

Axioms for Automated Market Makers: A Mathematical Framework in FinTech and Decentralized Finance

Maxim Bichuch *

Zachary Feinstein †

Wednesday 5th October, 2022

Abstract

Within this work we consider an axiomatic framework for Automated Market Makers (AMMs). By imposing reasonable axioms on the underlying utility function, we are able to characterize the properties of the swap size of the assets and of the resulting pricing oracle. We have analyzed many existing AMMs and shown that the vast majority of them satisfy our axioms. We have also considered the question of fees and divergence loss. In doing so, we have proposed a new fee structure so as to make the AMM indifferent to transaction splitting. Finally, we have proposed a novel AMM that has nice analytical properties and provides a large range over which there is no divergence loss.

Keywords: Decentralized Finance, FinTech, Decentralized Exchange, Automated Market Makers, Divergence Loss, Blockchain.

1 Introduction

Decentralized Finance (DeFi) is a new paradigm for finance which replaces traditional intermediaries with innovative financial technologies based on blockchain. DeFi companies are providing services in areas such as lending and borrowing, insurance underwriting, and trading *without* working with the traditional financial intermediaries. Within this work, we focus on the use of DeFi for constructing markets to trade financial instruments; specifically, Automated Market Makers

*Department of Mathematics, SUNY at Buffalo Buffalo, NY 14260. mbichuch@buffalo.edu. Work is partially supported by NSF grant DMS-1736414.

†School of Business, Stevens Institute of Technology, Hoboken, NJ 07030, USA, zfeinste@stevens.edu.

(AMMs) are a decentralized approach for creating financial markets. The key idea of an AMM is to create a (liquidity) pool of assets against which a trader can transact; a swap is executed on an AMM by balancing the reserves according to mathematical formulas. A key benefit of DeFi and AMMs is that any individual can pool resources into an AMM so that he or she can share in the benefits from providing these key services in the financial system.

The organization of this paper is as follows. The motivation for studying DeFi and, more specifically, AMMs is provided within Section 1.1. A review of the literature on AMMs is provided within Section 1.2. The introduction is then concluded by an overview of the primary contributions and results of this work in Section 1.3. The mathematical construction of a generic AMM is presented within Section 2. With that discussion, the properties of the realized swap value and the pricing oracle derived from the AMM are provided. In Section 3, these axioms and properties are then compared to AMMs that exist in practice as well as a new mathematical structure that can be used for generating new AMMs. Finally, in Section 4, we present a discussion on how AMMs can collect fees along with the possible risks that are involved with becoming a liquidity provider (i.e., the divergence or impermanent loss). We summarize and conclude in Section 5. The proofs of all results are provided within Appendix B.

1.1 Motivation

At the most recent peak for cryptocurrency valuation on Nov 8, 2021, the total market capitalization of various DeFi projects was nearly \$180B.¹ Since then, and especially after the onset of the so-called “crypto winter” in May 2022, the risk of various DeFi projects has come into full view of the public. To highlight just a few DeFi failures: the demise of the algorithmic stablecoin TerraUSD – which was triggered by a run on the Terra Luna coin – wiped out billions of dollars in wealth in a single week; separately, the DeFi lending platform Celsius Networks, which had approximately \$12B in assets under management prior to the crypto winter, filed for bankruptcy in July 2022. With the onset of the crypto winter and the crash in cryptocurrencies, the total value locked in to AMMs has dropped precipitously as well with, e.g., Curve falling from a market capitalization of almost \$3B in early January 2022 to just over \$300M in June 2022.² With the irrational exuberance

¹<https://tradingview.com/markets/cryptocurrencies/global-charts/>

²<https://coinmarketcap.com/currencies/curve-dao-token/>

subsiding, now is the perfect time to explore the viability and risks associated with DeFi projects. Specifically, for the purposes of this work, we wish to quantify the risks, and understand the pitfalls, of AMMs while highlighting the benefits for investors and liquidity providers.

One beneficial aspect of AMMs, and a defining property of it, is the decentralization. While much has been written on the decentralization of transaction verification through blockchain, AMMs also allow for decentralization in rewards. This is because anybody can become a liquidity provider in, and therefore a shareholder of, the AMM. Due to this democratization of market making, AMMs lower the barriers for listing new securities (or tokens) considerably.

Of course, with any type of investment also comes risk; as such, understanding the downsides for liquidity providers (i.e., investors in an AMM) is vital. We tackle this problem by formalizing the axioms that AMMs operate under. For example, we prove that the typical constructions of AMMs in practice (without fees) always have a divergence loss – a detrimental result for liquidity providers. In fact [20] states “this “loss” only disappears when the current proportions of the pool assets equal exactly those at liquidity provision, which is rarely the case.” As such, fees are necessary to provide a cushion for the investors against this loss and, thereby, to encourage investment in AMMs; however, not every fee structure works well. For example, an AMM can charge fees on any of its quoted assets either before or after the verification of a trade. While any combination of fees can intuitively work, some fee structures can lead to, e.g., the AMM charging smaller fees for bulk trades. As far as we are aware, the implication of fees on optimal investor behavior has not previously been studied.

Due to these (and other) conceptual benefits and risks for AMMs, in this work we postulate (intuitive) axioms for AMMs to follow and deduce their implications for traders and liquidity providers. Providing such a mathematical foundation for AMMs permits an exploration of the fundamental properties of these DeFi products; this includes both investigating real-world AMMs and proposing new AMMs that satisfy the appropriate axioms. As touched on above, studying these AMMs mathematically allows us to consider the implications of different fee structures and, importantly, propose a new fee structure for AMMs which is ambivalent to trade execution (i.e., between trading in bulk or splitting a transaction).

1.2 Literature review

AMMs for cryptocurrencies and other digital assets have existed since, at least, 2018 with the launch of Uniswap. As summarized by the defining whitepapers [21, 1], this initial AMM follows a constant product rule for swapping assets. Briefly, and explained more in depth within Section 3.1 and Appendix A.1, if the pool holds two types of assets then the product of the reserves of those assets must be the same before and after any swap is realized. This notion of keeping the value of a function (e.g., the product) of asset reserves invariant to swaps was later generalized into the idea of *constant function market making*.

The basic construction of constant function market makers was formalized in [6]. These structures were studied for use with making foreign exchange markets for digital assets in [18]. Typically for simplicity, and as is taken within this work, these AMMs are presented for markets with two assets only. In [5], trading in multi-asset AMM structures was considered. Alternatively, trading against multiple AMMs was presented within [15]. [9] provides a generalized structure for the interactions that can occur between investors and the AMM. We refer the interested reader to [20] for a summary of terminology and structures that are currently used in practice in this field. [7] studies specific widely-used AMM structures to investigate the implications that this parameterized AMM has on price stability to determine scenarios in which different structures may be most appropriate.

The profitability of AMMs in an economic framework with different investor classes was studied in [10]. The risks, and the appropriate hedging of those risks, for specific AMM structures have been studied in numerous works; we highlight the study of the divergence loss of Uniswap V2 [2] and Uniswap V3 [14]. (These constant product market makers were studied in a number of other works as well, e.g., [12, 4].) The costs of being a liquidity provider were further analyzed within [19]. Conversely, [8] proposes a method to construct AMMs which replicate the payoff of a financial derivative allowing for the study of derivative pricing to inform AMM valuation.

In a separate context, AMMs for prediction markets were first proposed in [16]. Such a structure is fundamentally different from the constant function market makers considered herein insofar as a prediction market includes a terminal time at which bets are realized. As summarized above, constant function market making has no terminal time but rather is focused merely on the spot market between two (or more) assets.

1.3 Primary contributions

In light of the aforementioned growth and contraction of DeFi, and keeping the specific motivations provided within Section 1.1 in mind, the primary contributions of this paper are as follows.

- We construct an **axiomatic definition for AMMs** and characterize the economic implications of these various axioms on the swap amount and pricing oracle within Section 2. As highlighted in Section 1.2, prior studies of AMMs have imposed strict requirements on the structure of the AMM for mathematical simplicity. As discussed in Section 3.1, some of these strict mathematical structures are *not* satisfied by many widely used AMMs, whereas the axioms proposed herein are satisfied.
- Beyond providing axioms and properties for AMMs, we consider (as far as the authors are aware) a novel **fee structure** for an AMM in Section 4. This framework, e.g., imposes a logical indifference to trade execution which is lost by other constructions presented within the literature. Along with the construction of fees, we provide a mathematical description and consideration of the divergence loss – also called impermanent loss – which defines the risk a liquidity provider assumes by pooling with the AMM.
- Of particular use for practitioners, we mathematically **characterize widely-used real-world AMMs** in Section 3 and expanded upon in Appendix A. By characterizing these AMMs, we are able to demonstrate which axioms are satisfied and violated by these structures. We then propose some new AMM constructions which extend real-world AMM constructions in novel ways satisfying the desired mathematical and financial properties discussed within this work.

2 Constant function market maker

Constant function market makers are the most prevalent AMMs that exist in practice; for instance, the most prominent AMM – Uniswap – is a constant function market maker. Due to this prominence, we will often equate the concepts of AMMs and constant function market makers within this work. Fundamentally, a constant function market maker is a multivariate utility function which codifies the value placed on a portfolio by the liquidity providers. This utility function has the

dual task of providing liquidity to the market via swaps and acting as a pricing oracle to quote spot prices on the assets. The construction and axioms of such a utility function is provided within Section 2.1. For simplicity, we will assume the AMM only permits swaps between two assets A and B , although similar axioms can be developed for multi-assets swaps as well. Simply put, and as expressed within e.g. [6], a trader exchanging quantity x of asset A with a constant function market maker u receives quantity $\mathcal{Y}(x)$ of asset B such $u(a+x, b-\mathcal{Y}(x)) = u(a, b)$ where the market maker has initial reserves (a, b) in the two assets; this is explored within Section 2.2. The pricing oracle provides exactly the swap amounts for a marginally small trade, i.e., $\mathcal{Y}'(0)$; this is explored in depth within Section 2.3. Recall that the proofs for all results are provided within Appendix B.

2.1 Axioms

As expressed in the introduction of this section, an AMM is a multivariate (herein always taken to be bivariate) utility function which codifies the value placed on a portfolio by the liquidity providers. This utility function defines the price slippage of swaps and acts as a pricing oracle to quote spot prices on the assets. Within the following definition, we encode the axioms on these AMMs we impose at various points within this work. To simplify notation, throughout we use subscripts to denote partial derivatives; in line with the nomenclature for our two assets, subscript A denotes the partial derivative w.r.t. the first input and B w.r.t. the second input.

Definition 2.1. *An AMM is a utility function $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ that may satisfy the following properties:*

(UfB) Unbounded from below: $u(x, 0) = u(0, y) = -\infty$ for every $x, y \geq 0$ and $u(z) > -\infty$ for every $z \in \mathbb{R}_{++}^2$.

(UfA) Unbounded from above: $\lim_{\bar{x} \rightarrow \infty} u(\bar{x}, y) = \lim_{\bar{y} \rightarrow \infty} u(x, \bar{y}) = \infty$ for every $x, y > 0$.

(SM) Strictly monotonic: $u(z) > u(\bar{z})$ if $z - \bar{z} \in \mathbb{R}_+^2 \setminus \{0\}$ for $z, \bar{z} \in \mathbb{R}_{++}^2$.

(C) Continuous: u is continuous.

(QC) Quasiconcave: u is quasiconcave.

(SI) Scale invariant: if $u(z) \geq u(\bar{z})$ for $z, \bar{z} \in \mathbb{R}_+^2$ then $u(tz) \geq u(t\bar{z})$ for any $t \geq 0$.

(I+) Inada+: u is differentiable with:

- $\lim_{\bar{x} \rightarrow \infty} u_A(\bar{x}, y) = \lim_{\bar{y} \rightarrow \infty} u_B(x, \bar{y}) = 0$,
- $\lim_{\bar{x} \rightarrow \infty} u_B(\bar{x}, y) \in (0, \infty)$, $\lim_{\bar{y} \rightarrow \infty} u_A(x, \bar{y}) \in (0, \infty)$,
- $\lim_{\bar{x} \rightarrow 0} u_A(\bar{x}, y) = \lim_{\bar{y} \rightarrow 0} u_B(x, \bar{y}) = \infty$,
- $\lim_{\bar{x} \rightarrow 0} u_B(\bar{x}, y) < \infty$, $\lim_{\bar{y} \rightarrow 0} u_A(x, \bar{y}) < \infty$

for every $x, y > 0$.

(SC) Single crossing: u is twice continuously differentiable with $u_A(z), u_B(z) > 0$, $u_B(z)u_{AA}(z) \leq u_A(z)u_{AB}(z)$, and $u_A(z)u_{BB}(z) \leq u_B(z)u_{AB}(z)$ for every $z \in \mathbb{R}_{++}^2$.

Remark 1. We wish to note that some of the axioms of Definition 2.1 can imply others. For instance, (SC) implies (SM) and (C) and, additionally, (QC) if at least one of the defining inequalities is strict; this condition is further implied by (SM) and a monotone differences property ($u_{AA}, u_{BB} \leq 0$ and $u_{AB} \geq 0$) that is explicitly given in Assumption 1 of [10] for AMMs. Within our discussion of some real-world AMMs (see Section 3.1), we note that this monotone difference condition is not satisfied in many cases. However, the relevant mathematical properties from monotone differences of an AMM – as shown in [10] – appear to be satisfied under the weaker (SC) condition proposed herein.

Remark 2. We refer to condition (I+) as the Inada+ condition as the usual Inada conditions (i.e., $\lim_{\bar{x} \rightarrow 0} u_A(\bar{x}, y) = \lim_{\bar{y} \rightarrow 0} u_B(x, \bar{y}) = \infty$ and $\lim_{\bar{x} \rightarrow \infty} u_A(\bar{x}, y) = \lim_{\bar{y} \rightarrow \infty} u_B(x, \bar{y}) = 0$ for any $x, y > 0$) are satisfied; in addition to these properties, (I+) also provides the strict monotonicity of $u(x, y)$ in y as $x \rightarrow \infty$ (and vice versa for monotonicity of x as $y \rightarrow \infty$) as well as behavior of the derivatives at 0.

The first task of an AMM, encoded by the utility function $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$, is to act as a liquidity provider to facilitate swaps between the two assets.

