

Improved Price Oracles: Constant Function Market Makers

Guillermo Angeris
angeris@stanford.edu

Tarun Chitra
tarun@gauntlet.network

June 2020

Abstract

Automated market makers, first popularized by Hanson’s logarithmic market scoring rule (or LMSR) for prediction markets, have become important building blocks, called ‘primitives,’ for decentralized finance. A particularly useful primitive is the ability to measure the price of an asset, a problem often known as the pricing oracle problem. In this paper, we focus on the analysis of a very large class of automated market makers, called constant function market makers (or CFMMs) which includes existing popular market makers such as Uniswap, Balancer, and Curve, whose yearly transaction volume totals to billions of dollars. We give sufficient conditions such that, under fairly general assumptions, agents who interact with these constant function market makers are incentivized to correctly report the price of an asset and that they can do so in a computationally efficient way. We also derive several other useful properties that were previously not known. These include lower bounds on the total value of assets held by CFMMs and lower bounds guaranteeing that no agent can, by any set of trades, drain the reserves of assets held by a given CFMM.

1 Introduction

As natively digital assets continue to grow, there is an increasing need for mechanisms of exchange similar to those found in traditional financial markets. These digital assets, which include online ad impressions, cryptocurrencies, and prediction market bets, are often complex to interact with and suffer from low liquidity [1]. Over the last decade, a number of designs for automated market makers (AMMs) have been proposed to reduce this complexity. AMMs encourage passive market participants with low time preference to lend their digital assets to asset pools. The assets are then priced via a *scoring rule* which maps the current pool sizes to a marginal price. One of the most popular scoring rules is Hanson’s *logarithmic market scoring rule* (LMSR) [2]. This rule has been implemented in numerous online settings including online ad auctions [3], prediction markets [4, 5], and instructor rating markets [6].

Recently, the cryptocurrency community has constructed alternative automated market makers to the LMSR (and its counterparts), which we call the *constant function market makers* (CFMMs). Examples of CFMMs include Uniswap’s constant product AMM [7] and the constant mean AMM [8], among others [9]. Most applications of CFMMs have been to construct decentralized exchanges, which allow for the exchange of security-like assets without the need for a trusted third-party. One main concern for users of these markets is whether prices on decentralized exchanges accurately follow those on centralized exchanges, which currently have more liquidity. If the price of a decentralized exchange prices matches external prices, then such an exchange is said to be a good *price oracle* that other smart contracts can query as a source of ground truth.

The oracle problem. One of the main difficulties in decentralized systems is the ability to query data external to the smart contract. For example, a prediction market betting on the future weather in Seattle would need to know the resulting weather report, once the event has happened. Doing this in a trustless manner is difficult, as participants who have a losing bet are encouraged to try to dupe the smart contract, *i.e.*, to manipulate the response of the contract’s query. In our previous example, if the prediction market bets on the question “will the weather in Seattle be greater than 25°C?” then a malicious participant with an active bet on “no” is incentivized to manipulate the query response to say that the temperature is less than 25°C. In the cryptocurrency community, the problem of providing external data to a blockchain is known as the *oracle problem*, as an homage to oracles queried in theoretical computer science [10].

Decentralized oracles. Formally, an *oracle* refers to any computational device that provides the smart contract data external to the underlying blockchain [11]. There are two types of oracles in smart contract prediction markets: centralized and decentralized. Centralized oracles involve a trusted individual or organization that provides data to the smart contract. Examples of centralized oracles include Provable/Oraclize [12, 13], Wolfram Alpha [14], and the MakerDAO oracle [15]. If these oracles are used to decide on LMSR prediction market events, they still rely on participants trusting that the centralized authority will not manipulate the data determining the final outcome of the market. For highly valuable markets, such as the prediction of the US presidential election, it is usually untenable to trust a single individual or organization and one defers to *decentralized oracles*.

