Axioms and Properties of Automated Market Makers

Zach Feinstein

Joint work with Maxim Bichuch

Vienna University of Economics and Business
May 20, 2022

Motivation

Motivation:

- Decentralized finance (DeFi) takes advantage of blockchain technology to provide financial services
- Utilized in lending, borrowing, trading, and insurance underwriting *without* traditional financial intermediaries
- Total value locked up (in dollar denominated terms) in DeFi has grown 9000% between January 1, 2020 and January 1, 2022
- In many areas, DeFi can now directly compete with established companies

Motivation:

- Automated market makers [AMMs] are a decentralized approach for creating financial markets
- Key Idea: Create a (liquidity) pool of assets to trade against instead of a (central) order book
- AMMs create markets by balancing reserves according to mathematical formulas to execute swaps
- There is no counterparty risk: settlement occurs on blockchain, prior to settlement traders retain full control of tokens
- Any individual can pool resources into an AMM and can earn fees from trading activities
- Fast growing literature investigating current AMM structures Angeris et al (2020a,2020b,2021a,2021b), Xu et al (2021), Capponi & Jia (2021), ...

Automated Market Makers:

- There are hundreds of AMMs
- Employ a constant function concept
  Accept trades so that a utility function $u(a, b)$ is invariant for the trade
- Example: Given current pool size with two assets $(a, b) \in \mathbb{R}^2_{++}$
  Buying y assets of type 2 in exchange for x assets of type 1 means:
  $$u(a, b) = u(a + x, b - y)$$
- UniSwap V2 is most well-reported form
  $u(a, b) = \log(a) + \log(b)$
  This is replicated by many other AMMs (SushiSwap, PancakeSwap, ...)

Automated Market Makers:

- There are hundreds of AMMs
- Employ a constant function concept
  Accept trades so that a utility function $u(a,b)$ is invariant for the trade
- Example: Given current pool size with two assets $(a,b) \in \mathbb{R}^2_{++}$
  Buying y assets of type 2 in exchange for x assets of type 1 means:
  $$u(a,b) = u(a+x, b-y)$$
- UniSwap V2 is most well-reported form
  $u(a,b) = \log(a) + \log(b)$
  This is replicated by many other AMMs (SushiSwap, PancakeSwap, ...)
- Goal of this talk: Analyize markets made by generic AMM

Axioms of Automated Market Makers

Axioms:

Let $u : \mathbb{R}^2_+ \to \mathbb{R} \cup \{-\infty\}$ be a utility function on $\mathbb{R}^2_+$

Automated Market Maker

- (UfB) **Unbounded from below:** $u(x,0) = u(0,y) = -\infty$ for $x, y \geq 0$ and $u(z) > 0$ for $z \in \mathbb{R}^2_{++}$
- (UfA) **Unbounded from above:** $\lim_{\bar{x}\to\infty} u(\bar{x}, y) = \lim_{\bar{y}\to\infty} u(x, \bar{y}) = \infty$ for $x, y > 0$
- (SM) **Strictly Monotonic:** $u(z) > u(\bar{z})$ if $z - \bar{z} \in \mathbb{R}^2_+ \backslash \{0\}$ for $z, \bar{z} \in \mathbb{R}^2_{++}$
- (C) **Continuous:** u is continuous
- (QC) **Quasiconcave:** u is quasiconcave
- (I+) **Inada+:** u is differentiable with $\lim_{\bar{x}\to\infty} u_x(\bar{x}, y) = \lim_{\bar{y}\to\infty} u_y(x, \bar{y}) = 0$, $\lim_{\bar{x}\to\infty} u_y(\bar{x}, y) > 0$, and $\lim_{\bar{y}\to\infty} u_x(x, \bar{y}) > 0$ for every $x, y > 0$
- (MD) **Monotone differences:** u is twice differentiable with $u_{xx}, u_{yy} \leq 0$ and $u_{xy} \geq 0$

AMM Swaps:

Swaps

Consider AMM reserves $a, b > 0$. Let $x, y \geq 0$:

$$\mathcal{Y}(x; a, b) := \sup\{y \in [0, b] \mid u(a + x, b - y) \geq u(a, b)\}$$
$$\mathcal{X}(y; a, b) := \sup\{x \in [0, a] \mid u(a - x, b + y) \geq u(a, b)\}$$

