CauchyAMM*

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 the scale parameter from the Cauchy distribution.

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] and 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 [8] and clever solutions against centralization at the cost of trade-offs [9]. 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 [10]. We combine this feature with a mechanism based on the Kelly criterion [11] 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 to the Cauchy distribution - a power law that does not obey the law of large numbers [12]. The scale parameter $c = [0, \infty)$ defines the concentration of liquidity.

$$\varphi_{Cauchy}(x) = \frac{1}{\pi} \cdot \frac{c}{x^2 + c^2} \tag{1}$$

cauchyamm@gmail.com, kylekoshiya@gmail.com

* Released on December, 1, 2023

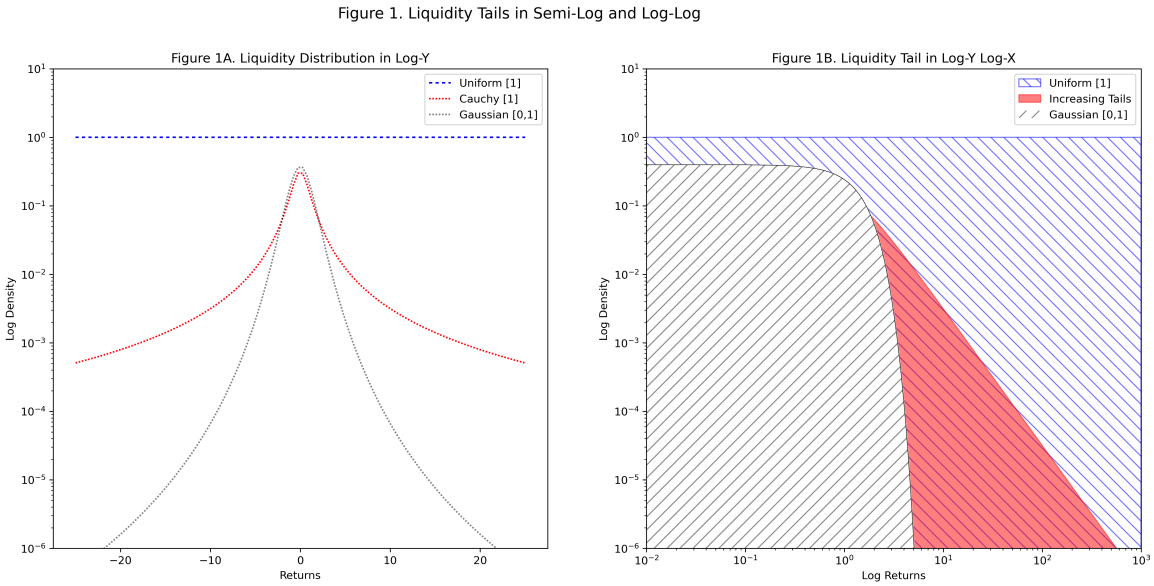

Figure 1. The outlier events of digital assets can extend beyond the Gaussian distribution into fatter tails outlined in red. Extending into the full-range liquidity of a Uniform distribution in blue with Uniswap v2 is capital inefficient, yet concentrating liquidity in Uniswap v3 through a discrete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

The AMM invariant becomes:

$$\left(\pi + \psi(x)\right)\left(\pi - \psi\left(x\right)\right)^{-1} y = s \tag{2}$$

Where $\psi(x) = 2\arctan(\frac{\ln(x)}{2c})$, x is the reserve of the asset, y is the reserve of the numeraire, and s is liquidity with derivation in Appendix A. The liquidity fingerprint in price space becomes the Log-Cauchy distribution.

$$\varphi_{Log-Cauchy}(p) = \frac{1}{\pi p} \cdot \frac{c}{ln(p)^2 + c^2} \tag{3}$$

The build-up of liquidity at the current price and as price approaches zero as well as the heaviness of the right tail as price rapidly jumps is a simply a property of the log-transform of a Cauchy distribution [Figure 2C]. Interestingly, this power law liquidity pattern happens to match the aggregate nature of digital assets where most assets drift towards zero, a select few rapidly jump upwards in market capitalization, and stablecoins remain at the current price. Despite the asymmetric liquidity in the left tail of Log-Cauchy, there is nothing that prevents liquidity from flowing into the negative domain except for the zero bound. In fact it has been empirically observed, with commodities especially, that prices can become negative. Examples being oil in 2020 [13], electricity in Nebraska at night [14], fat-finger trading mistakes in Finland in 2023 [15], and synthetic financial products consisting of highly liquid US treasury bonds [16]. 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 D.

