Dirac AMM*

V. Tolstikov[1] and K. Koshiyama[2]

[1] *University of California, Davis*
1 Shields Ave,
Davis, CA 95616, USA
[2] *University of Michigan*
500 S State St
Ann Arbor, MI 48109, USA

ABSTRACT

Swapping and Liquidity Provision (LP) transactions of an Automated Market Maker (AMM) whose liquidity fingerprint is a power law distribution are obfuscated using Fully Homomorphic Encryption (FHE) to avoid Maximum Extractable Value (MEV) in the public mempool. Liquidity concentration is adjusted using a scale parameter and can be modified with a hook in Uniswap v4. Furthermore, we show that it is possible to enter the negative liquidity domain with such an AMM.

1. INTRODUCTION

Uniswap v2 introduced a continuous uniform liquidity fingerprint [1] laying no claim to the dynamics of the underlying stochastic process of digital assets resulting in capital inefficiency as liquidity is stretched to infinity [2]. To address this problem Uniswap v3 was introduced to allow for the concentration of liquidity based on an LP's preferred viewpoint on the range of price movement [3]. The complexity of price dynamics led to the rise of automated liquidity management protocols [4] specializing in allocating sets of concentrated liquidity positions in price space on behalf of LPs. The constrained nature of a discrete set of uniform liquidity fingerprints of a uniswap v3 position creates a problem of capital inefficiency in the tails a.k.a long tail liquidity, and an LP can wind up out of range while earning no fees [Figure1]. To deal with being out of range, alternative AMM invariants can be made that match particular price behavior such as Geometric Brownian Motion [5]. We extend this approach by making the empirical observation that financial assets can exhibit power law behavior [6][7] as well as enter the negative price domain [8]. We adjust the liquidity fingerprint accordingly.

With the switch to Proof-of-Stake Ethereum has undergone a reorganization in the block construction supply chain bringing about MEV issues [9] and clever solutions against centralization at the cost of trade-offs [10]. Our proposed trade-off involves increased gas expenditure based on fully homomorphic encryption combined with threshold protocols. Due to the deterministic properties of homomorphic function evaluation, everyone can perform computations on encrypted data. This intentionally preserves one of the key benefits of transparency on blockchains: the computation carried out remains public, while only the data that is being computed on is temporarily hidden in the mempool [11]. We combine this feature with a mechanism based on the Kelly criterion [12] to mitigate MEV by pushing the desired Kelly betting amount of a MEV attacker to zero through variable obfuscation.

1.1. *Power Law AMM*

We set the liquidity fingerprint L to a power law that starts to elude the law of large numbers [13]. The fingerprint tail happens to be the Student's-t distribution with degree of freedom $df = 2$, making the variance completely unpredictable despite increasing sample size [14].

$$L(x) = \frac{1}{(1+x^2)^{\frac{3}{2}}} \tag{1}$$

cauchyamm@gmail.com, kylekoshiya@gmail.com

* December, 12, 2023.

Figure 1. Liquidity Tails in Semi-Log and Log-Log

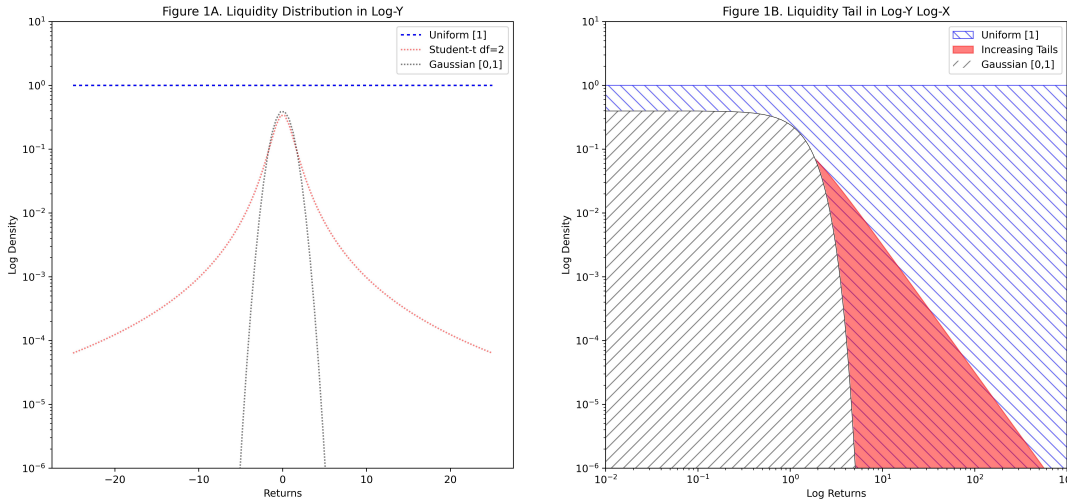

Figure 1. The outlier events of digital assets can extend beyond the Gaussian distribution into fatter tails outlined in red. Extending into the full-range liquidity of a Uniform distribution in blue with Uniswap v2 is capital inefficient, yet concentrating liquidity in Uniswap v3 through a discrete Uniform distribution makes it difficult for LPs to capture fees in such unpredictable tails, hence the need for a power law liquidity fingerprint.