- Trades *cannot* decrease AMM utility
- AMM *cannot* provide more assets than it has in reserve

Properties of Automated Market Makers

Fundamental Properties:

Theorem

Fix $a, b > 0$ and $x \geq 0$

- If (C) then $u(a + x, b - \mathcal{Y}(x)) \geq u(a, b)$
- If (C) and $\mathcal{Y}(x) \neq b$ then $u(a + x, b - \mathcal{Y}(x)) = u(a, b)$
- If (UfB) and (C) then $\mathcal{Y}(x) < b$
- If (SM) then $\mathcal{Y}(0) = 0$
- If (UfB), (SM), and (C) then $\mathcal{Y}$ is strictly increasing
- If (UfB), (UfA), (SM), and (C) then $\lim_{\bar{x} \to \infty} \mathcal{Y}(\bar{x}) = b$
- If (C) then $\mathcal{Y}$ is upper semicontinuous
- If (C) and (QC) then $\mathcal{Y}$ is concave (+ continuous and a.e. differentiable)

Splitting a Trade:

- Question: Is it better to make a single large transaction or many small transactions?
- Without fees this does *not* matter
- Property: If (UfB), (SM), and (C) then

$$\mathcal{Y}(x_1 + x_2; a, b) = \mathcal{Y}(x_1; a, b) + \mathcal{Y}(x_2; a + x_1, b - \mathcal{Y}(x_1; a, b))$$

Splitting a Trade:

- Question: Is it better to make a single large transaction or many small transactions?
- Without fees this does *not* matter
- Property: If (UfB), (SM), and (C) then

$$\mathcal{Y}(x_1 + x_2; a, b) = \mathcal{Y}(x_1; a, b) + \mathcal{Y}(x_2; a + x_1, b - \mathcal{Y}(x_1; a, b))$$

- If trades are made slower to allow for AMM recovery then small transactions are preferred by the trader
- Property: If (SM), (C), (QC) then $\mathcal{Y}$ is subadditive

$$\mathcal{Y}(x_1 + x_2) \leq \mathcal{Y}(x_1) + \mathcal{Y}(x_2)$$

Impacts of Liquidity:

- Increasing pool in 1st asset should increase value of 2nd asset and vice versa
- Property: If (UfB), (SM), and (MD) then $\mathcal{Y}_a(x;a,b) \leq 0$ and $\mathcal{Y}_b(x;a,b) \in [0,1)$
- Property: If (UfB), (SM), and (MD) then

$$\lim_{\bar{a} \searrow 0} \mathcal{Y}(x;\bar{a},b) = b \text{ and } \lim_{\bar{b} \searrow 0} \mathcal{Y}(x;a,\bar{b}) = 0$$

- Property: If (UfB), (SM), (I+), and (MD) then

$$\lim_{\bar{a} \nearrow \infty} \mathcal{Y}(x;\bar{a},b) = 0 \text{ and } \lim_{\bar{b} \nearrow \infty} \mathcal{Y}(x;a,\bar{b}) = \infty$$

No Arbitrage:

- Round trip trade should *not* produce risk-free profit
- Without fees round trip trading results in initial portfolio
- Property: If (UfB), (SM), and (C) then $\mathcal{X}(\mathcal{Y}(x;a,b);a+x,b-\mathcal{Y}(x;a,b)) = x$ and vice versa for $\mathcal{Y}$

Price Oracle and Pooling

Price Oracle:

Prices

The price oracle $P : \mathbb{R}^2_{++} \to \mathbb{R}_{++}$ proves the marginal units of asset 2 obtained from selling a marginal number of units of asset 1
That is, $P(a, b) = \mathcal{Y}'(0; a, b)$

If (UfB), (SM), and (C) then there does *not* exist a bid-ask spread in the price oracle:

$$P(a, b) = \mathcal{Y}'(0; a, b) = \frac{1}{\mathcal{X}'(0; a, b)}$$

Price Oracle Properties:

Proposition

Assume (UfB), (SM), (I+), and (MD)

- The pricing oracle P is differentiable
- For any $a > 0$, $b \mapsto P(a, b)$ is nondecreasing and surjective on $\mathbb{R}_{++}$
- For any $b > 0$, $a \mapsto P(a, b)$ is nonincreasing and surjective on $\mathbb{R}_{++}$

Pooling Resources:

- AMMs allow investors to join the liquidity pool to capture a fraction of the profits
- Current procedure: Add pair of assets so that price does not change
  In practice, often based on ratio of assets in the AMM
- Idea: Guarantee that pooling increases liquidity

$$\mathcal{Y}(x; a+\alpha, b+\beta) \geq \mathcal{Y}(x; a, b) \text{ and } \mathcal{X}(y; a+\alpha, b+\beta) \geq \mathcal{X}(y; a, b)$$

- Keeping constant price is necessary but not sufficient to guarantee increased liquidity
- Sufficient condition for increased liquidity:

$$P_b P_{aa} - (P P_b + P_a) P_{ab} + P P_a P_{bb} \geq 0$$

Largest Current Automated Market Makers

5. Current AMMs

UniSwap V2:

- Also used by: SushiSwap, DeFiSwap, ...
- $u(a, b) = \log(a) + \log(b)$
- $P(a, b) = b/a$
- Pooling at current ratio of reserves
- Satisfies all axioms considered
- Has high price impacts

UniSwap V3:

- Also used by: KyberSwap, MooniSwap, ...
- $u(a, b) = \log(\alpha + a) + \log(\beta + b)$
- Parameters α, β can be dynamic in time or based on current reserves
- $P(a, b) = (\beta + b)/(\alpha + a)$
- Pooling at ratio of virtual reserves (modified by α, β)
- Does *not* satisfy (UfB)
- α, β allow control of price impacts

Balancer:

- Also used by: Bancor, ...
- $u(a,b) = w_1 \log(a) + w_2 \log(b)$ for $w_1, w_2 \in (0,1)$ with $w_1 + w_2 = 1$
- $P(a,b) = (w_1 b)/(w_2 a)$
- Pooling at current ratio of reserves
- Satisfies all axioms considered
- Reduces to UniSwap if $w_1 = w_2$

mStable:

- $u(a, b) = \log(a + b)$
- $P(a, b) = 1$
- Pooling in equal proportion
- Does *not* satisfy (UfB), (I+), (MD)
- No price impacts but at expense of limited liquidity

StableSwap:

- Also used by: Saber, Saddle, ...
- $u(a, b) = \log(C(a + b) + ab)$ for $C > 0$
- $P(a, b) = (b + C)/(a + C)$
- Pooling at ratio of virtual reserves (modified by C)
- Does *not* satisfy (UfB), (MD)
- C allows control of price impacts

Curve:

- The largest AMM by value locked up
- $u(a,b)$ is the *unique* root of $\exp(3u) + 4(C-1)ab\exp(u) - 4C(a+b)ab = 0$ for $C \geq 1$
- $P(a,b) = \frac{b[C(2a+b)-(C-1)u(a,b)]}{a[C(a+2b)-(C-1)u(a,b)]}$
- Pooling at current ratio of reserves
- Extends StableSwap to satisfy (UfB)
- Still does *not* satisfy (MD)
- C allows control of price impacts
  - Low price impacts at $a \approx b$
  - Very high price impacts otherwise

Dodo:

- Requires exogenous price P
- $u(a,b) = \log(P\alpha(a,b) + \beta(a,b))$ where:
  1. Targets match the price: $P\alpha(a,b) = \beta(a,b)$
  2. Pool is in equilibrium: $Pf(a,b)(\alpha(a,b) - a) + (\beta(a,b) - b) = 0$ for

$$f(a,b) = \begin{cases} 1 + C\left(\alpha(a,b)/a - 1\right) & \text{if } Pa \leq b \\ \left[1 + C\left(\beta(a,b)/b - 1\right)\right]^{-1} & \text{if } Pa \geq b \end{cases}$$

  with $C \in [0,1]$

- If $C = 0$ then $u(a,b) = Pa + b$ is mStable
- If $C = 1$ then $u(a,b) = 2\sqrt{Pab}$ is UniSwap V2
- Closed form for u exists
- Does *not* satisfy (MD)
- Does *not* provide a pricing oracle