Definition 2.2. Let $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ be an AMM. Let $(a, b) \in \mathbb{R}_+^2$ be the size of the reserves of asset A and B within the AMM respectively. The swap values $\mathcal{Y} : \mathbb{R}_+^3 \rightarrow \mathbb{R}_+$ and $\mathcal{X} : \mathbb{R}_+^3 \rightarrow \mathbb{R}_+$ are defined for any $x, y \geq 0$ as:

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

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

Where clear, we will drop the explicit dependence of \mathcal{Y}, \mathcal{X} on the pool sizes $(a, b) \in \mathbb{R}_+^2$.

Remark 3. Though Definition 2.2 differs slightly from the typical form of a constant function market maker (see, e.g., [6]) in that the “constant function” can be an inequality here. Provided the equality is attained (see, e.g., the conditions in Theorem 2.4(2) below), i.e., $u(a + x, b - \mathcal{Y}(x)) = u(a, b)$, we can recover a notion of the indifference price for the quantity x (see, e.g., [11] but for AMMs).

The second task of an AMM, encoded by the utility function $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$, is to act as a pricing oracle $P : \mathbb{R}_{++}^2 \rightarrow \mathbb{R}_{++}$. Throughout this work we will consider the price P of asset A denominated in units of asset B . For B in terms of A , the reciprocal $1/P$ is taken instead; further considerations of the change of numéraire and a bid-ask spread are presented within Sections 2.3 and 4. For the purposes of the definition of the pricing oracle, we will assume that the swap function \mathcal{Y} is differentiable at $(0; a, b)$; we will use the above axioms on the utility u to guarantee this derivative exists within Section 2.2 below.

Definition 2.3. The pricing oracle $P : \mathbb{R}_{++}^2 \rightarrow \mathbb{R}_{++}$ provides the marginal units of asset B obtained from selling a marginal number of units of asset A , i.e., $P(a, b) := \mathcal{Y}'(0; a, b)$ for any $a, b > 0$.

2.2 Swaps

Herein we wish to study the swap values \mathcal{Y}, \mathcal{X} when transferring between the assets using an AMM. To reduce redundancy, throughout this section, we will focus on the properties of the swap of units of A for B only, i.e., properties of \mathcal{Y} as given in Definition 2.2. By symmetry of the AMM, comparable results can be provided for the swap of units of B for A (i.e., \mathcal{X}). We will, specifically, investigate the implications of the axioms of AMMs on: (i) the impact of the swap amount x (Theorem 2.4); (ii) the impact of the pool size a, b (Theorem 2.6); and (iii) a no round-trip arbitrage condition (Lemma 2.7).

Theorem 2.4. Consider an AMM $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$. Fix the initial AMM reserves $a, b > 0$ and swap amounts $x, x_1, x_2 \geq 0$.

1. If (C) then $u(a+x, b-\mathcal{Y}(x)) \geq u(a, b)$.
2. If (C) and $\mathcal{Y}(x) \neq b$ then $u(a+x, b-\mathcal{Y}(x)) = u(a, b)$.
3. If (UfB) and (C) then $\mathcal{Y}(x) < b$.
4. If (SM) then $\mathcal{Y}(0) = 0$.
5. If (SM) then \mathcal{Y} is nondecreasing in x . If, additionally, (UfB) and (C) then \mathcal{Y} is strictly increasing in x .
6. If (UfA), (SM), and (C) then $\lim_{x \rightarrow \infty} \mathcal{Y}(x) = b$.
7. If (C) then \mathcal{Y} is upper semicontinuous.
8. If (C) and (QC) or (SC) then \mathcal{Y} is concave, continuous and a.e. differentiable.
9. If (C) and (SI) then \mathcal{Y} is positive homogeneous in $(x; a, b)$, i.e., $\mathcal{Y}(tx; ta, tb) = t\mathcal{Y}(x; a, b)$ for any $t > 0$.
10. If (SM), (C), and (QC) or (SC) then \mathcal{Y} is subadditive.
11. If (UfB), (SM), and (C) then $\mathcal{Y}(x_1 + x_2; a, b) = \mathcal{Y}(x_1; a, b) + \mathcal{Y}(x_2; a + x_1, b - \mathcal{Y}(x_1; a, b))$.

Remark 4. Theorem 2.4(11) implies an investor is indifferent to trade execution, i.e., splitting a transaction over time between completing it in one trade or splitting it into smaller trades. However, as will be discussed in Remark 13 below, naively assessing fees to transactions can result in this equality no longer holding in general. Theorem 2.4(10) implies splitting a transaction with AMM recovery receives a higher value.

Remark 5. Assume (C) and (QC) or (SC). It follows from Theorem 2.4(8) that \mathcal{Y} and \mathcal{X} are concave. Therefore, sub-differentials of \mathcal{Y} and \mathcal{X} are always well defined, and will a.s. coincide with the derivative. This allows us to give the following definition.

Definition 2.5. Denote $\mathcal{Y}'(x; a, b) := \lim_{\varepsilon \searrow 0} \frac{\mathcal{Y}(x+\varepsilon; a, b) - \mathcal{Y}(x; a, b)}{\varepsilon}$, and similarly for $\mathcal{X}'(x; a, b)$ if they exist. If the AMM is differentiable (with nonzero partial derivatives) then $\mathcal{Y}'(x; a, b) = \frac{u_A(a+x, b-\mathcal{Y}(x; a, b))}{u_B(a+x, b-\mathcal{Y}(x; a, b))}$ by implicit differentiation (similarly for $\mathcal{X}'(x; a, b)$). Furthermore, assuming differentiability of the AMM, denote $\mathcal{Y}_a(x; a, b) = \lim_{\varepsilon \searrow 0} \frac{\mathcal{Y}(x; a+\varepsilon, b) - \mathcal{Y}(x; a, b)}{\varepsilon}$, and similarly for $\mathcal{Y}_b(x; a, b)$, $\mathcal{X}_a(x; a, b)$, $\mathcal{X}_b(x; a, b)$, which can all be formulated via implicit differentiation as well.

Within the next theorem, we want to study the implications of changing the pool sizes a, b for the AMM. Specifically, how altering the pool composition changes the value of a swap and the limiting behavior as pool sizes shrink to 0 or grow to infinity.

Theorem 2.6. *Assume (UfB) and (SC).*

1. $\mathcal{V}_a(x; a, b) \leq 0$ and $\mathcal{V}_b(x; a, b) \in [0, 1)$ for any $x \geq 0$ and $a, b > 0$.
2. $\lim_{\bar{a} \searrow 0} \mathcal{V}(x; \bar{a}, b) = b$ and $\lim_{\bar{b} \searrow 0} \mathcal{V}(x; a, \bar{b}) = 0$ for every $a, b, x > 0$ with the latter limit converging uniformly in a, x .
3. If additionally (QC) and (I+) then $\lim_{\bar{a} \nearrow \infty} \mathcal{V}(x; \bar{a}, b) = 0$ and $\lim_{\bar{b} \nearrow \infty} \mathcal{V}(x; a, \bar{b}) = \infty$ for every $a, b, x > 0$.

Remark 6. *Theorem 2.6(1) provides the interpretation of (SC) as providing a single crossing condition for both $f^A((x, y), \delta) := u(a + \delta + x, b - y)$ and $f^B((x, y), \delta) := u(a + x, b + \delta - y)$ for any $a, b > 0$. Specifically, for any feasible $(x', y') \geq (x'', y'')$ and $\delta' \geq \delta''$,*

$$\begin{aligned} f^A((x', y'), \delta') \geq f^A((x'', y''), \delta') &\Rightarrow f^A((x', y'), \delta'') \geq f^A((x'', y''), \delta'') \\ f^B((x', y'), \delta'') \geq f^B((x'', y''), \delta'') &\Rightarrow f^B((x', y'), \delta') \geq f^B((x'', y''), \delta'). \end{aligned}$$

Similarly, the results can be shown for subtracting x and adding y .

We conclude our discussion of the properties of swaps without fees by considering round-trip arbitrage opportunities. That is, to study if swapping A to B and then back to A (or vice versa of B to A to B) ever provides risk-free profits. In particular, as found in Lemma 2.7 below, a round-trip swap will always leave the trader back with (at most) their initial portfolio. We study the implications of fees within Section 4 below.

Lemma 2.7. *If (SM) and (C) then $\mathcal{X}(\mathcal{V}(x; a, b); a + x, b - \mathcal{V}(x; a, b)) \leq x$ and $\mathcal{V}(\mathcal{X}(y; a, b); a - \mathcal{X}(y; a, b), b + y) \leq y$ for any $x, y \geq 0$ and $a, b > 0$. If, additionally, (UfB) then these inequalities hold as equalities for every $x, y \geq 0$ and $a, b > 0$.*

2.3 Pooling and the pricing oracle

Recall from Definition 2.3 that the pricing oracle $P : \mathbb{R}_{++}^2 \rightarrow \mathbb{R}_{++}$ provides the marginal units of asset B obtained from selling a marginal number of units of asset A , i.e., $P(a, b) := \mathcal{Y}'(0; a, b)$ for any $a, b > 0$.

Remark 7. *Following Lemma 2.7, if (SM) and the AMM u is differentiable then there does not exist a bid-ask spread in the pricing oracle for strictly positive reserves, i.e., $P(a, b) = \mathcal{Y}'(0; a, b) = \frac{1}{\mathcal{X}'(0; a, b)}$ for any $a, b > 0$.*

Proposition 2.8. *Assume (SC).*

- *The pricing oracle P is differentiable with $P_A \leq 0$ and $P_B \geq 0$.*
- *If, additionally, (UfB), (QC), and (I+) then for any $a > 0$, $b \mapsto P(a, b)$ is nondecreasing and surjective on \mathbb{R}_{++} .*
- *If, additionally, (UfB), (QC), and (I+) then for any $b > 0$, $a \mapsto P(a, b)$ is nonincreasing and surjective on \mathbb{R}_{++} .*
- *If, additionally, (SI) then P is scale invariant, i.e., $P(ta, tb) = P(a, b)$ for any reserves $a, b > 0$ with scaling $t > 0$.*

As opposed to more traditional market makers, an AMM allows investors to join the liquidity pool and capture a fraction of the profits (see Section 4 below for a discussion of fee structures). As presented in, e.g., [5], pooling should be accomplished so that the price is unaffected by the injection of additional liquidity into the market. That is, adding $(\alpha, \beta) \in \mathbb{R}_+^2 \setminus \{0\}$ to a pool of size $(a, b) \in \mathbb{R}_{++}^2$ so that $P(a + \alpha, b + \beta) = P(a, b)$. Within the following theorem, we consider a sufficient condition on the pricing oracle so that increasing the size of the reserves actually increases market liquidity, i.e., pooling $(\alpha, \beta) \in \mathbb{R}_+^2 \setminus \{0\}$ results in

$$\mathcal{Y}(x; a + \alpha, b + \beta) \geq \mathcal{Y}(x; a, b), \quad \forall x \geq 0, \quad (2.1)$$

$$\mathcal{X}(y; a + \alpha, b + \beta) \geq \mathcal{X}(y; a, b), \quad \forall y \geq 0. \quad (2.2)$$

Theorem 2.9. *If (UfB) , (QC) , $(I+)$, (SC) , and*

$$P_B(z)P_{AA}(z) - (P(z)P_B(z) + P_A(z))P_{AB}(z) + P(z)P_A(z)P_{BB}(z) \geq 0, \quad \forall z \in \mathbb{R}_{++}^2, \quad (2.3)$$

then pooling (i.e., injecting $(\alpha, \beta) \in \mathbb{R}_+^2 \setminus \{0\}$ to the initial pool $(a, b) \in \mathbb{R}_{++}^2$ such that $P(a + \alpha, b + \beta) = P(a, b)$) increases market liquidity as defined in (2.1) and (2.2).

Remark 8. *Maintaining a constant price is a necessary condition for increased liquidity as $P(a, b) = \mathcal{Y}'(0; a, b) = \frac{1}{\mathcal{X}'(0; a, b)}$. Under (SI), this reduces to the simpler “proportional to current reserves” rule-set that is often assumed instead (see, e.g., [10]).*

Remark 9. *As far as the authors are aware, there is no meaningful financial condition that implies (2.3). This is merely a mathematical argument on the pricing oracle P that provides sufficient conditions for the desired increasing liquidity property of (2.1) and (2.2). As highlighted in Section 3 below, all AMMs studied within this work satisfy this condition.*

3 Examples of AMMs

Within this section we wish to explore a number of different AMMs. Within Section 3.1, we will summarize a number of AMMs that exist in practice; the detailed mathematical representations of these AMMs are provided within Appendix A. A summary of the axioms satisfied by these real-world AMMs is provided within Table 1. Within Section 3.2, we construct a novel generalized AMM structure; we use that structure to provide a new concentrated liquidity swap structure which has strong theoretical stability properties. We wish to remind the reader that many of the AMMs presented below, and detailed in Appendix A, are often characterized as the exponential of the utility functions provided herein; as the definition of the swap values \mathcal{X}, \mathcal{Y} are based on relative utilities, this exponentiation does not impact the implementation, only the description, of the AMM.

3.1 AMMs in practice

Herein we summarize a number of AMMs that exist in practice. The details for all of these AMMs are provided within Appendix A. We, also, refer the reader to Table 1 which summarizes the

AMM	Details	(UfB)	(UfA)	(SM)	(C)	(QC)	(SI)	(I+)	(SC)	(2.3)
<i>Uniswap V2</i>	A.1	X	X	X	X	X	X	X	X	X
<i>Balancer</i>	A.2	X	X	X	X	X	X	X	X	X
<i>Uniswap V3</i>	A.3		X	X	X	X		X	X	X
<i>mStable</i>	A.4		X	X	X	X	X		X	X
<i>StableSwap</i>	A.5.1		X	X	X	X		X	X	X
<i>L.StableSwap</i>	A.5.2	X	X	X	X	X	X	X	X	X
<i>Curve</i>	A.6	X	X	X	X	X*	X	X	X*	X*
<i>Dodo</i>	A.7	X	X	X	X	X	X	X	X	
<i>SDAMM</i>	3.2	X [†]	X [†]	X [†]	X [†]	X [†]		X [†]	X [†]	X [†]

Table 1: Summary of popular AMMs and the axioms satisfied.

†: Under some conditions specified in Proposition 3.1.

*: Axiom verified numerically.

findings about all example AMMs considered within this work.