We discover that the AMM invariant becomes:

$$(x - z)^2 + (y - z)^2 = z^2 \tag{2}$$

Where x is the reserve of the asset, y is the reserve of the numeraire, and z is the liquidity range parameter where $z > x$ and $z > y$ with invariant derivation outlined in Appendix A. The liquidity amount can be found with the following equation:

$$L = \sqrt{\frac{\left(\sqrt{2}z - z\right)^2}{2}} \tag{3}$$

Due to the circular nature of the invariant equation, this Concentrated Circular Market Maker (CCMM) can be programmed to transition into the negative liquidity domain. Uniswap v2 happens to also provide liquidity in the negative domain (see Appendix B), but the region is difficult to access due to the hyperbolic nature of the invariant. The phenomenon of negative prices has been observed empirically, especially in commodity prices. Examples being oil in 2020 [15], electricity in Nebraska at night [16], fat-finger trading mistakes in Finland in 2023 [17], and synthetic financial products consisting of derivatives of highly liquid US treasury bonds [18]. For such occurrences the left tail of an AMM can be extended into the negative domain using the full spectrum of the conic section outlined in Appendix C. A unique feature of the CCMM is that it allows one to trade two negatively priced assets between one another. While appearing bizarre, it is normal to be able to exchange a barrel of oil costing negative four dollars for two natural gas costing a negative two dollars each. This is at the present moment not doable in centralized exchanges, which in the middle of COVID-19 had difficulty accounting for negative prices by having to switch to Arithmetic Brownian Motion from Geometric Brownian Motion via the Bachelier Model [19]. Furthermore, for an AMM where both x and y can go negative, the value of the LP position also loops on itself and, in the event of borrowing such an LP position, can exhibit double convexity [20]. Yet the purpose of the CCMM does not necessarily have to apply to the underlying price going negative. Rather, it can simply apply to an offset representation of the price. For example, an asset can be worth \$100 and yet its offset price token can be \$0 and now a negative offset price of \$ -1 would simply mean a reduction in the price of the underlying to \$99, creating a variety of intriguing non-linear payoffs seen in Figure 2.

Figure 2.
CCMM Invariant Quadrant and Equivalent Non-linear LP Payoff of $(x-z)^2+(y-z)^2=z^2$; z[1,1.1...2]

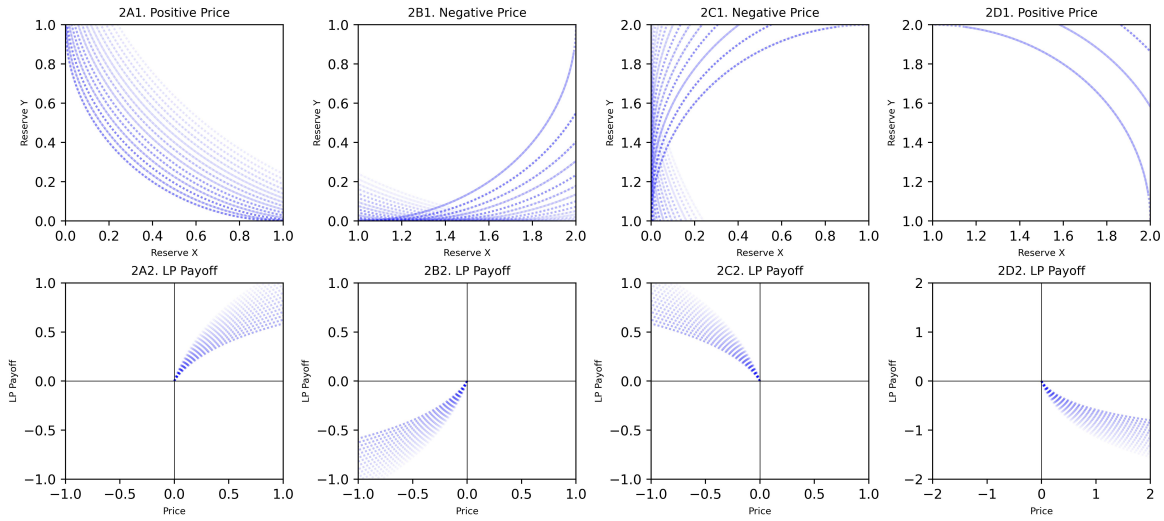

Figure 2. An LP Position with negative prices can exhibit negative concavity.