Decentralized oracles are smart contracts that rely on users voting on particular prediction market outcomes. A final outcome is chosen via a social choice function [16], similar to how majority or weighted majority voting is used to decide outcomes in elections. In the case of smart contracts, the social choice function is usually significantly more complicated as the voting mechanism needs to account for adverse selection, bribery, and collusion amongst voters. In order to reduce the likelihood of such *oracle manipulation*, decentralized oracle designs often have exit games and/or complicated multiparty games that allow for certain users to challenge votes that they dispute. Moreover, to encourage a large swath of potential users to participate in a vote, prediction market smart contracts usually provide users with

a reward. This reward is disbursed in a manner similar to how cryptocurrency rewards are given to miners and/or validators [17]. These oracles are difficult to design as one has to balance mechanism complexity with provable defenses against collusion between prediction market participants. Examples of decentralized oracles include Augur, Astraea [18], Gnosis, and UMA [19]. We note that a stated design goal of Augur is for the prices implied by the LMSR to be used as an oracle input into other smart contracts. For instance, if another smart contract relies on the probability of whether Seattle’s temperature is greater or less than 25°C, then that contract simply has to subscribe to the data and pricing provided by an Augur market. In this way, prediction market smart contracts aim to serve as the single source of off-chain data that is accessible to an arbitrarily large number of on-chain smart contracts.

Decentralized exchanges. Decentralized exchanges (DEXs) provide a method for participants to trade pairs of on-chain assets without ever needing to trust a centralized authority [20, 21], while additionally providing a means for measuring the relative price of this pair of assets. (For example, one simple but effective way in which these exchanges can provide a price would be to report the price at which the last trade was executed.) t Currently, there are roughly \$100 million of digital assets locked in DEXs with trading volume often surpassing \$10 million per day [22, 23]. A design for a secure decentralized exchange for cryptocurrencies has been desired almost since the advent of Bitcoin, since centralized exchanges such as Mt. Gox [24], Quadriga [25], and Bitfinex [26] have had catastrophic losses that aggregate to billions of dollars of depositors’ funds.

Many decentralized exchanges have been proposed, each with specific trading and pricing mechanisms. These range from classic order book mechanisms [20] to other, more complicated cases [27]. Yet, Uniswap [7, 28, 29], an AMM whose pricing mechanism for comparing two assets is relatively simple in both theory and practice, has become an extraordinarily popular decentralized exchange, as measured by total trading volumes and total funds in their reserves [23]. This has led other protocols such as Celo [30] to use the Uniswap mechanism as a price oracle.

Generalizations of Uniswap. The success of Uniswap, which required far fewer resources to develop than competing decentralized exchanges¹ has led to a number of generalizations. A natural first question is whether the Uniswap constant product formula is optimal for all types of assets. For instance, a pair of assets which have a common mean price but different volatilities can incur large losses for the corresponding market makers and liquidity providers at specific instances in time.

¹Uniswap was created with a \$100,000 grant from the Ethereum Foundation [28], whereas 0x [31] and Bancor raised \$24 million and \$153 million in Initial Coin Offerings, respectively. On-chain data provider Dune Analytics reports that Uniswap had \$370,703,652 of volume in 2019, whereas 0x had \$228,271,968 of volume and Bancor had \$154,427,142 of volume [32, 33]. Note that naïvely comparing liquidity (as opposed to volume) is more involved, as 0x currently routes orders to Uniswap and a number of aggregators exist that partition orders between different exchanges [34]

An example of such assets are *stablecoins*, which are digital assets whose value is (approximately) pegged to be equal to \$1. The price of these assets naturally fluctuate around \$1 USD, but tend to stay within a bounded range of $[1 - \epsilon, 1 + \epsilon]$ for some $\epsilon > 0$. The fluctuations of these assets is dictated by their natural sources of demand and can vary greatly, even though these digital assets are all meant to represent the same real world asset. For instance, a stablecoin that is popular in Venezuela will likely have different demand characteristics than one that is popular in China. In order to incentivize traders, the trading mechanism should instead charge lower fees when two stablecoins are near \$1 USD and higher fees when the stablecoins are farther from \$1 USD. This approach has been implemented in Curve (previously known as StableSwap) [9], which ensures that the trading prices around \$1 USD are relatively small, but quickly becomes expensive as coins trade away from one another.