The nature of an LP's payoff 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 C), 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 [17]. The LP is effectively short volatility [18], but instead of being short volatility in a discrete price range as in Uniswap v3, with a Cauchy distribution one is always providing liquidity and in range despite rapid price movements. This makes the LP payoff function a trade-off between a full-range v2 and a concentrated position in v3 [Figure 2B].

Note the unusual behavior of the second derivative Γ_c of the LP in Figure 2D. As c falls below the value of $2/3$ with increased liquidity concentration, Γ_c transitions from a concave function to one with a collapsing fold that resembles the Gamma of a Uniswap v3 position at a tightening tick range [19]. As Gamma approaches zero it forms a local minimum at the current price of 1 and a local maximum at 0.5. The unusual dynamics of this AMM caused by the Cauchy distribution lead us to name it CauchyAMM.

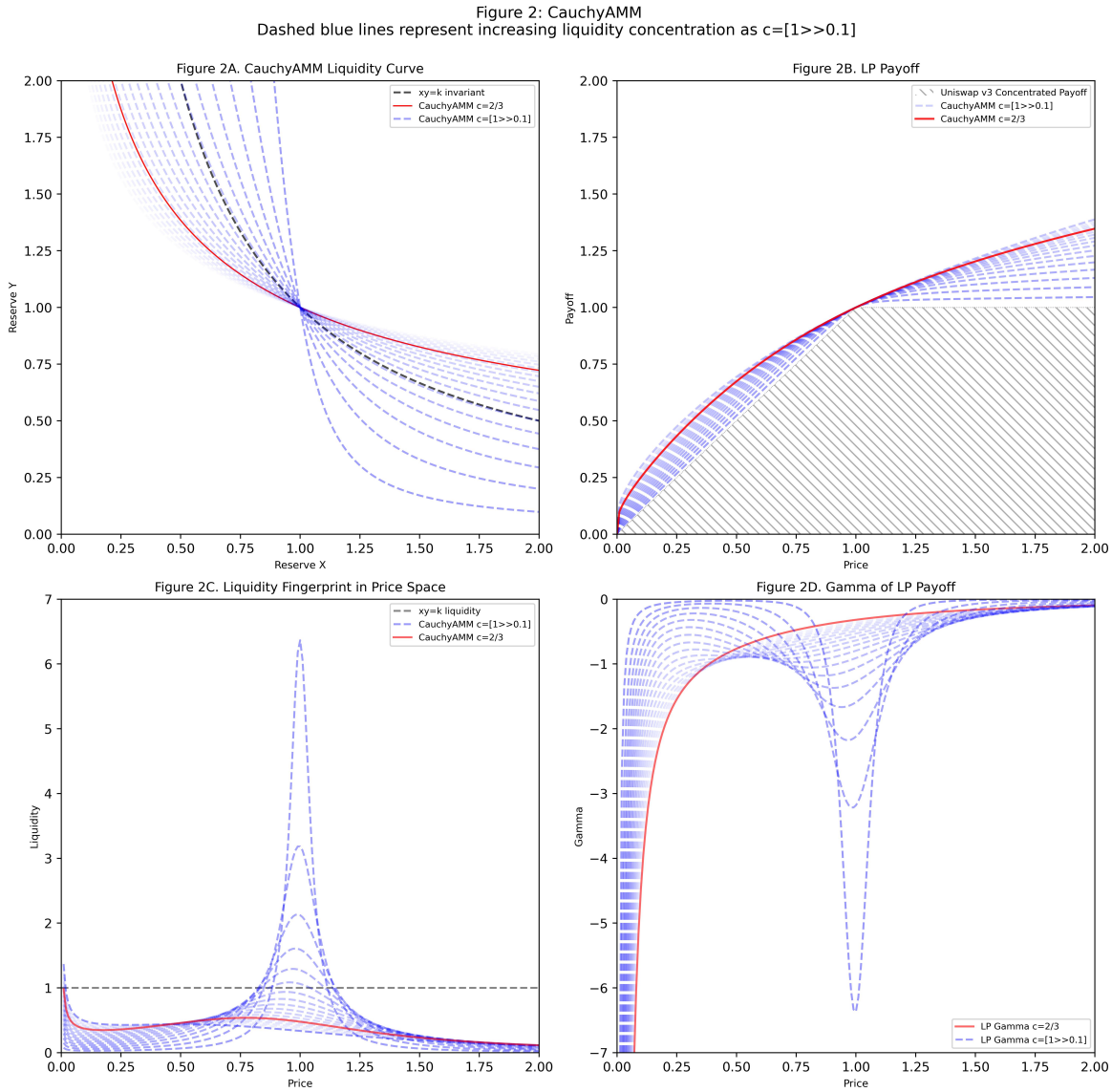

Figure 2. 2A. CauchyAMM invariant with inflection point $c = 2/3$ highlighted in red with Uniswap v2 invariant in dotted black for comparison. 2B: Notice how the LP value of a CauchyAMM does not fully flatten diagonally below the price nor horizontally above the price like a Uniswap v3 LP position despite 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 with more liquidity concentration.

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 [10]. 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 [20] we are able to obfuscate the contents of the transactions in the mempool, converting formally non-fungible individual transactions into completely fungible transactions. 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:

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

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 [21], 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. CAUCHY INVARIANT DERIVATION

Start with the Cauchy distribution.

$$\varphi_c(x) = \frac{1}{\pi} \cdot \frac{c}{x^2 + c^2} \tag{A1}$$

Perform log-transform.

$$\varphi_{lc}(x) = \frac{1}{\pi x} \cdot \frac{c}{\ln(x)^2 + c^2} \tag{A2}$$