Fundamentally, most current AMMs are built based on two structures:

- *Uniswap V2*: As presented in Appendix A.1, Uniswap V2 is the AMM with logarithmic utility function, i.e., $u(x, y) = \log(x) + \log(y)$. Notably, this simple structure satisfies all axioms presented within this work. However, Uniswap V2 is often criticized as it is subject to high price slippage as it tends to save a lot of liquidity solely for the tail of the price distribution (so as to guarantee infinite liquidity).
- *mStable*: As presented in Appendix A.4, mStable is an AMM that has no price slippage at all, i.e., $u(x, y) = \log(x + y)$. In order to guarantee the constant price of mStable, this AMM fails to satisfy (UfB) and (I+).

By combining the notions of these AMMs in different ways, a liquidity provider is able to concentrate liquidity, i.e., control the price slippage from trades. *StableSwap* ($u(x, y) = \log(C(x + y) + xy)$ for parameter $C > 0$; see Appendix A.5.1) considers a linear combination of Uniswap V2 and mStable *within* the logarithm. By doing so, there is less price impact than Uniswap V2 but at the expense of infinite liquidity and positive homogeneity (i.e., (UfB) and (SI) are not satisfied). *Curve* is an extension of StableSwap that satisfies (UfB) and (SI) but is only implicitly defined ($u(x, y) = \log(D(x, y))$ for $D(x, y)^3 + 4(C - 1)xyD(x, y) - 4C(x + y)xy = 0$ with parameter $C \geq 1$; see Appendix A.6). To maintain the infinite liquidity and concentrate liquidity around a price of 1, the price impacts in the tails (i.e., when one of the pools is nearly exhausted) become exceedingly

high. Within Appendix A.5.2, we introduce a new AMM structure, as the linear combination of UniSwap V2 and mStable, which we call *L.StableSwap* ($u(x, y) = C \log(x + y) + \log(x) + \log(y)$ for parameter $C > 0$). As with Uniswap V2 and Curve, all axioms are satisfied for this new construction and it is subject to low price slippage near pool balance ($a \approx b$ for reserves $a, b > 0$). Notably, in contrast to Curve, L.StableSwap is constructed with a simple analytical utility function.

Other AMMs are built from the structure of Uniswap V2 directly. *Balancer* ($u(x, y) = w \log(x) + (1 - w) \log(y)$ for parameters $w \in (0, 1)$; see Appendix A.2) is merely a weighted version of Uniswap V2 so as to scale the asset pools when pricing. *Uniswap V3* ($u(x, y) = \log(\alpha + x) + \log(\beta + y)$ for parameters $\alpha, \beta > 0$; see Appendix A.3) introduces “virtual reserves” so as to concentrate liquidity and decrease price slippage. However, the concentrated liquidity introduced in Uniswap V3 comes at the expense of (UfB) and (SI) so that, much like StableSwap, it only has finite liquidity and does not scale linearly.

The final AMM which we consider that is used in practice is *Dodo* ($u(x, y) = \log(P\alpha(x, y) + \beta(x, y))$ for external price $P > 0$; see Appendix A.7). Dodo is fundamentally different from all other AMMs considered within this work as it uses an *exogenous* pricing oracle (such as a centralized exchange) and does not provide its own pricing oracle. Because there is no endogenous pricing oracle, Dodo permits pooling and withdrawing in any combination of assets (though with the possibility of withdrawal fees so as to guarantee the withdrawal is possible). The utility for Dodo is constructed in such a way to attempt to match the external price.

Remark 10. *As noted within Remark 1, [10] assumes AMMs satisfy a monotone differences property ($u_{AA}, u_{BB} \leq 0$ and $u_{AB} \geq 0$). However, the utility functions for mStable, StableSwap, Curve, and Dodo do not satisfy this stronger property.*

3.2 Symmetric Decomposable AMM

Herein we propose a new class of AMMs which we name *Symmetric Decomposable AMMs* (SDAMMs) that provides a simple analytical structure for the utility function. This is in contrast to the majority of currently existing AMMs which, by and large, are combinations of Uniswap V2 and mStable. Specifically, define the SDAMM utility function as

$$u(x, y) = U(x) + U(y)$$

for any $x, y \geq 0$ with the univariate utility function $U : \mathbb{R}_+ \rightarrow \mathbb{R} \cup \{-\infty\}$. This can be seen as a generalization of Uniswap V2 since taking $U(z) := \log(z)$ for any $z \geq 0$ exactly replicates this well-known AMM.

The following proposition relates the properties of the univariate utility function U to the axioms of the associated SDAMM. We omit the proof of this proposition as these properties are trivial to verify.

Proposition 3.1. *Let $U : \mathbb{R}_+ \rightarrow \mathbb{R} \cup \{-\infty\}$ be a twice-differentiable univariate utility function and let u be the associated SDAMM. Immediately, u satisfies (C).*

- *If $U(0) = -\infty$ and $U(z) > -\infty$ for any $z > 0$ then (UfB).*
- *If $\lim_{z \rightarrow \infty} U(z) = \infty$ then (UfA).*
- *If U is strictly increasing then (SM).*
- *If U is concave then (QC) and (SC).*
- *If $\lim_{z \rightarrow \infty} U'(z) = 0$ and $\lim_{z \rightarrow 0} U'(z) = \infty$ then (I+).*
- *If U' is log-convex then (2.3).*

Proposition 3.1 provides simple conditions on $U : \mathbb{R}_+ \rightarrow \mathbb{R} \cup \{-\infty\}$ to guarantee the various axioms proposed within this work. As these properties are easily satisfied (see, e.g., Uniswap V2 and Example 3.2), we highlight in Table 1 that SDAMM satisfies these axioms.

With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{U'(x)}{U'(y)}$$

for $x, y \geq 0$. In contrast to many of the aforementioned AMMs, pooling for SDAMM can be much more complex as it need not satisfy (SI). In fact, to accomplish pooling in such a case, we recommend a scheme in which the liquidity provider supplies the assets in any ratio which the AMM then swaps appropriately to maintain a constant price. For instance, in Example 3.2 below, we consider a specific function U that satisfies all of properties proposed in Proposition 3.1 but is not scale invariant (SI); this proposed new AMM structure concentrates liquidity around the

balanced reserve price of 1. Within Section 4.2 below, we investigate some important implications of dropping the scale invariance (SI) axiom.

Example 3.2. *Let $U(z) = \log(\sinh(Cz^q))$ with $C > 0$ and $q \in (0, 1]$ for any $z \geq 0$. This satisfies all the properties considered within Proposition 3.1 except for (SI) if $q < 1$; however, if $q = 1$, then (I+) is no longer satisfied as well. We use the hyperbolic sine function because it limits to the exponential function as the pool size grows to infinity. As such this AMM limits to mStable when the pool size is large enough (and as $q \rightarrow 1$). In this way, this AMM can have extremely stable prices at 1, even more than Curve, and have infinite liquidity. In order to gain this price stability, an (extremely) unbalanced pool has extremely high price impacts in order to remain liquid.*

4 Fee structures and divergence loss

Thus far, we have only discussed AMMs without any explicit fees collected by the liquidity providers. Within this section we propose a novel structure for assessing fees on a swap. We will provide an explicit formulation of a bid-ask spread and how this fee structure impacts the value of swaps. Additionally, we will present some implications of this fee structure; in doing so, we will also directly compare this construction to the prior methods of assessing fees discussed within the literature (e.g., [6, 18]). We conclude this section by commenting briefly on the so-called “impermanent loss” or divergence loss [20] for the liquidity providers of the AMM. As before, we will primarily focus on the properties of \mathcal{Y} as the results are symmetric to \mathcal{X} .

4.1 Assessing fees on the marginal price

Herein we wish to propose a novel structure for assessing fees on a swap. Specifically, we propose that a fee $\gamma \in [0, 1]$ is assessed to each marginal unit being bought. This is accomplished by assessing the fees directly on the price as given by the pricing oracle P . This interpretation is consistent with a typical financial interpretation of a bid-ask spread (see, e.g., [13]). This structure is compared with prior fee structures for AMMs in Remark 13.

Definition 4.1. *Let $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ be an AMM with associated pricing oracle $P : \mathbb{R}_{++}^2 \rightarrow \mathbb{R}_{++}$. Let $a, b > 0$ be the size of the reserves of asset A and B within the AMM respectively. Let*

$\gamma \in [0, 1]$ be the fee level assessed on a transaction. The swap functions with fees $\mathcal{Y}_\gamma : \mathbb{R}_+^3 \rightarrow \mathbb{R}_+$ and $\mathcal{X}_\gamma : \mathbb{R}_+^3 \rightarrow \mathbb{R}_+$ are defined for any $x, y \geq 0$ as:

$$\mathcal{Y}_\gamma(x; a, b) := (1 - \gamma) \int_0^x P(a + z, b - \mathcal{Y}_\gamma(z; a, b)) dz, \quad (4.1)$$

$$\mathcal{X}_\gamma(y; a, b) := (1 - \gamma) \int_0^y \frac{1}{P(a - \mathcal{X}_\gamma(z; a, b), b + z)} dz. \quad (4.2)$$

Where clear, we will drop the explicit dependence of $\mathcal{Y}_\gamma, \mathcal{X}_\gamma$ on the pool sizes $(a, b) \in \mathbb{R}_{++}^2$.

The intuition behind the constructions (4.1) and (4.2) is that the AMM should be indifferent to the size of transactions; a sequence of unidirectional small trades should have the same result for the AMM as a single large trade (assuming nothing happens in between the transactions). In other words, a trade of $\mathcal{Y}_\gamma(x; a, b)$ and then another (infinitesimal) trade $\mathcal{Y}_\gamma(dx; a + x, b - \mathcal{Y}_\gamma(x; a, b))$ should be equivalent to a single trade of $\mathcal{Y}_\gamma(x + dx; a, b)$ from the perspective of the AMM. Charging γ proportion in fees, and using the fact that $\mathcal{Y}_\gamma(dx; a + x, b - \mathcal{Y}_\gamma(x; a, b)) \approx \mathcal{Y}'_\gamma(0; a + x, b - \mathcal{Y}_\gamma(x; a, b))dx = (1 - \gamma)P(a + x, b - \mathcal{Y}_\gamma(x; a, b))dx$, we arrive at an equivalent ODE formulation for (4.1):

$$\mathcal{Y}'_\gamma(x) = (1 - \gamma)P(a + x, b - \mathcal{Y}_\gamma(x)) =: (1 - \gamma)g(x, \mathcal{Y}_\gamma(x)) \quad \forall x \geq 0 \quad (4.3)$$

with initial value $\mathcal{Y}_\gamma(0) = 0$. (An ODE can similarly be provided for \mathcal{X}_γ).

Assumption 4.2. *Throughout the remainder of this paper, we will consider AMMs satisfying (UfB), (QC), (I+), and (SC).*

Before continuing with the discussion of these fees, we will prove that the AMM with fees is well-defined in that there exists unique swap functions $\mathcal{Y}_\gamma, \mathcal{X}_\gamma$ given by Definition 4.1.

Lemma 4.3. *Let $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ be an AMM satisfying Assumption 4.2. There exists unique swap functions $\mathcal{Y}_\gamma, \mathcal{X}_\gamma$ for any $\gamma \in [0, 1]$.*

Remark 11. *By construction of the pricing oracle of an AMM satisfying Assumption 4.2, if the fees are zero ($\gamma = 0$), we recover $\mathcal{Y}_0 \equiv \mathcal{Y}$ since $P(a + x, b - \mathcal{Y}(x; a, b)) = \mathcal{Y}'(0; a + x, b - \mathcal{Y}(x; a, b)) = \mathcal{Y}'(x; a, b)$. That is, the AMM recovers the swap amounts \mathcal{Y} as presented in the prior sections when no fees are assessed.*

Before studying the properties of the modified swap functions and pricing oracle, we wish to provide an explicit example of the swap function \mathcal{Y}_γ under a real-world AMM construction.

Example 4.4. Consider the Uniswap V2 utility function $u(x, y) = \log(x) + \log(y)$ as discussed in Section 3.1 and Appendix A.1. For this AMM, the pricing oracle $P(x, y) = y/x$ is the ratio of the reserves. The swap for $x \geq 0$ with fee level $\gamma \in [0, 1]$ can be found to be

$$\mathcal{Y}_\gamma(x; a, b) = b \left(1 - \frac{a^{1-\gamma}}{(a+x)^{1-\gamma}} \right)$$

by solving the differential equation (4.3).

We now consider our first property of the AMM with fees. Specifically, as expected, as the fees γ increase then the AMM will pay out less in a swap.

Proposition 4.5. Let $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ be an AMM satisfying Assumption 4.2. For any $0 \leq \gamma_1 < \gamma_2 \leq 1$,

$$0 \leq \mathcal{Y}_{\gamma_2}(x; a, b) < \mathcal{Y}_{\gamma_1}(x; a, b) \leq \mathcal{Y}(x; a, b), \quad (4.4)$$

$$0 \leq \mathcal{X}_{\gamma_2}(y; a, b) < \mathcal{X}_{\gamma_1}(y; a, b) \leq \mathcal{X}(y; a, b),$$

for every $x, y > 0$ and $a, b > 0$.

We now turn our attention to the fundamental properties of AMMs that, without fees, were studied previously in Theorem 2.4. Within the following corollary, we find that all relevant properties are satisfied by \mathcal{Y}_γ with strictly positive fees. For this result we restrict ourselves to fee levels $\gamma \in (0, 1)$; if $\gamma = 0$ then we recover the original swap values (as discussed in Remark 11) and if $\gamma = 1$ then $\mathcal{Y}_1 \equiv 0$ by construction.

Corollary 4.6. Consider an AMM $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ satisfying Assumption 4.2. Fix the fee level $\gamma \in (0, 1)$, initial AMM reserves $a, b > 0$, and swap amounts $x, x_1, x_2 \geq 0$.

1. $u(a+x, b-\mathcal{Y}_\gamma(x)) \geq u(a, b)$ with strict inequality if $x > 0$.
2. \mathcal{Y}_γ is strictly increasing, concave, and subadditive in x .
3. If, additionally, (UfA), then $\lim_{x \rightarrow \infty} \mathcal{Y}_\gamma(x) = b$.

4. If, additionally, (SI), then \mathcal{Y} is positive homogeneous in $(x; a, b)$, i.e., $\mathcal{Y}_\gamma(tx; ta, tb) = t\mathcal{Y}_\gamma(x; a, b)$ for any $t > 0$.