Multi-coin generalizations. Another generalization of the Uniswap mechanism involves pricing multiple assets simultaneously. Instead of providing a scoring rule that is a function of the quantities of two assets, these scoring rules take are able to price m assets in terms of a set of n other assets. This allows for users to exchange portfolios of assets for other portfolios, reducing the number of transactions that the network has to handle. On an exchange that only allows for pairwise trades, a participant would need to do m trades to a numéraire asset (*e.g.*, Bitcoin or USD) and then n trades from the numéraire to the output assets. Multi-asset generalizations of Uniswap, such as Balancer [8], would execute such a trade atomically, reducing fees and price slippage. The choice of scoring rule affects how easy it is for arbitrageurs to keep the portfolio prices synchronized with the prices of the underlying components.

While this mechanism might seem arbitrary, there are a number of examples of similar assets from traditional finance that involve trading baskets of good for other baskets of goods. For instance, an Exchange Traded Fund (ETF) is a single equity instrument S_E that represents a weighted set of shares S_1, \dots, S_n . There are currently over \$5 trillion of assets locked in ETFs [35]. Many ETFs represent a share of S_E by a weighted linear combination of the shares, $S_E = \sum_{i=1}^n w_i S_i$ for some positive integer weights w_i . If any of the prices of shares S_i change, leaving S_E mispriced, an arbitrageur can perform creation-redemption arbitrage [36]. This arbitrage works due to two steps:

- Creation: A market participant can create a single share S_E by providing the ETF underwriter with w_i shares of S_i for all i
- Redemption: A market participant can redeem a single share S_E by giving the ETF underwriter S_E and receiving $\{w_i S_i : i \in [n]\}$.

If the price of S_E is higher than the weighted sum of the prices of S_i , then an arbitrageur can buy the basket $\{w_i S_i : i \in [n]\}$ for less than $\text{price}(S_E)$, create a share of S_E and sell it for a profit of $\text{price}(S_E) - \sum_{i=1}^n w_i \cdot \text{price}(S_i)$. Similarly, the arbitrageur can use a redemption to arbitrage a low S_E price. Multi-asset generalizations of Uniswap allow for precisely this type of arbitrage to occur without the need for a trusted intermediary (*e.g.*, the ETF underwriter).

Summary. In this paper, we show that many of the generalizations presented are special cases of a large family of *constant function market makers*, or CFMMs, which all satisfy relatively similar and useful theoretical properties, under mild conditions.

In particular, in §2, we provide a complete and very general framework for analyzing CFMMs that includes all major examples currently used in practice, by introducing a special object of study: the trading set (§2.1). We show that all major CFMMs in practice satisfy an additional convexity property (§2.2), which lets us show several interesting properties and often implies that many of the optimization problems presented in this paper can be efficiently solved. We also provide sufficient conditions for these CFMMs to be well-behaved, in the sense that (a) agents can never drain the assets that a CFMM contains by only trading with the given CFMM (§2.3), and (b) agents are incentivized to have the CFMM correctly report the price of its assets, when compared to a reference market (§2.4). We then give some simple derivations of a few properties of interest, including the total asset value that a given CFMM holds, as a function of the external market prices (§2.5). Finally, we provide some simple extensions of the current analysis and possible future directions for a more general analysis in §3.

2 Constant function market makers

In this section, we will discuss the basic definitions of constant function market makers and how Uniswap, among other CFMMs, fit directly into the provided framework.

Definition of a CFMM. A *constant function market maker*, or CFMM, is a type of automated market maker defined by its *trading function*, $\varphi : \mathbf{R}_+^n \times \mathbf{R}_+^n \times \mathbf{R}_+^n \rightarrow \mathbf{R}$, and its *reserves*, $R \in \mathbf{R}_+^n$. Here, R_i specifies how much of coin i the CFMM is allowed to use or interact with, while the trading function specifies what constitutes a valid trade.

In all of the applications we will see, a decentralized smart contract will implement a given CFMM. In this scenario, the CFMM will have some balance of various tokens available to it (with the i th entry of the reserves vector R specifying the amount of token i that is available), and agents can interact with this CFMM in various ways.