Taking the antiderivative and square root of x we get:

$$F_{lc}(x) = \frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2} \tag{A3}$$

For x_r and y_r we get:

$$x_r = 1 - \left(\frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}\right); y_r = \frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2} \tag{A4}$$

The value function [22] becomes:

$$V(x) = x\left(1 - \left(\frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}\right)\right) + \left(\frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}\right) \tag{A5}$$

Deriving liquidity curve:

$$y = \frac{1 - \left(\frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}\right)}{\frac{1}{\pi} \arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}} \tag{A6}$$

Introducing liquidity variable $s = 1$:

$$y = \frac{s\left(1 - \left(\frac{1}{\pi}\arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}\right)\right)}{\frac{1}{\pi}\arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) + \frac{1}{2}} \tag{A7}$$

Solving for s:

$$s = \frac{y\left(2\arctan\left(\frac{\ln(x)}{2c}\right) + \pi\right)}{\pi - 2\arctan\left(\frac{\ln(x)}{2c}\right)} \tag{A8}$$

Simplify and rearrange for s on RHS with $\psi(x)$ where:

$$\psi(x) = 2\arctan\left(\frac{\ln\left(\sqrt{x}\right)}{c}\right) \tag{A9}$$

Resulting in the CauchyAMM invariant outlined in Figure 2A.

$$\left(\pi + \psi(x)\right)\left(\pi - \psi\left(x\right)\right)^{-1} y = s \tag{A10}$$

B. CAUCHY GREEKS

The Greeks for Delta=Δ_c, Gamma=Γ_c, and Theta=Θ_c are given below and available in desmos with the Cauchy AMM at https://www.desmos.com/calculator/vniqyn7zml.

$$\Delta_c\left(x\right) = \frac{1}{2} - \frac{1}{\pi}\left(\arctan\left(\frac{\ln\left(x\right)}{2c}\right) + \frac{2c}{\ln^2\left(x\right) + 4c^2}\right) + \frac{2c}{\pi x\left(\ln^2\left(x\right) + 4c^2\right)} \tag{B11}$$

Gamma undergoes an inflection point as $c < 2/3$.

$$\Gamma_c\left(x\right) = -\frac{2c\left(\ln^2\left(x\right) + 2\ln\left(x\right) + 4c^2\right)}{\pi x^2\left(\ln^2\left(x\right) + 4c^2\right)^2} - \frac{1}{\pi}\left(\frac{2c}{x\left(\ln^2\left(x\right) + 4c^2\right)} - \frac{4c\ln\left(x\right)}{x\left(\ln^2\left(x\right) + 4c^2\right)^2}\right) \tag{B12}$$