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

Remark 12. In contrast to the fee-less construction provided within Section 2 (and as expected), introducing a fee $\gamma \in (0, 1)$ immediately introduces a bid-ask spread. Specifically, the bid price is given by $\mathcal{Y}'_\gamma(0) = (1 - \gamma)P(a, b)$ and the ask price is given by $\mathcal{X}'_\gamma(0)^{-1} = (1 - \gamma)^{-1}P(a, b)$ for any pool reserves $(a, b) \in \mathbb{R}_{++}^2$. Note that the pricing oracle $P(a, b)$ is between the bid and ask prices but is not the mid-price.

As a direct consequence of the bid-ask spread discussed in Remark 12, the introduction of fees guarantees a strict no-arbitrage condition.

Corollary 4.7. Consider an AMM $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ satisfying Assumption 4.2. If $\gamma \in (0, 1]$ then $\mathcal{X}_\gamma(\mathcal{Y}_\gamma(x; a, b); a + x, b - \mathcal{Y}_\gamma(x; a, b)) < x$ and $\mathcal{Y}_\gamma(\mathcal{X}_\gamma(y; a, b); a - \mathcal{X}_\gamma(y; a, b), b + y) < y$ for any $x, y > 0$ and $a, b > 0$.

We wish to conclude the discussion of properties of the swap amounts with fees by studying the dependence of \mathcal{Y}_γ on the reserves (a, b) as well as the fees γ .

Corollary 4.8. Consider an AMM $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ satisfying Assumption 4.2. Fix the fee level $\gamma \in (0, 1]$. Then $\frac{\partial}{\partial a}\mathcal{Y}_\gamma(x; a, b) \leq 0$ and $\frac{\partial}{\partial b}\mathcal{Y}_\gamma(x; a, b) \in [0, 1)$ for any $x \geq 0$ and $a, b > 0$.

Remark 13. The fee structure introduced herein is not the only approach that can be used for an AMM. We wish to highlight two alternate structures which can be viewed as assessing the fees on the assets sold or bought by the investor respectively. With both of these structures we wish to briefly comment on how an investor may want to optimally split a transaction when transacting with the AMM; this lack of indifference to trade splitting leads to strange implications for the AMM (i.e., the liquidity provider should only care about the final state of the AMM rather than how trades are executed).

1. Consider the fees collected on the asset being sold to the AMM. That is, a fraction $\gamma \in [0, 1]$ of x is taken by the AMM to compensate it for acting as a liquidity provider. Mathematically, this is encoded by

$$\bar{\mathcal{Y}}_\gamma(x; a, b) := \mathcal{Y}((1 - \gamma)x; a, b).$$

That is, the collected fees are γx of asset A so that the realized pool size, after the swap is completed, is still of the form $(a + x, b - \mathcal{Y}_\gamma(x; a, b))$. We wish to note that this is the fee structure considered in, e.g., [6, 18].

Though a simple structure to implement, this fee structure provides a discount to buying in bulk, i.e., $\bar{\mathcal{Y}}_\gamma(x_1 + x_2; a, b) \geq \bar{\mathcal{Y}}_\gamma(x_1; a, b) + \bar{\mathcal{Y}}_\gamma(x_2; a + x_1, b - \bar{\mathcal{Y}}_\gamma(x_1; a, b))$. By imposing costs to an investor who splits her transaction, the AMM is subsidizing large traders.

2. Consider the fees collected on the asset being bought by the trader. That is, a fraction $\gamma \in [0, 1]$ of \mathcal{Y} is taken by the AMM to compensate it for acting as a liquidity provider. Mathematically, this is encoded by

$$\bar{\mathcal{Y}}^\gamma(x; a, b) := (1 - \gamma)\mathcal{Y}(x; a, b).$$

That is, the collected fees are $\gamma\mathcal{Y}(x; a, b)$ of asset B so that the realized pool size, after the swap is completed, is still of the form $(a + x, b - \bar{\mathcal{Y}}^\gamma(x; a, b))$.

In contrast to the fees on the sold asset, imposing fees on the bought asset provides a benefit to an investor who splits her trade over time, i.e., $\bar{\mathcal{Y}}^\gamma(x_1 + x_2; a, b) \leq \bar{\mathcal{Y}}^\gamma(x_1; a, b) + \bar{\mathcal{Y}}^\gamma(x_2; a + x_1, b - \bar{\mathcal{Y}}^\gamma(x_1; a, b))$. By encouraging these small transactions, the AMM incentivizes traders to make a series of infinitesimally small transactions; that is, an intelligent trader will, in fact, implement the integral strategy \mathcal{Y}_γ we propose in Definition 4.1.

4.2 Divergence loss

The divergence loss, also known as impermanent loss, is defined as the cost of providing liquidity to the pool. Note that this cost is only realized once the provider withdraws their liquidity provision from the AMM. We note that even though the concept appears to be simple, a rigorous mathematical definition would require a dynamic treatment. Therefore, to simplify the divergence loss and match the construction used elsewhere in the literature (see, e.g., [2, 14]), we assume that the withdrawal happens after a single swap. That is, first the liquidity provider invests the funds, second the price moves because of a trade, and finally the liquidity is withdrawn. This cost can be viewed as the mark-to-market loss from repurchasing the original pooled portfolio after withdrawal. Formally this is defined directly below.

Definition 4.9. Consider an AMM with reserves $(a, b) \in \mathbb{R}_{++}^2$ and fee level $\gamma \in [0, 1]$. Let $(\alpha, \beta) \in \mathbb{R}_+^2 \setminus \{0\}$ such that $P(a + \alpha, b + \beta) = P(a, b)$. The divergence loss $\Delta : (0, \infty) \rightarrow \mathbb{R}$ depending implicitly on (a, b, α, β) is the difference between the mark-to-market value of (α, β) being held and being pooled, i.e.,

$$\Delta(p) := \begin{cases} [p\alpha + \beta] - \frac{P(a,b)\alpha + \beta}{P(a,b)[a+\alpha] + [b+\beta]} [p(a + \alpha + x_p) + (b + \beta - \mathcal{Y}_\gamma(x_p; a + \alpha, b + \beta))] & \text{if } p < P(a, b) \\ 0 & \text{if } p = P(a, b) \\ [p\alpha + \beta] - \frac{P(a,b)\alpha + \beta}{P(a,b)[a+\alpha] + [b+\beta]} [p(a + \alpha - \mathcal{X}_\gamma(y_p; a + \alpha, b + \beta)) + (b + \beta + y_p)] & \text{if } p > P(a, b) \end{cases}$$

where $x_p > 0$ is such that $p = P(a + \alpha + x_p, b + \beta - \mathcal{Y}_\gamma(x_p; a + \alpha, b + \beta))$ and $y_p > 0$ is such that $p = P(a + \alpha - \mathcal{X}_\gamma(y_p; a + \alpha, b + \beta), b + \beta + y_p)$.

Remark 14. Note that the domain of Δ is $(0, \infty)$ under Assumption 4.2. In other words, for any $p < P(a, b)$ there exists some $x_p > 0$ such that $p = P(a + \alpha + x_p, b + \beta - \mathcal{Y}_\gamma(x_p; a + \alpha, b + \beta))$, and similarly for any $p > P(a, b)$ there exists some $y_p > 0$ such that $p = P(a + \alpha - \mathcal{X}_\gamma(y_p; a + \alpha, b + \beta), b + \beta + y_p)$. To see this, recall that the pricing oracle P is differentiable with $P_A \leq 0$ and $P_B \geq 0$. As \mathcal{Y}_γ is strictly increasing, we find that $P(a + \alpha + x, b + \beta - \mathcal{Y}_\gamma(x; a + \alpha, b + \beta)) < P(a, b)$ for any $x > 0$. Furthermore, $0 \leq \lim_{x \rightarrow \infty} P(a + \alpha + x, b + \beta - \mathcal{Y}_\gamma(x; a + \alpha, b + \beta)) \leq \lim_{x \rightarrow \infty} P(a + \alpha + x, b + \beta) = 0$. Therefore, together with continuity, this guarantees the existence of such x_p .

Often it is convenient to consider the divergence loss as a function of the swap amounts rather than prices. That is, $\bar{\Delta} : \mathbb{R} \rightarrow \mathbb{R}$ defined as:

$$\bar{\Delta}(z) := \begin{cases} \Delta(P(a + \alpha + z, b - \mathcal{Y}_\gamma(z; a + \alpha, b + \beta))) & \text{if } z \geq 0, \\ \Delta(P(a + \alpha - \mathcal{X}_\gamma(-z; a + \alpha, b + \beta), b + \beta - z)) & \text{if } z < 0, \end{cases}$$

so as to remove the explicit dependence of Δ on the mappings x_p, y_p .

Lemma 4.10. Consider an AMM satisfying Assumption 4.2 and (SI). The divergence loss can be

simplified as:

$$\Delta(p) = \begin{cases} \frac{\delta}{1+\delta}[\mathcal{Y}_\gamma(x_p; (1+\delta)a, (1+\delta)b) - px_p] & \text{if } p < P(a, b), \\ 0 & \text{if } p = P(a, b), \\ \frac{\delta}{1+\delta}[p\mathcal{X}_\gamma(y_p; (1+\delta)a, (1+\delta)b) - y_p] & \text{if } p > P(a, b), \end{cases}$$

where, implicitly, $\alpha := \delta a$ and $\beta := \delta b$ for some $\delta > 0$. Furthermore, the sign of the divergence loss can be characterized w.r.t. the fees:

1. if $\gamma = 0$ then $\Delta(p) \geq 0$ with strict inequality if $p \neq P(a, b)$;
2. if $\gamma \in (0, 1]$ then there exist $p_* < P(a, b) < p^*$ such that $\Delta(p) < 0$ for $p \in (p_*, p^*) \setminus \{p\}$.

We now want to consider the divergence loss for two AMMs. First, we revisit Uniswap V2 with fees (Example 4.4) in order to formalize the results of Lemma 4.10 for this well-known AMM. Second, we consider SDAMM with the log of the hyperbolic sine (Example 3.2) to consider the divergence loss when (SI) is not satisfied.

Example 4.11. Recall the Uniswap V2 AMM with fees from Example 4.4 with initial reserves $(a, b) \in \mathbb{R}_{++}^2$. That is, given the fee level $\gamma \in (0, 1)$, $\mathcal{Y}_\gamma(x; a, b) = b \left(1 - \left(\frac{a}{a+x}\right)^{1-\gamma}\right)$ and $\mathcal{X}_\gamma(y; a, b) = a \left(1 - \left(\frac{b}{b+y}\right)^{1-\gamma}\right)$ for any transactions $x, y \geq 0$. As Uniswap V2 satisfies (SI), the results of Lemma 4.10 hold. Furthermore, as noted within Remark 8 and used in Lemma 4.10, we take the liquidity injection to be $\alpha = \delta a$ and $\beta = \delta b$ for some $\delta > 0$. We wish to consider the form of the divergence loss (characterized as $\bar{\Delta}$) and the threshold prices p_*, p^* which construct the interval of divergence gains for the liquidity provider. Let $z \in \mathbb{R}$ then

$$\bar{\Delta}(z) = \begin{cases} \delta b \left(1 - 2 \left(\frac{(1+\delta)a}{(1+\delta)a+z}\right)^{1-\gamma} + \left(\frac{(1+\delta)a}{(1+\delta)a+z}\right)^{2-\gamma}\right) & \text{if } z \geq 0 \\ \delta b \left(1 - 2 \left(\frac{(1+\delta)b-z}{(1+\delta)b}\right) + \left(\frac{(1+\delta)b-z}{(1+\delta)b}\right)^{2-\gamma}\right) & \text{if } z < 0. \end{cases}$$

We will now direct our attention to determining the threshold prices p_*, p^* . Consider, first, $p_* \leq P(a, b) = b/a$ which involves studying $\bar{\Delta}(z)$ for $z \geq 0$. It can be determined that $\bar{\Delta}(z) < 0$ for $z \geq 0$ if and only if $z \in (0, x_* := \frac{(1+\delta)(1-t_*)a}{t_*})$ where $t_* \in (0, 1 - \gamma)$ solves $1 - 2t^{1-\gamma} + t^{2-\gamma} = 0$. The lower bound p_* for divergence gains can be determined by finding the price assuming x_* assets were

transacted, i.e.,

$$p_* := P((1 + \delta)a + x_*, (1 + \delta)b - \mathcal{Y}_\gamma(x_*; (1 + \delta)a, (1 + \delta)b) = \frac{b}{a} t_*^{2-\gamma} < \frac{b}{a} = P(a, b).$$

Following similar arguments, we determine that the divergence loss is negative for $z < 0$ if and only if $z \in (-y^* := -(1 + \delta)b(t^* - 1), 0)$ where $t^* \in (1 + \gamma)^{\frac{1}{1-\gamma}} + (0, -\frac{1-2(1+\gamma)^{\frac{1}{1-\gamma}} + (1+\gamma)^{\frac{2-\gamma}{1-\gamma}}}{\gamma(1-\gamma)})$ solves $1 - 2t + t^{2-\gamma} = 0$, i.e., the upper bound p^* for divergence gains is

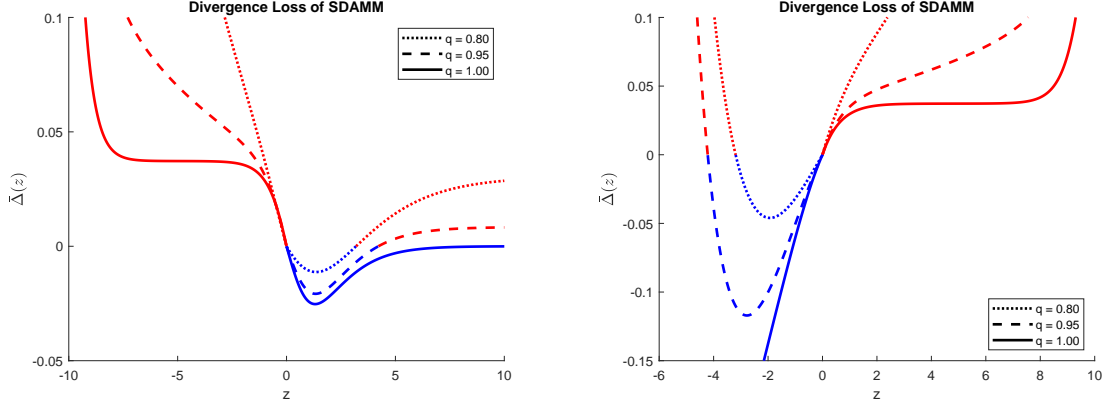
$$p^* := P((1 + \delta)a - \mathcal{X}_\gamma(y^*; (1 + \delta)a, (1 + \delta)b), (1 + \delta)b + y^*) = \frac{b}{a} (t^*)^{2-\gamma} > \frac{b}{a} = P(a, b).$$

Remark 15. Though only provided as a sufficient condition for divergence gain, we hypothesize that Lemma 4.10(2) can be strengthened insofar as we conjecture that $\Delta(p) > 0$ for $p \notin [p_*, p^*]$ under (SI) with fees $\gamma \in (0, 1)$. We highlight in Example 4.11, that this stronger conjecture is satisfied in that special case. To be proven for a generic AMM, this requires that $\mathcal{Y}_\gamma(x; a, b) - P(a + x, b - \mathcal{Y}_\gamma(x; a, b))x \geq 0$ for $x > x^*$ (wlog suppressing the need for $\delta \geq 0$ in this expression). However, this expression is not necessarily monotonic nor convex in x which makes such a proof highly non-trivial and beyond the scope of this work.