The nature of an LP's payoff, if bound by the zero barrier, is exposure to impermanent loss due to price movement along a concave payoff structure and, if no fees are earned, would underperform a simple holding strategy. While it is possible to construct LP payoffs that avoid impermanent loss (see Appendix D), they would come at a cost of either an increased price impact for the swapper, thereby discouraging the use of such an AMM, or at the cost of the LP's expected yield through hedging expenses [21]. The LP is effectively short volatility [22], but instead of being short volatility in a discrete price range as in Uniswap v3, with a power law distribution that more closely matches the reality of digital and financial assets [7] one is always providing liquidity despite rapid price movements, a trade-off between a full-range v2 and a concentrated position in v3 [Figure 4C].

The unusual dynamics of this AMM with its ability to transition into the negative domain lead us to name it after Paul Dirac, who discovered anti-matter by noticing that energy can be negative before one takes the square root of its square in the energy-momentum relation [23].

1.2. *FHE MEV Approach with Kelly Criterion*

Today the standard practice for on-chain privacy entails the use of zero knowledge proofs (ZKP). However ZKP's are limited by their ability to manage a shared state which negatively impacts composabilty [24]. ZK proofs tackle the privacy challenge by keeping only committed data and proofs of correct computation on-chain. However, the data must be known in plaintext to compute on it, meaning a plain-text copy of the data must be kept somewhere. This can work well when only data from a single party is required for any computation, but raises the issue of what to do for applications requiring data from multiple parties. Through the TFHE-rs decrypt and as encrypted unsigned integer (*euint*) operations [25] we are able to obfuscate the contents of the transactions in the mempool, converting formally non-fungible individual transactions into completely fungible transactions as seen in Figure 3 below. We can combine the obfuscation of *euint* with the following game theory. As MEV extractors grow in sophistication, a rational approach to decision-making is to maximize compounding returns by using the Kelly criterion:

$$f^* = p - \frac{1-p}{b} \tag{4}$$

where f^* represents a MEV extractor's portfolio allocation in a MEV attack with the probability of success p and betting odds b. By aiming for Kelly-neutrality we set a MEV extractor's Kelly betting amount $f^* = 0$ rearranging for the following equality to hold:

$$p = \frac{1-p}{b} \tag{5}$$

We do so by introducing two encrypted boolean values for swapping and providing liquidity:

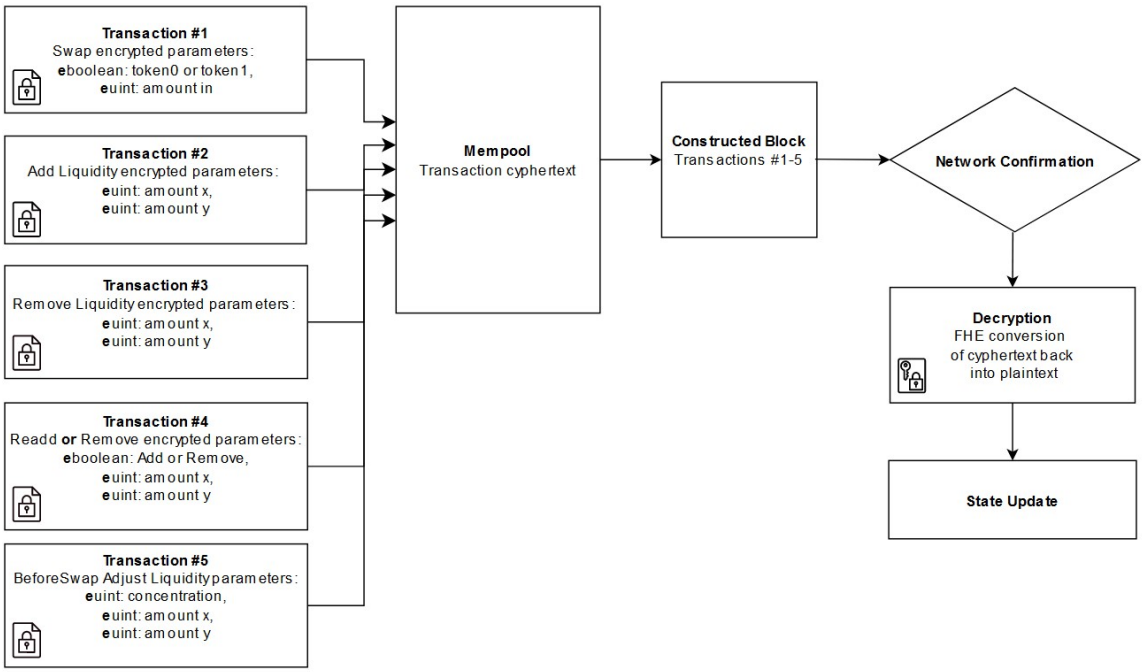

Figure 3. Variables for AMM interaction are obfuscated before entering the mempool. After network confirmation the cyphertext is converted back to plaintext.

$$B_{swap} = [0,1], B_{LP} = [0,1] \tag{6}$$

Is the LP removing ($B_{LP} = 0$) or re-adding ($B_{LP} = 1$) liquidity? Is the swapper exchanging USDC for ETH ($B_{swap} = 0$) or exchanging ETH for USDC ($B_{swap} = 1$)? We can also encrypt as euints the quantity of the swap amount dx and the liquidity concentration parameter c, which could be modified with a hook function similar to $beforeSwap$ in Uniswap v4 [26], thereby making it unclear of what the size of the betting odds b is. Where the odds for a MEV extractor can be expressed in terms of gain G and the cost L of attempting to re-arrange or decrypt a transaction.

$$E\langle B_{swap/LP}\rangle = \frac{1 - E\langle B_{swap/LP}\rangle}{\frac{E\langle G\rangle}{E\langle L\rangle}} \tag{7}$$

$$0.5 = \frac{1 - 0.5}{\frac{U_{[0,\infty)}}{U_{[0,\infty)}}} = \frac{0.5}{1} \tag{8}$$

Setting the expected value of a MEV extractor's Kelly bet $E\langle f^*\rangle = 0$.

APPENDIX

A. CCMM INVARIANT LIQUIDITY FINGERPRINT

Start with the full invariant.

$$(x-a)^2 + (y-b)^2 = z^2 \tag{A1}$$

Rewrite it as a function of the numeraire.

$$y_n = \pm\sqrt{z^2 - x^2 + 2ax - a^2} + b \tag{A2}$$

Taking the derivative and negating it:

$$y_x = -\frac{dy_n}{dx} = \frac{-x+a}{\sqrt{z^2-x^2+2ax-a^2}} \tag{A3}$$

We invert to solve for the price of x due to symmetric nature of invariant:

$$y_y = \frac{\sqrt{z^2-x^2+2ax-a^2}}{-x+a} \tag{A4}$$

Rearranging the equation for x:

$$x = \frac{ay_y^2 + a + y_y z\sqrt{y_y^2+1}}{y_y^2+1} \tag{A5}$$

Rewrite as $l(x)$ and take derivative to get the liquidity fingerprint:

$$l(x) = \frac{ax^2 + a + xz\sqrt{x^2+1}}{x^2+1} \tag{A6}$$

Liquidity happens to be a heavy tailed distribution with a Pareto tail index of $\alpha = 3$:

$$L(x) = \frac{dl(x)}{dx} = \frac{z}{(1+x^2)^{\frac{3}{2}}} \tag{A7}$$

Converting it to price space p with natural log to get a super heavy tailed distribution:

$$L(p) = \frac{z}{(1+ln(p)^2)^{\frac{3}{2}}} \tag{A8}$$

The value function [27] of an LP payoff is given by:

$$V_{LP}(p) = 2p\frac{\left(a+bp-\sqrt{z^2p^2-a^2p^2+2abp+z^2-b^2}\right)}{1+p^2}. \tag{A9}$$

The Greeks for Delta=Δ_{ccmm}, Gamma=Γ_{ccmm}, and Theta=Θ_{ccmm} are available in desmos with the DiracAMM and a comparison to a replicating market maker [27] at https://www.desmos.com/calculator/hftsrbp1xj. Expected theta is derived from the relationship of concavity to yield as originally outlined by Louis Bachelier in 1900 [28].

$$\Theta_c(x) = E\langle -\frac{\sigma_{iv}^2}{2}\Gamma_c(x)\rangle \tag{A10}$$

Here implied volatility σ_{iv} can be found by looking at the implied volatility at the current ATM strike price or from the relationship between volatility and liquidity at the current tick in Uniswap v3 [29]. Both volatility values, given a no arbitrage assumption, undergo Lambertian convergence [22][29].