Theta is derived from the relationship of concavity to yield as originally outlined by Louis Bachelier in 1900 [23].

$$\Theta_c\left(x\right) = E\langle -\frac{\sigma_{iv}^2}{2}\Gamma_c\left(x\right)\rangle \tag{B13}$$

Here an LP's implied volatility σ_{iv} and can be found by looking at the implied volatility at the current ATM strike price or or from the relationship between volatility and liquidity at the current tick [18]. Both approaches should undergo Lambertian convergence and give the same value over time due to the no arbitrage assumption [18].

C. 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, such as Curve.

$$\frac{2xy}{x+y} = k \tag{C14}$$

This equation, outlined in red in Figure 3B, happens to be a unique condition first derived from ring theory by Forgy and Lau [24] when parameter k_{FL} of the following equation is set to 1.

$$\left(1 - k_{FL}\right)\left(x + y - 2\right) = k_{FL}\left(\frac{1}{x} + \frac{1}{y} - 2\right) \tag{C15}$$

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 3B]. An AMM set to $k_{FL} = 1$ can be useful for charitable/non-profit digital auctions.

D. NEGATIVE PRICE AMM

The spectrum of the conic section discovered by the Apollonius of Perga [25] outlines also the set of liquidity curves that can be constructed in two dimensions with the full equation being:

$$A(x^2) + B(xy) + C(y^2) + D(x) + E(y) + F = 0 \tag{D16}$$

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}.

$$(x - x_{offset})^2 + (y - y_{offset})^2 - B_{fold}(xy) = k \tag{D17}$$

When $B_{fold} < 2$ the AMM folds in on itself see Figure 3D below. 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 [26]. 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, exhibits double convexity[1] [27].

E. FURTHER WORK

The solution to the extreme case of a heavy tail distribution has been presented herein, but is it possible to construct an invariant beyond the heavy tail, a super-fat tailed [28], or a super power distribution invariant that is in-between the Uniform and the Cauchy distribution with basic elementary functions without having to rely on the complex plane?

[1] a condition when two non-linearities work in one's favor, potentially explaining why non-synthetically originating negative prices are metastable.

