Axioms for Constant Function Market Makers

Jan Christoph Schlegel
Mateusz Kwaśnicki
Akaki Mamageishvili

28 August 2023
A constant function market maker (CFMM) is a simple mechanism to trade financial assets.

- Originally introduced for prediction markets
- Most popular for trading cryptocurrencies
Motivation of DEXes

- A decentralized alternative to an order-book exchange
  - In the spirit of blockchains: less trust, faster, happening on-chain
  - Simple design because computation on-chain is expensive
  - No censorship, no KYC, no need for intermediation

- Around 10% of crypto trading:
  - An average of $3.4B trading volume a day in 2022
  - $45B total value locked
Liquidity is pooled

Liquidity providers (LPs) provide tokens of type A and type B in a fixed ratio to the pool

Traders swap tokens with the pool

The market is made such that (ignoring trading fees) some function of inventories is kept constant

To compensate LPs for the risk they take on, a trading fee is levied
Example: Constant Product Market Maker (CPMM): Invariant is the product of inventories

Two tokens $A$ and $B$ with current inventories $I = (I_A, I_B)$.

A trader can swap $x$ type $A$ tokens for $y$ type $B$ tokens such that

$$(I_A + x)(I_B - y) = I_A I_B.$$
Contribution

- Systematic approach to constructing invariants
- Axiomatic approach: distill desiderata for useful trading functions
- Characterize a simple class of trading functions by a combination of intuitive axioms
- Characterize the CPMM as "trader optimal" within that class
- Bonus: Get an axiomatic characterization of LMSR MMs from prediction markets almost for free
A finite set of asset types $\mathcal{A}$

A **trading function** is a strictly increasing, continuous function $f : \mathbb{R}_+^\mathcal{A} \to \mathbb{R}$ (other authors also require quasi-concavity)

$f(I)$ is the value of the inventory $I$ measured in a numéraire

A **trade** $r \leq I$ changes the inventory from $I$ to $I - r$.

To execute a trade, a trader needs to compensate the MM with $f(I) - f(I - r)$ units of numéraire
Trading and the numéraire

In a DEX there are w.l.o.g. two types of trades:

**Swapping**: Let $A, B \in \mathcal{A}$. If inventory prior to trading is $I \in \mathbb{R}_+^\mathcal{A}$, then $x > 0$ type $A$ tokens are exchanged for $y > 0$ type $B$ tokens such that

$$f(I) = f(I_A + x, I_B - y, I_{\neq \{A,B\}})$$

**Adding/Removing Liquidity**: Let $\lambda \leq 1$. A trader can trade $\lambda I$ in exchange for $f(I) - f((1 - \lambda)I)$ shares of the pooled liquidity

What is the numéraire in a DEX?

The numéraire is a tokenized version of a share of the pooled liquidity
We ignore trading fees.

AMMs can be defined in more general terms.

Restriction to CFMMs is wlog under "path independence" (terms of trade are a function of current inventory only): Abernathy et al. 2013

In prediction markets it is more customary to work with cost functions or scoring function. Equivalence between

- trading and cost functions is straightforward
- scoring and cost functions needs translation invariance (see, however, Frongillo et al. 2023)
Examples

- Variants of the CFMM:
  - More than two asset types are pooled and a (weighted) geometric mean is maintained
    \[ f(I) = I_A^{\alpha} I_B^{\alpha} I_C^{\alpha} \ldots \]
  - "Curve" used for swapping stablecoins implicitly defined by
    \[
    \alpha n^n \sum_{A \in A} I_A + f(I) = \alpha n^n f(I) + \frac{\alpha f(I)^{n+1}}{n^n \prod_{A \in A} I_A}
    \]
  - "Concentrated" liquidity, "Uniswap V3"
    \[
    (I + \alpha)(J + \beta)
    \]
    where \( \alpha, \beta > 0 \) are constants
If no liquidity is removed/added we can consider a fixed curve/surface \( f(I) = \text{const} \).

Notion of \textbf{equivalence}: invariance under monotone transformations

If \( f \) is differentiable, we can define \textbf{marginal exchange rates}:

\[
p_{A,B}(I) = \frac{\partial f}{\partial I_A} = - \frac{dI_B}{dI_A}.
\]
Independence: For each subset of token types $B \subseteq A$ and inventories $I, J$

$$f(I_B, J_{-B}) = f(J) \iff f(I) = f(J_B, I_{-B})$$

For differentiable $f$, exchange rates only depend on the inventory of exchanged assets

$$p_{A,B}(l_{A,B}, l_{-A,B}) = p_{A,B}(l_{A,B}, J_{-A,B}),$$

for each $A, B \in A$ and $I, J \in \mathbb{R}_+^A$
**Independence**

- Geometric means are independent,
  \[
  p_{A,B}(I) = \frac{I_B}{I_A}
  \]

- Curve rules are not independent,
  \[
  p_{A,B}(I) = \frac{81 + \frac{f(I)^4}{I_A I_B I_C}}{81 + \frac{f(I)^4}{I_A I_B I_C}}
  \]
**Further Axioms**

**Scale invariance:** If liquidity is added/removed proportionally, then the market is made in the same way, formally, for $\lambda > 0$ and $I, J \in \mathbb{R}^A_+$ we have $f(I) = f(J) \Rightarrow f(\lambda I) = f(\lambda J)$

- Scale invariance allows to make liquidity positions fungible.