As previously mentioned, to conclude, we will focus on SDAMM with the hyperbolic sine (Example 3.2) to study divergence loss when some axioms may not be satisfied. Specifically, and comparing to Lemma 4.10, (SI) appears to be necessary to the positivity of divergence loss.

Example 4.12. Recall the SDAMM structure from Section 3.2 such that $u(x, y) = U(x) + U(y)$ for univariate utility functions U . Specifically, take $U(z) := \log(\sinh(Cx^q))$ for $C > 0$ and $q \in (0, 1]$ as in Example 3.2. Note that this structure does not satisfy (SI) and, therefore, the results of Lemma 4.10 do not hold. We wish to explore two cases herein: the possibility of divergence gains even without fees (and the impact of $q \in (0, 1]$ on the gains/losses) and the impact that fees have on decreasing the divergence loss.

For the first scenario, consider $q \in \{0.8, 0.95, 1\}$ (i.e., satisfying (I+) in the first two settings and not satisfying it in the $q = 1$ setting) without fees $\gamma = 0$. The divergence losses are plotted in Figure 1 with gains plotted in blue and losses in red. Notably, in all three choices of q we have regions in which there are divergence gains even though there are no fees. Though these plots may



(a) Pooling $\alpha = 1$ with reserves $(a, b) = (10, 1)$. (b) Pooling $\beta = 1$ with reserves $(a, b) = (1, 10)$.

Figure 1: Plot of the divergence loss $\bar{\Delta}$ for the hyperbolic sine SDAMM under varied $q \in \{0.8, 0.95, 1\}$.

appear as if the divergence loss is kept negative when trading is in the direction of the pool imbalance, this is only due to the x -axis used in these plots; if $|z|$ is large enough then $\bar{\Delta}(z) \geq 0$ in any choice of q . We also wish to note that the divergence loss decreases as we increase q .

In the second scenario, we focus solely on the $q = 1$ setting but vary the fee level $\gamma \in [0, 1)$.³ In order to study this case, we first note that the swaps with fees can be computed explicitly as:

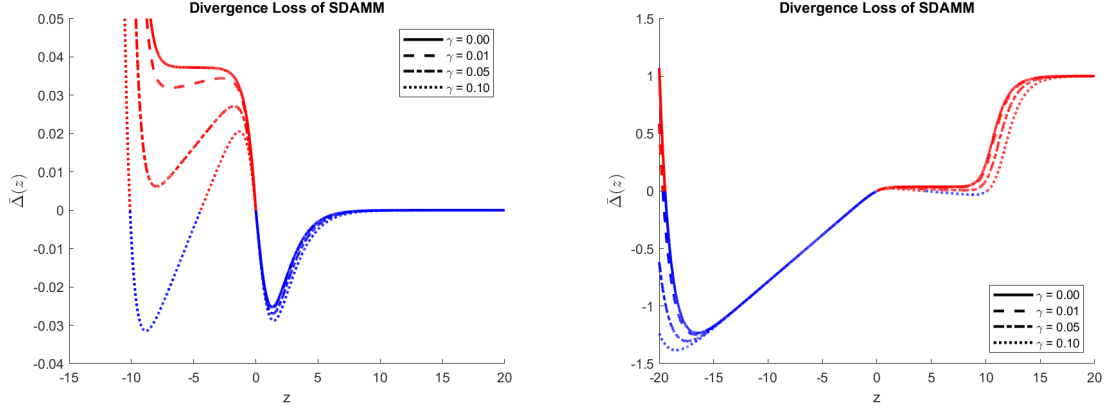
$$\begin{aligned}\mathcal{Y}_\gamma(x; a, b) &= b - \frac{1}{C} \sinh^{-1} \left(\left(\frac{\sinh(Ca)}{\sinh(C(a+x))} \right)^{1-\gamma} \sinh(Cb) \right), \\ \mathcal{X}_\gamma(y; a, b) &= a - \frac{1}{C} \sinh^{-1} \left(\sinh(Ca) \left(\frac{\sinh(Cb)}{\sinh(C(b+y))} \right)^{1-\gamma} \right),\end{aligned}$$

for $x, y \geq 0$ with reserves $(a, b) \in \mathbb{R}_{++}^2$. The divergence losses are plotted in Figure 2 with gains plotted in blue and losses in red. Not surprisingly, as the fees increase, the divergence loss decreases. However, for $|z|$ large enough, i.e. when the price moves far enough away from the initial price, there is always a divergence loss.

5 Conclusion

Within this work we have considered an axiomatic framework for AMMs. By imposing reasonable axioms on the underlying utility function, we are able to characterize the properties of the swap

³Though the $q = 1$ setting does not satisfy Assumption 4.2, the requisite properties for swaps with fees still hold in this case.



(a) Pooling $\alpha = 1$ with reserves $(a, b) = (10, 1)$ (b) Pooling $\beta = 1$ with reserves $(a, b) = (1, 10)$.

Figure 2: Plot of the divergence loss $\bar{\Delta}$ for the hyperbolic sine SDAMM under varied $\gamma \in \{0, 0.01, 0.05, 0.10\}$.

size of the assets and of the resulting pricing oracle. We have analyzed many existing AMMs and shown that the vast majority of them satisfy our axioms. Finally, we have also considered the question of fees and divergence loss. In doing so, we have proposed a new fee structure so as to make the AMM indifferent to trade execution. Finally, we have proposed a novel AMM that, while it does not satisfy all of our axioms, has nice analytical properties and provides a large range over which there is no divergence loss.

We wish to provide a few extensions for this work. First, and importantly, a rigorous study of the conjecture provided within Remark 15 would greatly enhance our understanding of the divergence loss and the impacts that scale invariance (SI) has on those costs. Second, within this work and throughout the literature on constant function market makers, a single utility function $u : \mathbb{R}_+^2 \rightarrow \mathbb{R} \cup \{-\infty\}$ is always considered; herein we propose considering the generalized AMM with incomplete preference relation \succeq on \mathbb{R}_+^2 so that, e.g., $\mathcal{V}(x; a, b) = \sup\{y \in [0, b] \mid (a + x, b - y) \succeq (a, b)\}$. In this way the fees can be endogenized within the preference relation itself. Related to the first two extensions, we propose further studies on new AMM constructions so as to minimize divergence loss (and maximize revenue for liquidity providers) much as we undertook with the SDAMM example within this work. Finally, within this paper, we only considered the traditional style AMMs, i.e., for swap markets. In order to grow the decentralized finance offerings, a rigorous study of AMMs for derivatives and other complex financial securities needs to be undertaken.

References

- [1] Hayden Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core. 2020.
- [2] Andreas A Aigner and Gurvinder Dhaliwal. Uniswap: Impermanent loss and risk profile of a liquidity provider. *arXiv preprint arXiv:2106.14404*, 2021.
- [3] Charalambos D. Aliprantis and Kim C. Border. *Infinite Dimensional Analysis: A Hitchhiker’s Guide*. Springer, 2007.
- [4] Álvaro Cartea, Fayçal Drissi, and Marcello Monga. Decentralised finance and automated market making: Execution and speculation. *Available at SSRN 4144743*, 2022.
- [5] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant function market makers: Multi-asset trades via convex optimization. *arXiv preprint arXiv:2107.12484*, 2021.
- [6] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 80–91, 2020.
- [7] Guillermo Angeris, Alex Evans, and Tarun Chitra. When does the tail wag the dog? curvature and market making. *arXiv preprint arXiv:2012.08040*, 2020.
- [8] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers. *arXiv preprint arXiv:2103.14769*, 2021.
- [9] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. A theory of automated market makers in defi. In *International Conference on Coordination Languages and Models*, pages 168–187. Springer, 2021.
- [10] Agostino Capponi and Ruizhe Jia. The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*, 2021.
- [11] René Carmona. *Indifference pricing: theory and applications*. Princeton University Press, 2008.
- [12] Joseph Clark. The replicating portfolio of a constant product market. *Available at SSRN 3550601*, 2020.
- [13] Harold Demsetz. The cost of transacting. *The quarterly journal of economics*, 82(1):33–53, 1968.
- [14] Jun Deng and Hua Zong. Static replication of impermanent loss for concentrated liquidity provision in decentralised markets. *arXiv preprint arXiv:2205.12043*, 2022.
- [15] Daniel Engel and Maurice Herlihy. Composing networks of automated market makers. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, pages 15–28, 2021.

- [16] Robin Hanson. Logarithmic markets coring rules for modular combinatorial information aggregation. *The Journal of Prediction Markets*, 1(1):3–15, 2007.
- [17] P. Hartman. *Ordinary Differential Equations: Second Edition*. Classics in Applied Mathematics. Society for Industrial and Applied Mathematics, 2002.
- [18] Alex Lipton and Artur Sepp. Automated market-making for fiat currencies. *arXiv preprint arXiv:2109.12196*, 2021.
- [19] Jason Milionis, Ciamac C Moallemi, Tim Roughgarden, and Anthony Lee Zhang. Automated market making and loss-versus-rebalancing. *arXiv preprint arXiv:2208.06046*, 2022.
- [20] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols. *arXiv preprint arXiv:2103.12732*, 2021.
- [21] Yi Zhang, Xiaohong Chen, and Daejun Park. Formal specification of constant product ($x \times y = k$) market maker model and implementation. 2018.

A Details of Existing Automated Market Makers

A.1 Uniswap V2

Though we refer to this example as Uniswap V2, the same mathematical structure is also utilized within many other AMMs in practice such as SushiSwap, DefiSwap, and Quickswap. Structurally, Uniswap V2 is the logarithmic utility function, i.e.,

$$u(x, y) = \log(x) + \log(y)$$

for $x, y \geq 0$. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{y}{x}$$

for $x, y \geq 0$. This AMM permits pooling at the ratio of the current reserves. As highlighted within Table 1, this AMM satisfies every axiom proposed within this work.

A.2 Balancer

Though we refer to this example as Balancer, the same mathematical structure is also utilized within many other AMMs in practice such as Bancor and Loopring. Structurally, Balancer is a weighted version of Uniswap V2, i.e.,

$$u(x, y) = w \log(x) + (1 - w) \log(y)$$

with $w \in (0, 1)$ for $x, y \geq 0$. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{wy}{(1 - w)x}$$

for $x, y \geq 0$. This AMM permits pooling at the ratio of the current reserves. As highlighted within Table 1, this AMM satisfies every axiom proposed within this work.

A.3 Uniswap V3

Though we refer to this example as Uniswap V3, the same mathematical structure is also utilized within many other AMMs in practice such as KyberSwap and MooniSwap. The generic structure of all of these AMMs is the same as Uniswap V2 but with “virtual reserves” to provide concentrated liquidity, i.e.,

$$u(x, y) = \log(\alpha + x) + \log(\beta + y)$$

with $\alpha, \beta > 0$ for $x, y \geq 0$. Each of these real-world AMMs select α, β in different ways which may be dynamic in time or based on the implemented trades. For instance, Uniswap V3 implements this AMM in such a way that α, β are adjusted dynamically so that the AMM maintains a fixed maximum and minimum quoted price. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{\beta + y}{\alpha + x}$$

for $x, y \geq 0$. This AMM permits pooling at the ratio of the current reserves *inclusive* of the virtual reserves α, β . As mentioned, these virtual reserves concentrate the liquidity to reduce price impacts from a transaction, but this comes at the cost of unbounded from below. Additionally, as constructed here with static α, β , Uniswap V3 fails to be scale invariant. As highlighted in Table 1, Uniswap V3 does *not* satisfy (UfB) or (SI).

A.4 mStable

mStable is an AMM constructed to have no price impacts from trading. This is accomplished through the mathematical structure

$$u(x, y) = \log(x + y)$$

for $x, y \geq 0$. This AMM comes with the constant pricing oracle

$$P(x, y) = 1$$

for any $x, y \geq 0$. Pooling for mStable can, in theory, be accomplished with any combination of assets; traditionally, pooling is done either at the current ratio of assets or so that the pooled assets are in equal proportion. As with Uniswap V3, the ability to reduce price impacts (in this case to 0) comes at the expense of unbounded from below (UfB); in fact, these 0 price impacts also cause the AMM to lose (I+). Furthermore, though (SC) is satisfied, it is only satisfied with an equality (and thus does not guarantee quasiconcavity by itself).

A.5 Stable swaps

A.5.1 StableSwap

Though we refer to this example as StableSwap, the same mathematical structure is also utilized with many other AMMs in practice such as Saber and Saddle. Much like Uniswap V3, StableSwap aims to concentrate liquidity towards the “balanced” pool. This is accomplished by taking a linear combination of

(the exponentials of) Uniswap V2 and mStable, i.e.,

$$u(x, y) = \log(C(x + y) + xy)$$

with $C > 0$ for $x, y \geq 0$. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{C + y}{C + x}$$

for $x, y \geq 0$. This AMM permits pooling at the ratio of the current reserves inclusive of the parameter C . As with Uniswap V3, the ability to reduce price impacts come at the expense of unbounded from below (UfB) and is not scale invariant (SI).