Figure 3.
AMMs in log-log with dashed diagonal line representing xy=k

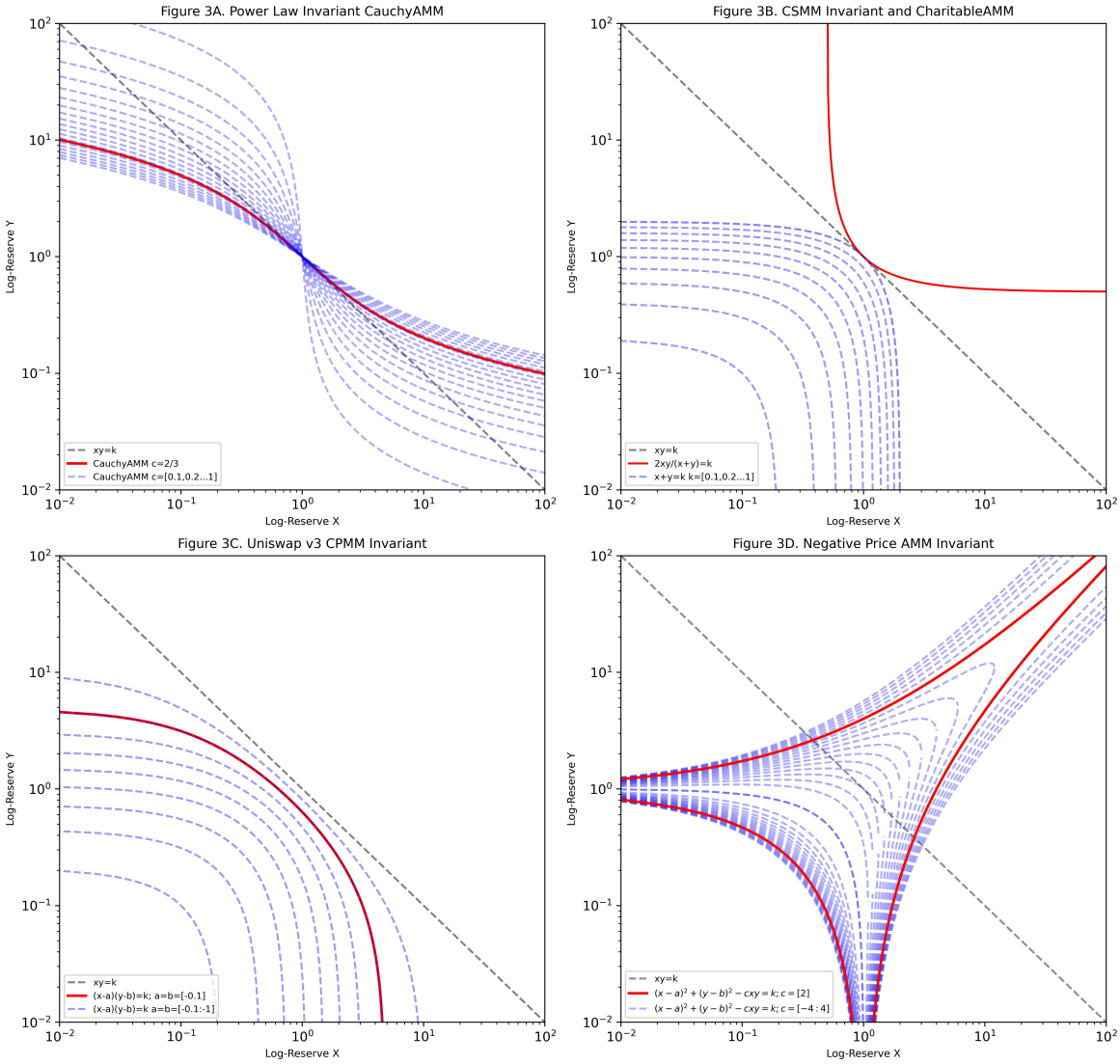

Figure 3. 1A. CauchyAMM with inflection point $c = 2/3$. 1B: AMM invariant of no impermanent loss and CSMM. 1C: Concentrated liquidity in Uniswap v3. 1D: Concentration of liquidity in a negatively priced AMM resembles a Uniswap v3 as long as price does not enter negative territory.

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] Barnabé Monnot. Notes on Proposer-Builder Separation (PBS) (2022).https://barnabe.substack.com/p/pbs
[9] 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
[10] Dahl et al. fhEVM (2023). https://github.com/zama-ai/fhevm/blob/main/fhevm-whitepaper.pdf
[11] Edward Thorp, Leonard Maclean, William Ziemba, The Kelly Capital Growth Investment Criterion: Theory and Practice (February 10, 2011).
[12] Jacoppo Bertolloti. Physics Factlet(249). (2023) https://commons.wikimedia.org/wiki/File:Mean_estimator_consistency.gif
[13] 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/
[14] Seel et al. Plentiful electricity turns wholesale prices negative (2021).https://www.sciencedirect.com/science/article/pii/S2666792421000652
[15] 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
[16] 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
[17] 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
[18] 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
[19] Guillaume Lambert. The Gamma of a Position. (2023) https://twitter.com/guil_lambert/status/1664275166451597315?s=46&t=e0EQ5vcj_HihnkeZ26T4eA
[20] 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
[22] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers (2021). https://arxiv.org/pdf/2111.13740.pdf
[21] Hayden Adams et al. Uniswap v4 (2023) https://github.com/Uniswap/v4-core/blob/main/docs/whitepaper-v4.pdf
[23] Louis Bachelier. Theorie de la Speculation (1900). https://archive.org/details/bachelier-theorie-de-la-speculation/page/n5/mode/2up
[24] 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
[25] Apollonius of Perga; Heath, Thomas Little (1896). Treatise on conic sections, edited in modern notation. Cambridge University Press.
[26] CME Group. Switch to Bachelier Options Pricing Model - Effective April 22, 2020. (2020) https://www.cmegroup.com/notices/clearing/2020/04/Chadv20-171.html
[27] 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
[28] 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

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.