between classical prediction markets and CFMMs
- [FPW23] demonstrate that by using the perspective transform, one can turn any smooth CFMM trading function into a proper scoring rule
- Recall: The perspective transform $\hat{f} : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}$ of a function $f : \mathbb{R}^n \to \mathbb{R}$ is

$$\hat{f}(\alpha, x) = \alpha f(x/\alpha)$$

- This is the same trading function as $\phi(\Delta) = -\inf\{\lambda > 0 : \Delta/\lambda \in T\}$
- *i.e.*, this formalism generalizes the perspective transform case to non-smooth $\phi$

## Maximal Extractable Value

- CFMMs are the major source of MEV in blockchains
  - MEV: Priviledged actors reorder, add, or censor transactions to increase their profit
  - Priviledged actors include but are not limited to: validators, sequencers, relayers
- Four main types of CFMM MEV:
  - *Sandwich MEV*: Front-running user transactions and then selling back afterwards
  - *Routing MEV*: Arbitraging spreads between different routes between the same pair of assets (c.f. [Ang+22] show how to compute the optimal route)
  - *Reordering MEV*: Reordering trades to cause (more/less) slippage
  - *Just-in-time Liquidity*: Adding liqudiity around big trades to inure LPs

# MEV Geometry?

- Prior results on MEV [KDC22] show properties such as:
  - Routing MEV has an $O(1)$ Price of Anarchy under sufficient liquidity constraints
  - Reordering MEV has logarithmic (sublinear) regret
- Can these be characterized fully geometrically without analytic assumptions?
  - JIT is adding/removing liquidity around trades — this is expressed purely geometrically
  - Routing MEV represents solving sequences of conic programs

# Privacy

- [AEC21] demonstrates that for 1-homogeneous CFMMs, one cannot achieve trade-level privacy
  - If I know the reserves at any initial time and the trading function, then I can invert any number of trades executed
- [CAE22] showed that you could recover a weaker notion of privacy (differential privacy) via an analytic argument
- Can this be done purely geometrically?

# References I


Guillermo Angeris and Tarun Chitra. "Improved price oracles: Constant function market makers". In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 2020, pp. 80–91.

Guillermo Angeris, Alex Evans, and Tarun Chitra. "A note on privacy in constant function market makers". In: *arXiv preprint arXiv:2103.01193* (2021).

Guillermo Angeris, Alex Evans, and Tarun Chitra. "Replicating market makers". In: *Digital Finance* (2023), pp. 1–21.

Guillermo Angeris et al. "Optimal Routing for Constant Function Market Makers". In: *arXiv preprint arXiv:2204.05238* (2022).

# References II


Tarun Chitra, Guillermo Angeris, and Alex Evans. "Differential Privacy in Constant Function Market Makers". In: *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer. 2022, pp. 149–178.

Rafael Frongillo, Maneesha Papireddygari, and Bo Waggoner. "An Axiomatic Characterization of CFMMs and Equivalence to Prediction Markets". In: *arXiv preprint arXiv:2302.00196* (2023).

Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. "Towards a theory of maximal extractable value i: Constant function market makers". In: *arXiv preprint arXiv:2207.11835* (2022).

# Appendix

# Outline

Alternate RMM derivation

# RMMs: alternate derivation

- Want to replicate a concave function $f(p)$ of the price $p$ of some asset
- Price $p_1 \rightarrow$ hold $f(p_1)$ in reserves. Price moves to $p_2$ we must buy (or sell)

$$\int_{p_1}^{p_2} \frac{f'(p)}{p} dp$$

# RMMs: alternate derivation

- Want to replicate a concave function $f(p)$ of the price $p$ of some asset
- Price $p_1 \to$ hold $f(p_1)$ in reserves. Price moves to $p_2$ we must buy (or sell)

$$\int_{p_1}^{p_2} \frac{f'(p)}{p} dp$$

- **Proof:** If the price increases from $p$ to $p+h$, we must sell some of asset 1 to increase our asset 2 position by $f(p+h) - f(p)$
- Thus, we must trade $(f(p+h) - f(p)) \cdot 1/p$ asset 1 for $f(p+h) - f(p)$ of asset 2. Assuming $f$ is differentiable, we take limits to get

$$\frac{f(p+h) - f(p)}{hp} \to \frac{f'(p)}{p}.$$

# How much of asset 2 do you need to hold?

- If we want to use this strategy, we must hold enough asset 2 to buy asset 1 as the exchange rate goes up.
- At some price $p$, we then need to hold at least

$$g(p) = \int_p^\infty \frac{f'(q)}{q} dq$$

## How much of asset 2 do you need to hold?

- If we want to use this strategy, we must hold enough asset 2 to buy asset 1 as the exchange rate goes up.
- At some price $p$, we then need to hold at least

$$g(p) = \int_p^\infty \frac{f'(q)}{q} dq$$

- The portfolio value is then

$$V(p) = f(p) + pg(p) = V(0) + \int_0^p g(q)dq$$

- $V(p)$ is nonnegative, nondecreasing, concave on $p > 0$

# RMMs: getting the trading function

- Let $\phi(R_1) = g \odot f^{-1}(x_1)$. Then $x_2 \geq \phi(x_1)$ iff $x \in S$
- We can verify that $\phi$ is convex, so $S$ is a convex set:

$$\phi'(x) = g'(f^{-1}(x)) \cdot (f^{-1}(x))' = -\frac{f'(f^{-1}(x))}{f^{-1}(x)} \frac{1}{f'(f^{-1}(x))} = -\frac{1}{f^{-1}(x)}.$$

- The fact that $f^{-1}$ is increasing implies $\phi'$ is increasing and therefore $\phi$ is convex

# RMMs: getting the trading function

- Let $\phi(R_1) = g \odot f^{-1}(x_1)$. Then $x_2 \geq \phi(x_1)$ iff $x \in S$
- We can verify that $\phi$ is convex, so $S$ is a convex set:

$$\phi'(x) = g'(f^{-1}(x)) \cdot (f^{-1}(x))' = -\frac{f'(f^{-1}(x))}{f^{-1}(x)} \frac{1}{f'(f^{-1}(x))} = -\frac{1}{f^{-1}(x)}.$$

- The fact that $f^{-1}$ is increasing implies $\phi'$ is increasing and therefore $\phi$ is convex
- Furthermore, $\phi^{-1}(R_2) = (-V)^*(-R_2)$, which can be proved directly