A.5.2 Liquid StableSwap [L.StableSwap]

As far as we are aware, this construction has never been implemented before as an AMM in practice. Rather than taking the linear combination of exponentials of Uniswap V2 and mStable, here we take the linear combination directly, i.e.,

$$u(x, y) = C \log(x + y) + \log(x) + \log(y)$$

with $C > 0$ for $x, y \geq 0$. This concentrates liquidity when the reserves of the AMM are not too far out of balance, but exacerbates price impacts once the reserves of the AMM become too skewed towards one asset. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{y[(C + 1)x + y]}{x[x + (C + 1)y]}$$

for $x, y \geq 0$. By taking this structure all axioms proposed within this work are satisfied in comparison to Uniswap V3, mStable and StableSwap.

A.6 Curve

Curve is a popular AMM that, much like our newly proposed Liquid StableSwap, extends StableSwap in such a way so as to guarantee infinite liquidity through satisfying (UfB). For the construction of Curve, let $D(x, y)$ denote the total number of coins when the reserves $(x, y) \in \mathbb{R}_{++}^2$ are traded into balance from a StableSwap AMM, i.e., $\log(C(x + y) + xy) = \log(CD(x, y) + D(x, y)^2/4)$. However, in contrast to StableSwap, Curve considers a *functional* parameter $\mathcal{C}(x, y)$; by dimensional analysis $\mathcal{C}(x, y)$ must have units in number of coins (so that $\mathcal{C}(x, y)(x + y)$ and xy are both in number of coins squared). Furthermore, with the notion that Curve desires a balanced pool, $\mathcal{C}(x, y)$ is constructed to be proportional to both the number of coins for the

balanced pool ($D(x, y)$) and to a unitless measure of pool balance, i.e., $\mathcal{C}(x, y) \propto D(x, y) \times \left(\frac{xy}{D(x, y)^2/4}\right)$ where $\frac{xy}{D(x, y)^2/4} \in [0, 1]$ provides a measure of AMM balance. With this functional parameter $\mathcal{C}(x, y) := \frac{Cxy}{D(x, y)}$ with constant C , the balanced pool size $D(x, y)$ satisfies the equation

$$\begin{aligned} \log(\mathcal{C}(x, y)(x + y) + xy) &= \log\left(\mathcal{C}(x, y)D(x, y) + \frac{D(x, y)^2}{4}\right) \\ \Leftrightarrow D(x, y)^3 + 4(C - 1)xyD(x, y) - 4C(x + y)xy &= 0. \end{aligned} \quad (\text{A.1})$$

It is this balanced pool size $D(x, y)$ which defines the utility function for Curve. Specifically,

$$u(x, y) = \log(D(x, y))$$

for $x, y \geq 0$ where $D(x, y)$ is implicitly defined as the *unique* nonnegative root of (A.1) for $C \geq 1$. Uniqueness of $D(x, y)$ follows from an application of Descartes' rule of signs. With this utility function, the pricing oracle is defined as

$$P(x, y) = \frac{y[C(2x + y) - (C - 1)D(x, y)]}{x[C(x + 2y) - (C - 1)D(x, y)]}$$

for $x, y \geq 0$. Despite the complex, implicit, structure of this pricing oracle, Curve permits pooling at the current ratio of reserves because it satisfies (SI). Due to the implicit construction of the Curve AMM, (some of) the axioms presented within this paper can only be verified numerically. Even so, as highlighted within Table 1, all axioms presented are satisfied for Curve either analytically or (for (QC), (SC), and (2.3)) numerically.

A.7 Dodo

In contrast to all other AMMs presented herein, Dodo is constructed based on an *exogenous* pricing oracle (e.g., a centralized exchange) and does not provide its own pricing oracle. In doing so, Dodo permits pooling in any combination of assets rather than guaranteeing the pricing oracle is kept constant. To guarantee that the AMM has the requisite liquidity, withdrawal fees may be assessed; these withdrawal fees take the place of the divergence loss (see Section 4.2) of other AMMs. Mathematically, Dodo takes the form

$$u(x, y) = \log(P\alpha(x, y) + \beta(x, y))$$

for exogenous pricing signal P and such that $\alpha, \beta : \mathbb{R}_+^2 \rightarrow \mathbb{R}_+$ satisfy price matching and equilibrium pooling, i.e.,

- *price matching*: the value of $\alpha(x, y)$ is equal to $\beta(x, y)$, i.e., $P\alpha(x, y) = \beta(x, y)$;

- *equilibrium pooling*: when an endogenized price $Pf(x, y)$ (to account for the actual AMM reserves) is used, the value of the portfolio (x, y) should be equivalent to $(\alpha(x, y), \beta(x, y))$, i.e., $Pf(x, y)(\alpha(x, y) - x) + (\beta(x, y) - y) = 0$. Within the current construction of Dodo, the price modifier function $f : \mathbb{R}_+^2 \rightarrow \mathbb{R}_+$ is defined as

$$f(x, y) := \begin{cases} 1 + C \left(\frac{\alpha(x, y)}{x} - 1 \right) & \text{if } Px \leq y, \\ \left[1 + C \left(\frac{\beta(x, y)}{y} - 1 \right) \right]^{-1} & \text{if } Px > y, \end{cases}$$

with $C \in [0, 1]$ for any $x, y \geq 0$.

Note that the construction of Dodo has a parameter $C \in [0, 1]$ for the appropriate notion of equilibrium pooling. If $C = 0$ then $u(x, y) = \log(Px + y)$ is equivalent to the mStable AMM; if $C = 1$ then $u(x, y) = \log(2\sqrt{Pxy}) \rightsquigarrow \log(x) + \log(y)$ is equivalent to the Uniswap V2 AMM. In fact, a closed form for the Dodo construction can be provided for $C \in [0, 1]$ such that

$$u(x, y) = \begin{cases} \log \left(2 \left[\frac{-(1-C)Px + \sqrt{(1-C)^2 P^2 x^2 + C Px((1-C)Px + y)}}{C} \right] \right) & \text{if } Px \leq y, \\ \log \left(2 \left[\frac{-(1-C)y + \sqrt{(1-C)^2 y^2 + C y(Px + (1-C)y)}}{C} \right] \right) & \text{if } Px > y. \end{cases}$$

As highlighted within Table 1, Dodo satisfies all *relevant* axioms proposed within this work provided $C > 0$; (2.3) is not studied for Dodo due to the use of the exogenous pricing oracle.

B Proofs

B.1 Proof of Theorem 2.4

- Proof.* 1. Let $C(\bar{z}) := \{z \in \mathbb{R}_+^2 \mid u(z) \geq u(\bar{z})\}$ denote the set of positions $z \in \mathbb{R}_+^2$ that exceed $\bar{z} \in \mathbb{R}_+^2$ in utility. By (upper semi)continuity, $C(\bar{z})$ is closed for every $\bar{z} \in \mathbb{R}_+^2$. Therefore $\mathcal{Y}(x) = \sup\{y \mid y \in [0, b], (a + x, b - y) \in C(a, b)\}$ is the supremum over a compact set and thus is attained.
2. Assume $\mathcal{Y}(x) < b$. Then, by construction of \mathcal{Y} , $u(a + x, b - [\mathcal{Y}(x) + \epsilon]) < u(a, b)$ for any $\epsilon \in (0, b - \mathcal{Y}(x)]$. By (lower semi)continuity, $u(a + x, b - \mathcal{Y}(x)) \leq \liminf_{\epsilon \searrow 0} u(a + x, b - [\mathcal{Y}(x) + \epsilon]) \leq u(a, b)$.
3. Assume $\mathcal{Y}(x) = b$ then $u(a + x, b - \mathcal{Y}(x)) = u(a + x, 0) \geq u(a, b)$ contradicts (UfB).
4. By (SM), $u(a, b) > u(a, b - y)$ for any $y \in (0, b]$, which immediately results in $\mathcal{Y}(0) = 0$.
5. It trivially follows from (SM) that $\mathcal{Y}(x) \leq \mathcal{Y}(x + \Delta)$ for any $\Delta \geq 0$. To prove the strict monotonicity, by contradiction, let $\Delta > 0$ and assume $\mathcal{Y}(x) = \mathcal{Y}(x + \Delta)$. Therefore, by (SM),

$$u(a + x + \Delta, b - \mathcal{Y}(x + \Delta)) = u(a + x + \Delta, b - \mathcal{Y}(x)) > u(a + x, b - \mathcal{Y}(x)) \geq u(a, b).$$

From item (3) within this theorem, we can already conclude that $\mathcal{V}(x), \mathcal{V}(x + \Delta) < b$. As such, we now obtain a contradiction to item (2). Therefore, it must follow that $\mathcal{V}(x + \Delta) > \mathcal{V}(x)$.

6. By the first claim in item (5) within this theorem and monotone convergence, $\mathcal{V}(x) \nearrow \mathcal{V}^*$ for some $\mathcal{V}^* \leq b$. Assume $\mathcal{V}^* < b$ (and therefore $\mathcal{V}(x) \neq b$ for every $x > 0$), then

$$u(a, b) = u(a + x, b - \mathcal{V}(x)) \geq u(a + x, b - \mathcal{V}^*) \quad \forall x > 0.$$

Taking the limit as x tends to infinity implies $\infty > u(a, b) \geq \lim_{\bar{a} \rightarrow \infty} u(\bar{a}, b - \mathcal{V}^*) = \infty$ which forms a contradiction, i.e., $\mathcal{V}^* = b$.

7. Note that $\bar{C}(x) := \{y \in [0, b] \mid u(a + x, b - y) \geq u(a, b)\}$ is upper continuous by the closed graph theorem [3, Theorem 17.11]. Thus by [3, Lemma 17.30], $\mathcal{V}(x) = \sup\{y \mid y \in \bar{C}(x)\}$ is upper semicontinuous.
8. First, under axioms (C) and (QC), the hypograph

$$\text{hypo } \mathcal{V} = \{(x, y) \in \mathbb{R}_+ \times \mathbb{R} \mid \mathcal{V}(x) \geq y\} = \{(x, y) \in \mathbb{R}_+ \times \mathbb{R} \mid y \leq b, u(a + x, b - y) \geq u(a, b)\}$$

is trivially convex. Now, instead, assume (SC) holds. By implicit differentiation, and with all derivatives of the utility u being taken at $(a + x, b - \mathcal{V}(x))$,

$$\mathcal{V}''(x) = \frac{u_B[u_B u_{AA} - u_A u_{AB}] + u_A[u_A u_{BB} - u_B u_{AB}]}{u_B^3} \leq 0.$$

9. By item (1) within this theorem, $u(a + x, b - \mathcal{V}(x; a, b)) \geq u(a, b)$. An application of (SI) implies $u(t[a + x], t[b - \mathcal{V}(x; a, b)]) \geq u(ta, tb)$ for any $t > 0$, i.e., $\mathcal{V}(tx; ta, tb) \geq t\mathcal{V}(x; a, b)$ by construction. The reverse inequality ($\mathcal{V}(tx; ta, tb) \leq t\mathcal{V}(x; a, b)$) follows trivially by applying this result to $(tx; ta, tb)$ with scaling factor t^{-1} .
10. By item (4) within this theorem, $\mathcal{V}(0) = 0$. Further, by item (8), \mathcal{V} is concave. Combining these properties, $\mathcal{V}(x_1) \geq \frac{x_1}{x_1 + x_2} \mathcal{V}(x_1 + x_2)$ and $\mathcal{V}(x_2) \geq \frac{x_2}{x_1 + x_2} \mathcal{V}(x_1 + x_2)$. Therefore, $\mathcal{V}(x_1) + \mathcal{V}(x_2) \geq \mathcal{V}(x_1 + x_2)$, i.e., \mathcal{V} is subadditive.
11. By items (2) and (3), it immediately follows that $u(a + x, b - \mathcal{V}(x; a, b)) = u(a, b)$ for any $x \geq 0$ and $a, b > 0$. By (SM), $u(a + x, b - \mathcal{V}(x; a, b) - \epsilon) < u(a, b)$ for any $x \geq 0$, $a, b > 0$, and $\epsilon \in (0, b - \mathcal{V}(x; a, b)]$. Therefore, if $u(a + x, b - y) = u(a, b)$ it must follow that $\mathcal{V}(x; a, b) = y$. Using this result we recover the desired property because:

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

□

B.2 Proof of Theorem 2.6

Proof. 1. By implicit differentiation (and noting $u_A, u_B > 0$ by (SC)):

$$\begin{aligned}\mathcal{Y}_a(x; a, b) &= \frac{u_A(a+x, b - \mathcal{Y}(x; a, b)) - u_A(a, b)}{u_B(a+x, b - \mathcal{Y}(x; a, b))} \\ \mathcal{Y}_b(x; a, b) &= \frac{u_B(a+x, b - \mathcal{Y}(x; a, b)) - u_B(a, b)}{u_B(a+x, b - \mathcal{Y}(x; a, b))} < 1.\end{aligned}$$

Therefore, the results hold if $\frac{\partial}{\partial x} u_A(a+x, b - \mathcal{Y}(x; a, b)) \leq 0$ and $\frac{\partial}{\partial x} u_B(a+x, b - \mathcal{Y}(x; a, b)) \geq 0$.

Consider these derivatives:

$$\begin{aligned}\frac{\partial}{\partial x} u_A(a+x, b - \mathcal{Y}(x; a, b)) &= u_{AA}(a+x, b - \mathcal{Y}(x; a, b)) - \mathcal{Y}'(x; a, b) u_{AB}(a+x, b - \mathcal{Y}(x; a, b)) \\ &= u_{AA}(a+x, b - \mathcal{Y}(x; a, b)) - \frac{u_A(a+x, b - \mathcal{Y}(x; a, b))}{u_B(a+x, b - \mathcal{Y}(x; a, b))} u_{AB}(a+x, b - \mathcal{Y}(x; a, b)) \leq 0, \\ \frac{\partial}{\partial x} u_B(a+x, b - \mathcal{Y}(x; a, b)) &= u_{AB}(a+x, b - \mathcal{Y}(x; a, b)) - \mathcal{Y}'(x; a, b) u_{BB}(a+x, b - \mathcal{Y}(x; a, b)) \\ &= u_{AB}(a+x, b - \mathcal{Y}(x; a, b)) - \frac{u_A(a+x, b - \mathcal{Y}(x; a, b))}{u_B(a+x, b - \mathcal{Y}(x; a, b))} u_{BB}(a+x, b - \mathcal{Y}(x; a, b)) \geq 0\end{aligned}$$

taking advantage of \mathcal{Y} strictly increasing and differentiable.