B. NEGATIVE LIQUIDITY

Taking the Uniswap invariant [2] with liquidity L

$$xy = L^2 \tag{B11}$$

Introducing price p as $p = y/x$ and $y = px$

$$x * p * x = L^2 \tag{B12}$$

Solving for x

$$x = \sqrt{\frac{L^2}{p}} \tag{B13}$$

Note the sign

$$x = \pm\frac{L}{\sqrt{p}} \tag{B14}$$

C. CONIC SECTION OF AMMS

The spectrum of the conic section discovered by the Apollonius of Perga [30] outlines also the set of liquidity curves that can be constructed in two dimensions with the full equation being:

$$A(x^2) + B(xy) + C(y^2) + D(x) + E(y) + F = 0 \tag{C15}$$

One can see how rearranging operators A, B, C, D, E, F in the above equation can give us known AMMs $[0, 1, 0, 1, 1, -1]$ gives us Curve and $[0, 1, 0, 0, 0, -1]$ gives us Uniswap. The case of $A \neq 0$ and $C \neq 0$ is largely unexplored. We can create such an AMM that would fold in on itself by controlling operator B_{fold}.

$$(x - x_{offset})^2 + (y - y_{offset})^2 - B_{fold}(xy) = k \tag{C16}$$

When $B_{fold} < 2$ the AMM folds in on itself see Figure 4D below. When $B_{fold} = 2$ the invariant transforms into a CSMM. The case of $B_{fold} = 0$ is the CCMM.

D. AMM WITH NO IMPERMANENT LOSS AT THE COST OF PRICE IMPACT FOR SWAPPERS

Impermanent Loss is a property of the curvature/concavity/gamma of the value function and can be neutralized by dividing two CPMMs, such as Uniswap, by a CSMM.

$$\frac{2xy}{x + y} = k \tag{D17}$$

This equation, outlined in red in Figure 4B, happens to be a unique condition first derived from ring theory by Forgy and Lau [31] when parameter k_{FL} of the following equation is set to 1.

$$(1 - k_{FL})(x + y - 2) = k_{FL}\left(\frac{1}{x} + \frac{1}{y} - 2\right) \tag{D18}$$

An AMM with an extreme price impact is of great benefit for an LP replicating a HODL position, but swappers aim to minimize one's price impact [Figure 4B]. An AMM set to $k_{FL} = 1$ can be useful for charitable/non-profit digital auctions.

E. FURTHER WORK

An approach to avoid negative liquidity can be to not provide liquidity beyond a discrete cutoff e.g. \$0.01. Yet here another exchange may provide it below \$0.01. Alternatively, one could construct a wall of liquidity, a liquidity fingerprint that asymmetrically increases non-linearly as price approaches zero, denting price impact. The super-heavy tailed distributions [32] like the Log-Cauchy distribution [33] with concentration parameter c come to mind with liquidity fingerprint in Figure 5C in price space being:

$$L_{Log-Cauchy}(p) = \frac{1}{\pi p} \cdot \frac{c}{\ln(p)^2 + c^2} \tag{E19}$$

Figure 4.
AMMs in log-log with dashed diagonal line representing xy=k

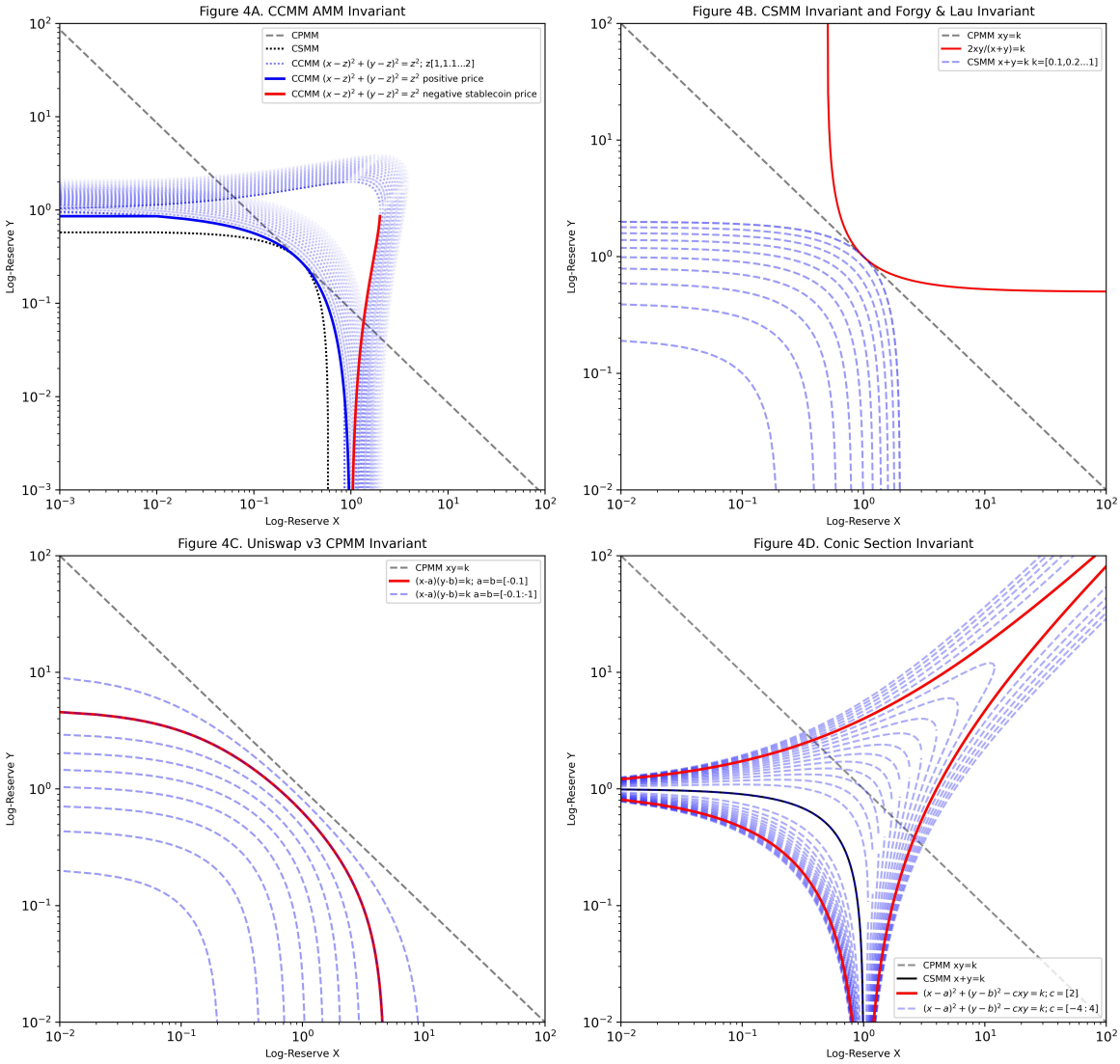

Figure 4. 4A. CCMM invariant with red line representing a negative price for an asset priced in a currency with a zero bound such as a stablecoin. 4B: AMM invariant of no impermanent loss and CSMM. 4C: Concentrated liquidity in Uniswap v3. 4D: Concentration of liquidity in a negatively priced AMM resembles a Uniswap v3 invariant as long as price does not enter negative territory.

Figure 5: CauchyAMM
Dashed blue lines represent increasing liquidity concentration as c=[1>>0.1]