- A stronger version is:

  **Homogeneity:** For $\lambda > 0$ and $I \in \mathbb{R}^A_+$ we have $f(\lambda I) = \lambda f(I)$

- Each scale invariant trading function is equivalent to a homogeneous one

- All previous examples except for Uniswap V3 satisfy homogeneity
Sufficient funds: The AMM should be able to make a market at each inventory level and for arbitrarily large trade sizes: For $I, J \in \mathbb{R}^A_+$ with $f(I) = f(J)$ we have

$$I_A > 0 \text{ for each } A \in \mathcal{A} \Rightarrow J_A > 0 \text{ for each } A \in \mathcal{A}$$

- Geometrically: liquidity curves do not intersect the axes
- Product rule, curve rule and geometric averages satisfy this.
Constant Inventory Elasticity

- Geometric averages satisfy proportionality between exchange rates and inventory ratios

- It is a natural idea to generalize this to:

\[ p_{A,B}(I) = \frac{I_B^m}{I_A^m} \]

for a constant \( m \geq 0 \)

- This leads to the class of constant inventory elasticity MMs (CEMM):

\[
f(I) = \begin{cases} 
(\sum_{A \in \mathcal{A}} I_A^{1-m})^{1/(1-m)}, & \text{for } m \neq 1, \\
\prod_{A \in \mathcal{A}} I_A, & \text{for } m = 1,
\end{cases}
\]

where \( 1/m \) is the inventory elasticity of the exchange rate
The class can be generalized to asymmetric AMMs by introducing different coefficients.

They are sufficiently funded for $m \geq 1$.

By construction, CEMMs are scale invariant and independent.
**Main Result**

**Theorem**

A trading function for $|A| > 2$ assets is independent, scale invariant, and sufficiently funded if and only if it is equivalent to a CEMM with $m \geq 1$.

Proof sketch:

- Independence gives an additive representation through monotone transformation by a classical result of Debreu (1960).
- Continuity, scale-invariance, and separability pin down functional form.
The result is not true for the two-dimensional case (we introduce another axiom later)

Need continuous liquidity curves but no differentiability assumption

If sufficient funds is dropped, then we still get constant inventory elasticity, but $m$ is not restricted

A natural alternative axiom quasi-concavity gives $m \geq 0$.

If symmetry is added we obtain CEMMs with equal coefficients
The result is not true for the two-dimensional case (we introduce another axiom later)

Need continuous liquidity curves but no differentiability assumption

If sufficient funds is dropped, then we still get constant inventory elasticity, but \( m \) is not restricted

A natural alternative axiom quasi-concavity gives \( m \geq 0 \).

If symmetry is added we obtain CEMMs with equal coefficients.

If SI is replaced by Homogeneity we get characterization of functions instead of equivalence classes under monotonic transformation.
Aside: Prediction Markets

In prediction market instead of multiplicative one usually considers additive scaling:

**Translation Invariance:** for each $I, J \in \mathbb{R}_+^A$ and $\alpha \in \mathbb{R}$ we have

$$f(I) = f(J) \Rightarrow f(I + \alpha \mathbb{1}) = f(J + \alpha \mathbb{1}).$$
Aside: Prediction Markets

- In prediction market instead of multiplicative one usually considers additive scaling:

  **Translation Invariance:** for each \( I, J \in \mathbb{R}_+^A \) and \( \alpha \in \mathbb{R} \) we have
  \[
  f(I) = f(J) \implies f(I + \alpha 1) = f(J + \alpha 1).
  \]

- Replacing SI with TI in the previous characterization gives us **Logarithmic Market Scoring Rule** (and Constant Sum) MMs

  \[
  f_{LMSR}(I) = -b \log \left( \sum_{A \in A} e^{(c_A - l_A)/b} \right)
  \]
Aside: Prediction Markets

- Replacing SI with TI in the characterization gives us LMSR (and Constant Sum) MMs.

\[ f_{LMSR}(l) = -b \log \left( \sum_{A \in A} e^{(c_A - l_A)/b} \right) \]

- Intuition: Change of variables. There is a bijection between SI and TI trading functions defined by

\[ g(l) := \log(f(\{e^{l_A}\}_{A \in A})) \]

- Independence is preserved under the above bijection.

- Transformation maps CEMM with parameter \( m \) to LMSR with parameter \( b = 1 - m \).

- \( \Rightarrow \) Axiomatic Foundation for LMSR, See the newest WP
We can rank CEMMs by convexity
This can be formalized in different ways, e.g. the following:

- Call \( f \) more favorable to traders than \( g \) if starting from a balanced inventory the trader obtains more through trading, formally for each \( I \) and for each \( A, B \in A \) with \( I_A = I_B \), \( x > 0 \) and \( y, y' > 0 \) such that:

\[
f(I_A + x, I_B - y, I_{-A,B}) = f(I) \quad \text{and} \quad g(I_A + x, I_B - y', I_{-A,B}) = g(I)
\]

we have \( y \geq y' \).

---

**Theorem**

Let \(|A| > 2\). The constant product rule \( f_{\text{product}} \) is trader optimal within the class of scale invariant, independent, symmetric and sufficiently funded AMMs.
The two dimensional case

- The previous characterization is not true for the case of two assets.
- We need separability, i.e. liquidity curves of the form
  \[ \phi_A(I_A) + \phi_B(I_B) = \text{const}, \]
  for increasing one-dimensional functions \( \phi_A, \phi_B \) which is no longer implied by the other axioms
- We can impose ”Liquidity Additivity” to get separability
- We can also characterize a much larger class without separability
- \( \rightarrow \) See the WP for details
Conclusion

- Have introduced an axiomatic approach for AMMs for DeFi
- Combination of homogeneity and separability gives meaningful restrictions on viable trading functions
- Characterize the CPMM as "trader optimal" within that class
- Replacing homogeneity by translation invariance gives most popular prediction market trading functions
- Separability is arguably not always desirable: what can we impose instead?
Thank you! Questions?