2. (a) By item (1) within this theorem and monotone convergence, $\mathcal{Y}(x; \bar{a}, b) \nearrow \mathcal{Y}^*$ for some $\mathcal{Y}^* \leq b$ as $\bar{a} \searrow 0$. Assume $\mathcal{Y}^* < b$, then

$$u(\bar{a}, b) = u(\bar{a} + x, b - \mathcal{Y}(x; \bar{a}, b)) \geq u(\bar{a} + x, b - \mathcal{Y}^*) \quad \forall \bar{a} > 0.$$

Taking the limit as \bar{a} tends to 0 leads to $-\infty = \lim_{\bar{a} \searrow 0} u(\bar{a}, b) \geq \lim_{\bar{a} \searrow 0} u(\bar{a} + x, b - \mathcal{Y}^*) = u(x, b - \mathcal{Y}^*) > -\infty$ which forms a contradiction, i.e., $\mathcal{Y}^* = b$.

- (b) For every $\epsilon > 0$, we have that $|\mathcal{Y}(x; a, \hat{b})| < \hat{b} \leq \epsilon$ for any $\hat{b} \in (0, \epsilon]$ by Theorem 2.4(3).

3. (a) By item (1) within this theorem and monotone convergence, $\mathcal{Y}(x; \bar{a}, b) \searrow \mathcal{Y}^*$ for some $\mathcal{Y}^* \geq 0$ as $\bar{a} \nearrow \infty$. Assume $\mathcal{Y}^* > 0$, then

$$u(\bar{a}, b) = u(\bar{a} + x, b - \mathcal{Y}(x; \bar{a}, b)) \leq u(\bar{a} + x, b - \mathcal{Y}^*) \quad \forall \bar{a} > 0.$$

By quasiconcavity this inequality implies $xu_A(\bar{a}, b) \geq \mathcal{Y}^* u_B(\bar{a}, b)$ for every $\bar{a} > 0$; in particular, this implies $0 = x \lim_{\bar{a} \rightarrow \infty} u_A(\bar{a}, b) \geq \mathcal{Y}^* \lim_{\bar{a} \rightarrow \infty} u_B(\bar{a}, b) > 0$ which forms a contradiction due to (I+), i.e., $\mathcal{Y}^* = 0$.

(b) By item (1) within this theorem and monotone convergence, $\mathcal{Y}(x; a, \bar{b}) \nearrow \mathcal{Y}^*$ for some $\mathcal{Y}^* \leq \infty$ (possibly infinite) as $\bar{b} \nearrow \infty$. Assume $\mathcal{Y}^* < \infty$, then

$$u(a, \bar{b}) = u(a + x, \bar{b} - \mathcal{Y}(x; a, \bar{b})) \geq u(a + x, \bar{b} - \mathcal{Y}^*) \quad \forall \bar{b} > \mathcal{Y}^*.$$

By quasiconcavity this inequality implies $\mathcal{Y}^* u_B(a + x, \bar{b} - \mathcal{Y}^*) \geq x u_A(a + x, \bar{b} - \mathcal{Y}^*)$; in particular, this implies $0 = \mathcal{Y}^* \lim_{\bar{b} \rightarrow \infty} u_B(a + x, \bar{b} - \mathcal{Y}^*) \geq x \lim_{\bar{b} \rightarrow \infty} u_A(a + x, \bar{b} - \mathcal{Y}^*) > 0$ which forms a contradiction due to (I+), i.e., $\mathcal{Y}^* = \infty$.

□

B.3 Proof of Lemma 2.7

Proof. We will only prove the first (in)equality, the second follows comparably. Denote $\mathcal{Y} := \mathcal{Y}(x; a, b)$ and $\mathcal{X} := \mathcal{X}(\mathcal{Y}; a + x, b - \mathcal{Y})$. Then, by Theorem 2.4(1),

$$u(a + x - \mathcal{X}, b) = u(a + x - \mathcal{X}, b - \mathcal{Y} + \mathcal{Y}) \geq u(a + x, b - \mathcal{Y}) \geq u(a, b).$$

By (SM), this implies $a + x - \mathcal{X} \geq a$, i.e., $\mathcal{X} \leq x$. If, additionally, (UfB) then the inequalities above hold as equalities and the result follows comparably. □

B.4 Proof of Proposition 2.8

Proof. First, we will prove that P is differentiable. By explicitly providing the derivatives, monotonicity of the pricing oracle can be proven directly. With this result, we will prove surjectivity of P by demonstrating that $\lim_{\bar{a} \searrow 0} P(\bar{a}, b) = \infty$, $\lim_{\bar{b} \searrow 0} P(a, \bar{b}) = 0$, $\lim_{\bar{a} \nearrow \infty} P(\bar{a}, b) = 0$, and $\lim_{\bar{b} \nearrow \infty} P(a, \bar{b}) = \infty$ for any $a, b > 0$.

As mentioned above, we will prove differentiability and monotonicity by explicitly providing the partial derivatives of P :

$$\begin{aligned} \frac{\partial}{\partial a} P(a, b) &= \frac{u_B(a, b) u_{AA}(a, b) - u_A(a, b) u_{AB}(a, b)}{u_B(a, b)^2} \leq 0, \\ \frac{\partial}{\partial b} P(a, b) &= \frac{u_B(a, b) u_{AB}(a, b) - u_A(a, b) u_{BB}(a, b)}{u_B(a, b)^2} \geq 0, \end{aligned}$$

using (SC) and the fact that $P(a, b) = \mathcal{Y}'(0; a, b) = u_A(a, b)/u_B(a, b)$.

Consider now the limits:

- Consider $\lim_{\bar{a} \searrow 0} P(\bar{a}, b)$: By concavity of \mathcal{Y} , $P(a, b) = \mathcal{Y}'(0; a, b) \geq \frac{\mathcal{Y}(x; a, b)}{x}$ for any $x > 0$. Therefore, by Theorem 2.6(2), $\lim_{\bar{a} \searrow 0} P(\bar{a}, b) \geq \lim_{\bar{a} \searrow 0} \mathcal{Y}(x; \bar{a}, b)/x = b/x$ for any $x > 0$. As this inequality holds

for any $x > 0$, it must follow that $\lim_{\bar{a} \searrow 0} P(\bar{a}, b) = \infty$.

- Consider $\lim_{\bar{b} \searrow 0} P(a, \bar{b})$: Recall that $P(a, b) = \frac{1}{\mathcal{X}'(0; a, b)}$ by the provided assumptions. Therefore $\lim_{\bar{b} \searrow 0} P(a, \bar{b}) = 0$ if $\lim_{\bar{b} \searrow 0} \mathcal{X}'(0; a, \bar{b}) = \infty$. By symmetry of the assets, this is equivalent to $\lim_{\bar{a} \searrow 0} \mathcal{Y}'(0; \bar{a}, b) = \infty$ which is proven in the prior case.
- Consider $\lim_{\bar{a} \nearrow \infty} P(\bar{a}, b)$: As in the prior case, recall that $P(a, b) = \frac{1}{\mathcal{X}'(0; a, b)}$ by the provided assumptions. Therefore $\lim_{\bar{a} \nearrow \infty} P(\bar{a}, b) = 0$ if $\lim_{\bar{a} \nearrow \infty} \mathcal{X}'(0; \bar{a}, b) = \infty$. By symmetry of the assets, this is equivalent to $\lim_{\bar{b} \nearrow \infty} \mathcal{Y}'(0; a, \bar{b}) = \infty$ which is proven in the next case.
- Consider $\lim_{\bar{b} \nearrow \infty} P(a, \bar{b})$: As in the first case, by concavity of \mathcal{Y} , $P(a, b) = \mathcal{Y}'(0; a, b) \geq \frac{\mathcal{Y}(x; a, b)}{x}$ for any $x > 0$. Therefore, by Theorem 2.6(3), $\lim_{\bar{b} \nearrow \infty} P(a, \bar{b}) \geq \lim_{\bar{b} \nearrow \infty} \mathcal{Y}(x; a, \bar{b})/x = \infty$ for any $x > 0$.

Finally, the scale invariance of P follows directly from the positive homogeneity of \mathcal{Y} (see Theorem 2.4(9)). Specifically, let $t > 0$ then

$$P(ta, tb) = \lim_{\epsilon \searrow 0} \frac{\mathcal{Y}(\epsilon; ta, tb)}{\epsilon} = \lim_{\epsilon \searrow 0} \frac{\mathcal{Y}(t\epsilon; ta, tb)}{t\epsilon} = \lim_{\epsilon \searrow 0} \frac{t\mathcal{Y}(\epsilon; a, b)}{t\epsilon} = \lim_{\epsilon \searrow 0} \frac{\mathcal{Y}(\epsilon; a, b)}{\epsilon} = P(a, b).$$

□

B.5 Proof of Theorem 2.9

Proof. Fix $(a, b) \in \mathbb{R}_{++}^2$. Define $\beta : [-a, \infty) \rightarrow [-b, \infty)$ such that $P(a, b) = P(a + \delta, b + \beta(\delta))$ for any $\delta \in (-a, \infty)$ which is guaranteed to exist by the surjective property of the pricing oracle P as provided in Proposition 2.8 (and with $\beta(-a) = -b$). This proof could comparably be defined w.r.t. $\alpha : [-b, \infty) \rightarrow [-a, \infty)$ constructed as with β but on the first asset.⁴

Recall $P(\bar{a}, \bar{b}) := \mathcal{Y}'(0; \bar{a}, \bar{b}) = u_A(\bar{a}, \bar{b})/u_B(\bar{a}, \bar{b})$ for any reserves $(\bar{a}, \bar{b}) \in \mathbb{R}_{++}^2$. Therefore, by implicit differentiation,

$$\beta'(\delta) = -\frac{P_A(\hat{a}, \hat{b})}{P_B(\hat{a}, \hat{b})},$$

where $(\hat{a}, \hat{b}) := (a + \delta, b + \beta(\delta))$ for any $\delta \in (-a, \infty)$.

We will prove this result only in the case of \mathcal{Y} ; the monotonicity of \mathcal{X} follows similarly. For shorthand, define $\bar{\mathcal{Y}}(\delta) := \mathcal{Y}(x; a + \delta, b + \beta(\delta))$ for fixed $x > 0$. Then $u(a + \delta + x, b + \beta(\delta) - \bar{\mathcal{Y}}(\delta)) = u(a + \delta, b + \beta(\delta))$ by

⁴Though (I+) was assumed for Theorem 2.9, it is not necessary for that result. Specifically, (I+) is only used to guarantee the existence of $\beta(\delta)$ for any $\delta \in [-a, \infty)$ through the surjectivity of $b \mapsto P(a, b)$ as provided in Proposition 2.8. However, if $\beta(\delta)$ does not exist, then pooling would need to be done primarily in A instead using the, similarly defined, function $\alpha : [-b, \infty) \rightarrow [-a, \infty)$. (At least one of α or β can be appropriately defined as, from the proof of Proposition 2.8, $\lim_{\bar{a} \searrow 0} P(\bar{a}, b) = \infty$ and $\lim_{\bar{b} \searrow 0} P(a, \bar{b}) = 0$ for any $a, b > 0$ *without* requiring (I+).)

construction. Using the same construction of $(\hat{a}, \hat{b}) := (a + \delta, b + \beta(\delta))$ as above, by implicit differentiation

$$\bar{\mathcal{Y}}'(\delta) = \frac{\left[u_A(\hat{a} + x, \hat{b} - \bar{\mathcal{Y}}(\delta)) + \beta'(\delta) u_B(\hat{a} + x, \hat{b} - \bar{\mathcal{Y}}(\delta)) \right] - \left[u_A(\hat{a}, \hat{b}) + \beta'(\delta) u_B(\hat{a}, \hat{b}) \right]}{u_B(\hat{a} + x, \hat{b} - \bar{\mathcal{Y}}(\delta))}.$$

Therefore $\bar{\mathcal{Y}}'(\delta) \geq 0$ if

$$\underbrace{\frac{\partial}{\partial x} \left[u_A(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b})) + \beta'(\delta) u_B(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b})) \right]}_{(*)} \geq 0.$$

Explicitly computing the derivative $(*)$, we recover the equivalent condition:

$$\beta'(\delta) = -\frac{P_A(\hat{a}, \hat{b})}{P_B(\hat{a}, \hat{b})} \geq -\frac{P_A(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b}))}{P_B(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b}))}.$$

In particular, this holds if

$$\underbrace{\frac{\partial}{\partial x} \left(\frac{P_A(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b}))}{P_B(\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b}))} \right)}_{(**)} \geq 0.$$

Explicitly computing the derivative $(**)$, we recover the desired monotonicity:

$$(**) := \frac{P_B(\hat{z})P_{AA}(\hat{z}) - [P(\hat{z})P_B(\hat{z}) + P_A(\hat{z})]P_{AB}(\hat{z}) + P(\hat{z})P_A(\hat{z})P_{BB}(\hat{z})}{P_B(\hat{z})^2} \geq 0$$

by assumption where $\hat{z} := (\hat{a} + x, \hat{b} - \mathcal{Y}(x; \hat{a}, \hat{b}))$. □