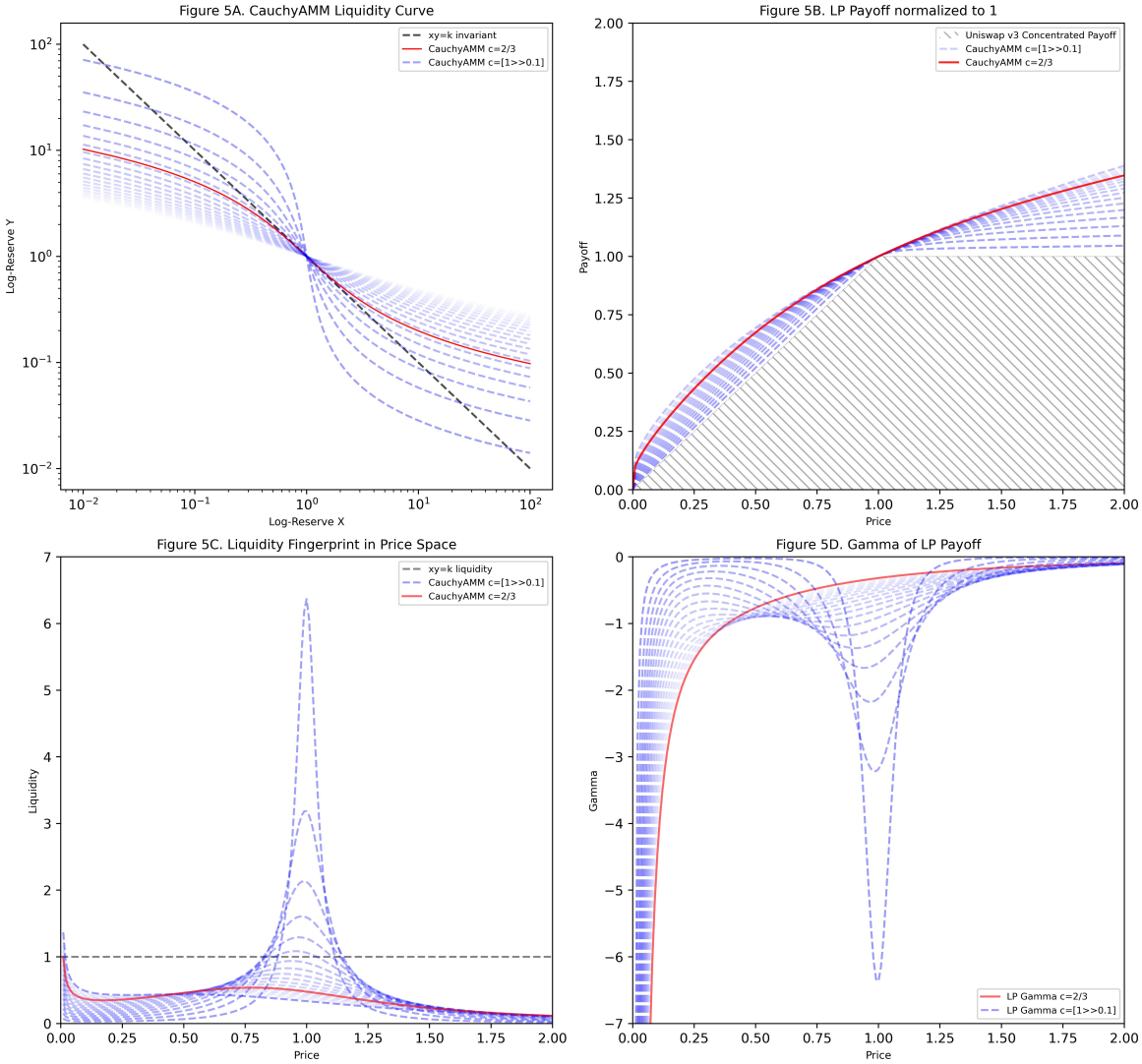

Figure 5. 2A. CauchyAMM with inflection point $c = 2/3$ highlighted in red with Uniswap v2 in dotted black for comparison. 2B: Notice how the LP value of a CauchyAMM does not fully flatten diagonally below the price nor horizontally above the price like a Uniswap v3 LP position despite increased concentration of liquidity. 2C: CauchyAMM asymmetrically concentrates liquidity following a Log-Cauchy distribution in price space. 2D: Gamma undergoes an inflection point and folds at the current price as c moves below 2/3.

F. REFERENCES

[1] Hayden Adams, Noah Zinsmeister, and Dan Robinson. 2020. Uniswap v2 Core. https://uniswap.org/whitepaper.pdf

[2] Dan Robinson. 2021. Uniswap v3: The Universal AMM. https://www.paradigm.xyz/2021/06/uniswap-v3-the-universal-amm

[3] Hayden Adams et al. Uniswap v3. https://uniswap.org/whitepaper-v3.pdf

[4] Maverick AMM. Retrieved from Medium Nov 20, 2023 from: https://medium.com/maverick-protocol/maverick-amm-the-revolutionary-amm-that-enables-directional-lping-unlocking-greater-capital-34427f5ac22f

[5] Alexander Angel, et al. Financial Virtual Machine. (2022) https://www.primitive.xyz/papers/yellow.pdf

[6] Gabaix, X., Gopikrishnan, P., Plerou, V. et al. A theory of power-law distributions in financial market fluctuations. Nature 423, 267–270 (2003). https://www.nature.com/articles/nature01624

[7] Jean-Philippe Bouchaud. Power-laws in Economy and Finance: Some Ideas from Physics (2018).https://arxiv.org/pdf/cond-mat/0008103.pdf

[8] Naureen S Malik. Negative Power Prices? Blame the US Grid for Stranding Renewable Energy. Retrieved from Bloomberg November 20, 2023 https://www.bloomberg.com/news/articles/2022-08-30/trapped-renewable-energy-sends-us-power-prices-below-zero

[9] Barnabé Monnot. Notes on Proposer-Builder Separation (PBS) (2022).https://barnabe.substack.com/p/pbs

[10] Alex Watts. Exploring paths to a decentralized, censorship-resistant, and non-predatory MEV Ecosystem (2023). https://ethresear.ch/t/exploring-paths-to-a-decentralized-censorship-resistant-and-non-predatory-mev-ecosystem/17312

[11] Dahl et al. fhEVM (2023). https://github.com/zama-ai/fhevm/blob/main/fhevm-whitepaper.pdf

[12] Edward Thorp, Leonard Maclean, William Ziemba, The Kelly Capital Growth Investment Criterion: Theory and Practice (February 10, 2011).