Symmetric Decomposable Automated Market Makers

Symmetric Decomposable AMM:

- Let $f : \mathbb{R}_+ \to \mathbb{R} \cup \{-\infty\}$ strictly increasing, concave with $f(0) = -\infty$, $f(z) > -\infty$ for $z > 0$, and $\lim_{z\to\infty} f(z) = \infty$
- $u(a, b) = f(a) + f(b)$
- $P(a, b) = \frac{f'(a)}{f'(b)}$
- Satisfies all axioms considered
- Pooling follows more complex formula

Hyperbolic Sine AMM:

- $f(x) = \log(\sinh(Cx))$
- Limits to mStable as pool size grows to infinity
- C allows control of price impacts
  - Prices remain stable around 1 until pool becomes very unbalanced
  - Unbalanced pools have extremely high price impacts

Impact of Fees

Assessment of Fees:

- 3 ways to assess fees on swaps:
    1. Fees collected after clearing on sold asset
    2. Fees collected before clearing on sold asset
    3. Fees collected on bought asset

Post-Clearing Fees on the Sold Asset:

- For fees $\gamma \in [0,1]$:

$$\begin{aligned}\mathcal{Y}_\gamma(x;a,b) &= \sup\{y \in [0,b] \mid u(a+[1-\gamma]x, b-y) \geq u(a,b)\} \\ &= \mathcal{Y}([1-\gamma]x;a,b)\end{aligned}$$

- Encourages large transactions:

$$\mathcal{Y}_\gamma(x_1+x_2;a,b) \geq \mathcal{Y}_\gamma(x_1;a,b)+\mathcal{Y}_\gamma(x_2;a+x_1,b-\mathcal{Y}_\gamma(x_1;a,b))$$

if (UfB), (SM), and (MD)

Pre-Clearing Fees on the Sold Asset:

- For fees $\gamma \in [0,1]$:

$$\begin{aligned}\mathcal{Y}_\gamma(x;a,b) &= \sup\{y \in [0,b] \mid u(a+x,b-y) \geq u(a+\gamma x,b)\} \\ &= \mathcal{Y}([1-\gamma]x;a+\gamma x,b)\end{aligned}$$

- Encourages small transactions:

$$\mathcal{Y}_\gamma(x_1+x_2;a,b) \leq \mathcal{Y}_\gamma(x_1;a,b)+\mathcal{Y}_\gamma(x_2;a+x_1,b-\mathcal{Y}_\gamma(x_1;a,b))$$

if (UfB), (SM), and (MD)

Fees on the Bought Asset:

- For fees $\gamma \in [0,1]$:

$$\mathcal{Y}_\gamma(x;a,b) = \sup\{y \in [0,b] \mid u(a+x, b-\frac{y}{1-\gamma}) \geq u(a,b)\}$$
$$= [1-\gamma]\mathcal{Y}(x;a,b)$$

  so that the collected fees are $\gamma\mathcal{Y}(x;a,b)$

- Encourages small transactions:

$$\mathcal{Y}_\gamma(x_1+x_2;a,b) \leq \mathcal{Y}_\gamma(x_1;a,b)+\mathcal{Y}_\gamma(x_2;a+x_1,b-\mathcal{Y}_\gamma(x_1;a,b))$$

  if (UfB), (SM), and (MD)

Open Questions and Future Projects

Open Questions and Future Projects

- Divergence loss: with large price swings, liquidity providers could be better off if they held their initial (pooled) portfolio instead
- Numeraire-based AMM: We constructed AMM pricing with 2nd asset as numeraire
  Define AMM so that the pool acts as numeraire
- AMM for derivatives: AMM is a smart contract. Construct pricing rules allowing the AMM to hedge automatically
- Optimal execution: How to trade against an AMM optimally when including gas fees
- Risk and contagion: Investigate impact of run on AMM
- ...

Thank You!

Thank You!