B.6 Proof of Lemma 4.3

Proof. We will prove the result for \mathcal{Y}_γ only, the proof for \mathcal{X}_γ follows comparably. Consider the ODE representation (4.3) and note the domain $\text{dom } g := \mathbb{R}_+ \times [0, b)$. By Proposition 2.8, g and $\frac{\partial}{\partial x}g, \frac{\partial}{\partial y}g$ are continuous, and thus bounded, on this domain. Therefore, by the Picard-Lindelöf Theorem and extension theorem (e.g., [17, Theorem II.1.1 and Theorem II.3.1]), there exists a unique solution $\mathcal{Y}_\gamma(x)$ on some maximal domain $x \in [0, x^*)$ for some $x^* > 0$. Furthermore, by the extension theorem, if $x^* < \infty$ then $\lim_{x \rightarrow x^*} \mathcal{Y}_\gamma(x) \in \{0, b\}$. Trivially, $\mathcal{Y}_\gamma(x) > 0$ for $x > 0$ by $g(x, y) > 0$ for any $y \in [0, b)$. Assume now that $x^* < \infty$ and $\lim_{x \rightarrow x^*} \mathcal{Y}_\gamma(x) = b$. To complete this proof, we will demonstrate that $\mathcal{Y}_\gamma(x) \leq \mathcal{Y}(x)$ for any $x \in [0, x^*)$, from which it will follow that $\lim_{x \rightarrow x^*} \mathcal{Y}_\gamma(x) \leq \lim_{x \rightarrow x^*} \mathcal{Y}(x) = \mathcal{Y}(x^*) < b$ (by Theorem 2.4(3)) to reach a contradiction. To show that $\mathcal{Y}_\gamma(x) \leq \mathcal{Y}(x)$ for any $x \in [0, x^*)$, assume by contradiction that this inequality is false and take $x^\dagger := \inf\{x \in [0, x^*) \mid \mathcal{Y}_\gamma(x) > \mathcal{Y}(x)\} < x^*$. Note that $\mathcal{Y}_\gamma(x^\dagger) = \mathcal{Y}(x^\dagger)$ by a simple continuity argument, and $\mathcal{Y}_\gamma(x^\dagger + \epsilon) > \mathcal{Y}(x^\dagger + \epsilon)$ for every $\epsilon \in (0, \delta)$ for some $\delta > 0$. However, this

implies $\mathcal{Y}'_\gamma(x^\dagger) = (1 - \gamma)g(x^\dagger, \mathcal{Y}_\gamma(x^\dagger)) \leq g(x^\dagger, \mathcal{Y}(x^\dagger)) = \mathcal{Y}'(x^\dagger)$ which results in a simple contradiction. \square

B.7 Proof of Proposition 4.5

Proof. As in prior proofs, we will provide the proof of this result for \mathcal{Y}_γ only as the proof for \mathcal{X}_γ follows comparably. First, we wish to note that the non-strict monotonicity encoded in (4.4) follows as a simple application of [17, Theorem III.4.1]. We now wish to prove the strict monotonicity of (4.4). Consider the ODE satisfied by $\frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma(x; a, b)$, i.e.,

$$\frac{\partial}{\partial \gamma} \mathcal{Y}'_\gamma(x; a, b) = -P(a + x, b - \mathcal{Y}_\gamma(x; a, b)) - (1 - \gamma) \frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma(x; a, b) P_B(a + x, b - \mathcal{Y}_\gamma(x; a, b)) \quad (\text{B.1})$$

where, by (SC), we have that $\frac{\partial}{\partial \gamma} \mathcal{Y}'_\gamma = \left(\frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma \right)'$. Furthermore, note that we can view $P(a + x, b - \mathcal{Y}_\gamma(x; a, b))$ and $P_B(a + x, b - \mathcal{Y}_\gamma(x; a, b))$ as functions of x (with fixed reserves $a, b > 0$). Therefore, together with the initial condition $\frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma(0; a, b) = 0$, we can explicitly solve (B.1) for $\frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma(x; a, b)$, i.e., for any $x \geq 0$

$$\frac{\partial}{\partial \gamma} \mathcal{Y}_\gamma(x; a, b) = - \int_0^x e^{-(1-\gamma) \int_t^x P_B(a+u, b-\mathcal{Y}_\gamma(u; a, b)) du} P(a+t, b-\mathcal{Y}_\gamma(t; a, b)) dt.$$

As this is strictly negative for any $x > 0$, (4.4) follows. \square

B.8 Proof of Corollary 4.6

- Proof.*
1. Let $x > 0$ as the case of equality when $x = 0$ is trivial. By Theorem 2.4(2) and Proposition 4.5, and recalling from Remark 11 that $\mathcal{Y}_0 \equiv \mathcal{Y}$, $u(a + x, b - \mathcal{Y}_\gamma(x)) > u(a + x, b - \mathcal{Y}(x)) = u(a, b)$.
 2. (a) Strict monotonicity of \mathcal{Y}_γ in x follows trivially from its integral representation as the pricing oracle is strictly positive on positive pool sizes.
 - (b) By implicit differentiation of (4.3) and the monotonicity of the pricing oracle as provided in Proposition 2.8, $\mathcal{Y}''_\gamma(x) = (1 - \gamma)[P_A(a + x, b - \mathcal{Y}_\gamma(x)) - (1 - \gamma)P(a + x, b - \mathcal{Y}_\gamma(x))P_B(a + x, b - \mathcal{Y}_\gamma(x))] \leq 0$.
 - (c) Subadditivity follows from concavity and $\mathcal{Y}_\gamma(0) = 0$ as demonstrated in the proof of Theorem 2.4(10).
 3. Note that $c_B(b) := \sup_{\bar{a} > 0} u_B(\bar{a}, b) < \infty$ for every $b > 0$, because u_B is continuous with limiting behavior $\lim_{\bar{a} \rightarrow 0} u_B(\bar{a}, b), \lim_{\bar{a} \rightarrow \infty} u_B(\bar{a}, b) < \infty$. Assume by contradiction that $\lim_{x \rightarrow \infty} \mathcal{Y}_\gamma(x) = \mathcal{Y}_\gamma^* < b$. Recall \mathcal{Y}_γ is strictly monotonic, therefore $\mathcal{Y}_\gamma(x) < \mathcal{Y}_\gamma^*$ for every x . Therefore,

$$\lim_{x \rightarrow \infty} \mathcal{Y}_\gamma(x) = \lim_{x \rightarrow \infty} (1 - \gamma) \int_0^x P(a + y, b - \mathcal{Y}_\gamma(y)) dy \geq (1 - \gamma) \int_0^\infty P(a + y, b - \mathcal{Y}_\gamma^*) dy$$

$$\begin{aligned}
&= (1 - \gamma) \int_0^\infty \frac{u_A(a + y, b - \mathcal{Y}_\gamma^*)}{u_B(a + y, b - \mathcal{Y}_\gamma^*)} dy \geq \frac{(1 - \gamma) \int_0^\infty u_A(a + y, b - \mathcal{Y}_\gamma^*) dy}{c_B(b - \mathcal{Y}_\gamma^*)} \\
&= \frac{1 - \gamma}{c_B(b - \mathcal{Y}_\gamma^*)} \left(\lim_{x \rightarrow \infty} u(a + x, b - \mathcal{Y}_\gamma^*) - u(a, b - \mathcal{Y}_\gamma^*) \right) = \infty.
\end{aligned}$$

4. Let $t > 0$. From (4.3) it follows that

$$\frac{\partial}{\partial x} \frac{1}{t} \mathcal{Y}_\gamma(tx; ta, tb) = (1 - \gamma)P(ta + tx, tb - \mathcal{Y}_\gamma(tx; ta, tb)) = (1 - \gamma)P(a + x, b - \frac{1}{t} \mathcal{Y}_\gamma(tx; ta, tb)).$$

Since for $x = 0$, we have that both $\frac{1}{t} \mathcal{Y}_\gamma(0; ta, tb) = 0 = \mathcal{Y}_\gamma(0; a, b)$, we can appeal to the existence and uniqueness result of Lemma 4.3 to recover $\frac{1}{t} \mathcal{Y}_\gamma(tx; ta, tb) = \mathcal{Y}_\gamma(x; a, b)$, i.e., positive homogeneity.

5. From (4.3) it follows that

$$\mathcal{Y}'_\gamma(x_1 + x_2; a, b) = (1 - \gamma)P(a + x_1 + x_2, b - \mathcal{Y}_\gamma(x_1; a, b) - [\mathcal{Y}_\gamma(x_1 + x_2; a, b) - \mathcal{Y}_\gamma(x_1; a, b)]) \quad (\text{B.2})$$

Note also that

$$\mathcal{Y}'_\gamma(x_1 + x_2; a, b) = \frac{\partial}{\partial x_2} [\mathcal{Y}_\gamma(x_1 + x_2; a, b) - \mathcal{Y}_\gamma(x_1; a, b)]. \quad (\text{B.3})$$

Combining (B.2) and (B.3), it follows that

$$\begin{aligned}
&\frac{\partial}{\partial x_2} [\mathcal{Y}_\gamma(x_1 + x_2; a, b) - \mathcal{Y}_\gamma(x_1; a, b)] \\
&= (1 - \gamma)P(a + x_1 + x_2, b - \mathcal{Y}_\gamma(x_1; a, b) - [\mathcal{Y}_\gamma(x_1 + x_2; a, b) - \mathcal{Y}_\gamma(x_1; a, b)]).
\end{aligned}$$

We also have, by construction of (4.3), that

$$\begin{aligned}
&\mathcal{Y}'_\gamma(x_2; a + x_1, b - \mathcal{Y}_\gamma(x_1; a, b)) \\
&= (1 - \gamma)P(a + x_1 + x_2, b - \mathcal{Y}_\gamma(x_1; a, b) - \mathcal{Y}_\gamma(x_2; a + x_1, b - \mathcal{Y}_\gamma(x_1; a, b)))
\end{aligned}$$

Since for $x_2 = 0$, we have that both $\mathcal{Y}_\gamma(x_1 + x_2) - \mathcal{Y}_\gamma(x_1) = 0 = \mathcal{Y}_\gamma(x_2; a + x_1, b - \mathcal{Y}_\gamma(x_1; a, b))$, we can appeal to the existence and uniqueness result of Lemma 4.3 to conclude

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

for any $x_1, x_2 \geq 0$.

□

B.9 Proof of Corollary 4.7

Proof. We will only prove the first inequality, the second follows similarly. By Theorem 2.4(5), Theorem 2.6(1), and Proposition 4.5,

$$\begin{aligned}\mathcal{X}_\gamma(\mathcal{Y}_\gamma(x; a, b); a + x, b - \mathcal{Y}_\gamma(x; a, b)) &< \mathcal{X}(\mathcal{Y}_\gamma(x; a, b); a + x, b - \mathcal{Y}_\gamma(x; a, b)) \\ &\leq \mathcal{X}(\mathcal{Y}_\gamma(x; a, b); a + x, b - \mathcal{Y}(x; a, b)) \\ &< \mathcal{X}(\mathcal{Y}(x; a, b); a + x, b - \mathcal{Y}(x; a, b)) = x.\end{aligned}$$

□

B.10 Proof of Corollary 4.8

Proof. We will prove this result for $\frac{\partial}{\partial a}\mathcal{Y}_\gamma(x; a, b) \leq 0$ only; the proof for $\frac{\partial}{\partial b}\mathcal{Y}_\gamma(x; a, b) \in (0, 1]$ follows similarly. Following the same strategy as in the proof of Proposition 4.5, we can construct the ODE

$$\frac{\partial}{\partial a}\mathcal{Y}'_\gamma(x; a, b) = (1 - \gamma)[P_A(a + x, b - \mathcal{Y}_\gamma(x; a, b)) - \frac{\partial}{\partial a}\mathcal{Y}_\gamma(x; a, b)P_B(a + x, b - \mathcal{Y}_\gamma(x; a, b))]$$

with initial condition $\frac{\partial}{\partial a}\mathcal{Y}_\gamma(0; a, b) = 0$ for every $a, b > 0$. By solving this ODE, we recover

$$\frac{\partial}{\partial a}\mathcal{Y}_\gamma(x; a, b) = (1 - \gamma) \int_0^x e^{-(1-\gamma) \int_t^x P_B(a+u, b-\mathcal{Y}_\gamma(u; a, b)) du} P_A(a+t, b-\mathcal{Y}_\gamma(t; a, b)) dt, \quad \forall x \geq 0.$$

From Proposition 2.8 it now follows that $\frac{\partial}{\partial a}\mathcal{Y}_\gamma(x; a, b) \leq 0$. □

B.11 Proof of Lemma 4.10

Proof. We will prove these results for $p < P(a, b)$ only; the case for $p > P(a, b)$ follows similarly. To simplify notation, let $\mathcal{Y}_\gamma(p) := \mathcal{Y}_\gamma(x_p; (1+\delta)a, (1+\delta)b)$. Furthermore, recall that $p = P((1+\delta)a + x_p, (1+\delta)b - \mathcal{Y}_\gamma(p)) = \frac{1}{1-\gamma}\mathcal{Y}'_\gamma(x_p; (1+\delta)a, (1+\delta)b)$. First, we wish to demonstrate that we recover the simplified version of the divergence loss:

$$\begin{aligned}\Delta(p) &= \delta[pa + b] - \frac{\delta}{1+\delta} [p((1+\delta)a + x_p) + ((1+\delta)b - \mathcal{Y}_\gamma(p))] \\ &= \frac{\delta}{1+\delta} [(1+\delta)(pa + b) - p((1+\delta)a + x_p) - ((1+\delta)b - \mathcal{Y}_\gamma(p))] \\ &= \frac{\delta}{1+\delta} [\mathcal{Y}_\gamma(p) - px_p].\end{aligned}$$

Therefore the sign of the divergence loss $\Delta(p)$ is completely characterized by the sign of $\mathcal{Y}_\gamma(p) - px_p$. As there is a one-to-one relation between Δ and $\bar{\Delta}$, we will consider the question of the sign of $\mathcal{Y}_\gamma(x; (1+\delta)a, (1+\delta)b) - P((1+\delta)a+x, (1+\delta)b - \mathcal{Y}_\gamma(x; (1+\delta)a, (1+\delta)b))x$ as $x \geq 0$ varies (corresponding to $p \leq P(a, b)$). To simplify notation, as before we will drop the arguments of these functions where the meaning is clear. Note that $[\mathcal{Y}_\gamma - Px]_{x=0} = 0$ by construction and $\frac{\partial}{\partial x}[\mathcal{Y}_\gamma - Px] = -\gamma P + x((1-\gamma)PP_B - P_A)$. Recall from Proposition 2.8 that $P_A \leq 0$ and $P_B \geq 0$. Therefore, at $\gamma = 0$, $\mathcal{Y}_\gamma - Px \geq 0$ for any $x > 0$ with equality if and only if $P((1+\delta)a+x, (1+\delta)b - \mathcal{Y}_\gamma(x; (1+\delta)a, (1+\delta)b)) = P(a, b)$, i.e., where $p = P(a, b)$. If $\gamma \in (0, 1)$ then, for x small enough, $\frac{\partial}{\partial x}[\mathcal{Y}_\gamma - Px] < 0$; thus there exists some $x_* \in (0, \infty]$ such that $\mathcal{Y}_\gamma - Px < 0$ for every $x \in (0, x_*)$ and $[\mathcal{Y}_\gamma - Px]_{x=x_*} = 0$. By the relation between x and p , we can define $p_* := P((1+\delta)a+x_*, (1+\delta)b - \mathcal{Y}_\gamma(x_*; (1+\delta)a, (1+\delta)b))$. \square