[13] Jacoppo Bertolloti. Physics Factlet(249). (2023) https://commons.wikimedia.org/wiki/File:Mean_estimator_consistency.gif

[14] Student's-t Distribution Moments. Retrieved from Wikipedia Nov 20, 2023 from: https://en.wikipedia.org/wiki/Student%27s_t-distribution#Special_cases

[15] Madeline Pace. How the COVID-19 Pandemic Plunged Global Oil Prices (2020).https://global.unc.edu/news-story/how-the-covid-19-pandemic-plunged-global-oil-prices/

[16] Seel et al. Plentiful electricity turns wholesale prices negative (2021).https://www.sciencedirect.com/science/article/pii/S2666792421000652

[17] Bloomberg. Trader Error Causes Huge Plunge in Finnish Power Prices (2023). https://www.bloomberg.com/news/articles/2023-11-23/trader-error-causes-huge-plunge-in-finnish-power-prices

[18] Francis A. Longstaff. Are Negative Option Prices Possible? The Callable U.S. Treasury-Bond Puzzle. Vol. 65, No. 4 (Oct., 1992), pp. 571-592 (22 pages) https://www.jstor.org/stable/2353198

[19] CME Group. Switch to Bachelier Options Pricing Model - Effective April 22, 2020. (2020) https://www.cmegroup.com/notices/clearing/2020/04/Chadv20-171.html

[20] Artemis Capital Management. Volatility at World's End: Deflation, Hyperinflation, and the Alchemy of Risk (2012). https://www.asx.com.au/content/dam/asx/investors/investment-options/vix/volatility-at-worlds-end.pdf

[21] Uniswap Insights 4 of 6: LP Hedging Part 1. Retrieved from Medium Nov 20, 2023 from: https://medium.com/@med456789d/uniswap-insights-4-of-6-lp-hedging-3b958161ab5a

[22] Guillaume Lambert. Pricing Uniswap v3 LP Positions: Towards a New Options Paradigm? (2021).https://lambert-guillaume.medium.com/pricing-uniswap-v3-lp-positions-towards-a-new-options-paradigm-dce3e3b50125

[23] Eisberg, R., Resnick, R. (1985) Quantum Physics of Atoms, Molecules, Solids, Nuclei, and Particles. 2nd Edition, John Wiley and Sons. New York. p.132.ISBN 0-471-87373-X

[24] Zama. TFHE-rs: A pure rust implementation of the TFHE scheme for boolean and integer arithmetics over encrypted data (2022). https://github.com/zama-ai/tfhe-rs

[25] Types. Retrieved from fhEVM, nov 20, 2023 from https://docs.zama.ai/fhevm/writing-contracts/types

[26] Hayden Adams et al. Uniswap v4 (2023) https://github.com/Uniswap/v4-core/blob/main/docs/whitepaper-v4.pdf

[27] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers (2021). https://arxiv.org/pdf/2111.13740.pdf

[28] Louis Bachelier. Theorie de la Speculation (1900). https://archive.org/details/bachelier-theorie-de-la-speculation/page/n5/mode/2up
[29] Yewbow. Retried Nov 20, 2023 from https://info.yewbow.org/#/pools
[30] Apollonius of Perga; Heath, Thomas Little (1896). Treatise on conic sections, edited in modern notation. Cambridge University Press.
[31] Eric Forgy and Leo Lau. A family of multi-asset automated market makers (2021). Retrieved Nov 20, 2023 from https://arxiv.org/pdf/2111.08115v2.pdf
[32] Nassim Nicholas Taleb. Statistical Consequences of Fat Tails: Real World Preasymptotics, Epistemology, and Applications, pp. 99-100 (2 pages) (2020). https://arxiv.org/ftp/arxiv/papers/2001/2001.10488.pdf
[33] Alves, M.I.F.; de Haan, L. and Neves, C. (March 10, 2006). "Statistical inference for heavy and super-heavy tailed distributions" (PDF). Archived from the original (PDF) on June 23, 2007.

G. DISCLAIMER

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of any individuals associated with them. The opinions reflected herein are subject to change without being updated.