Agents and actions. In one case, a *liquidity provider* provides some number of funds to the reserves of the contract. In return, the liquidity provider is given a form of IOU (usually in the form of other tokens) which can be later redeemed for some fixed percentage of the reserve amounts.

In contrast, a *trader* attempts to exchange some given amount of coins in reserves. For example, a trader may simply want to trade some amount of coin i for coin j , in which case the trader would deposit some amount of coin i into the reserves of the contract and withdraw some amount of coin j from these reserves.

The trading function. More generally, a trader may wish to trade any number of coins for any other coins in potentially very complicated ways. To specify this, we will write the

output trade, $\Lambda \in \mathbf{R}_+^n$, as a vector with n nonnegative entries. (We will often simply call this the *output*.) The output's i th entry, Λ_i , specifies how much of coin i the trader wishes to receive from the CFMM. Additionally, we will define the *input* $\Delta \in \mathbf{R}_+^n$, which is a vector whose i th entry, Δ_i specifies how much of coin i the trader has given the contract. We will call the resulting tuple, $(\Delta, \Lambda) \in \mathbf{R}_+^n \times \mathbf{R}_+^n$, a *trade*.

The trading function φ then specifies exactly when a trade is considered valid and therefore executed. In particular, the smart contract with reserves R only accepts the trade given by (Δ, Λ) whenever (Δ, Λ) satisfies

$$\varphi(R, \Delta, \Lambda) = \varphi(R, 0, 0). \quad (1)$$

In other words, the trade is accepted only if the trading function is kept constant. The contract then places the coins Δ provided by the trader into its reserves while paying out Λ to the trader. This results in the reserves being updated in the following way:

$$R \leftarrow R + \Delta - \Lambda,$$

after a valid trade is executed.

Examples. Throughout the remainder of this paper, we will use constant product markets (Uniswap) and constant mean markets (Balancer) as mathematically simple but very practical and useful instances of CFMMs and as the canonical examples for the definitions and derivations provided.

In the case of constant product markets with percentage fee $(1 - \gamma)$ (see, *e.g.*, [29, §2]), we have $n = 2$ and the trading function is:

$$\varphi(R, \Delta, \Lambda) = (R_1 + \gamma\Delta_1 - \Lambda_1)(R_2 + \gamma\Delta_2 - \Lambda_2). \quad (2)$$

Of course, no rational trader will ever opt to make both $\Delta_1 \neq 0$ and $\Lambda_1 \neq 0$ in the case of nonzero fees; *i.e.*, a rational trader will never trade a specific coin for a smaller amount of the same coin. The same is true for the pair Δ_2 and Λ_2 . This results in the more recognizable form:

$$\varphi(R, \Delta, \Lambda) = \begin{cases} (R_1 + \gamma\Delta_1)(R_2 - \Lambda_2) & \Delta_2 = \Lambda_1 = 0 \\ (R_1 - \Lambda_1)(R_2 + \gamma\Delta_2) & \Delta_1 = \Lambda_2 = 0 \\ \varphi(R, 0, 0) + \varepsilon & \text{otherwise.} \end{cases}$$

(One can make a similar argument in the fee-less case with $\gamma = 1$.) Here, $\varepsilon \neq 0$ can be any nonzero value, as it should simply prevent any trade which has both Λ_1 and Δ_1 nonzero or Λ_2 and Δ_2 nonzero, such that (1) cannot be satisfied in either of these cases. Throughout the rest of this paper, we will work with the form given by (2), since the construction is easier to handle mathematically, but both forms are easily seen to be equivalent in the sense described in §2.1

The CFMM for constant mean markets, originally proposed by Balancer [8] for n coins is (*cf.*, [29, §3]):

$$\varphi(R, \Delta, \Lambda) = \prod_{i=1}^n (R_i + \gamma\Delta_i - \Lambda_i)^{w_i}. \quad (3)$$

Here, $0 < \gamma \leq 1$ and the weights $w \in \mathbf{R}_+^n$ are nonnegative and satisfy $\mathbf{1}^T w = 1$. As before, no rational trader will have $\Delta_i \neq 0$ and $\Lambda_i \neq 0$ if $\gamma < 1$, and we can always take at least one of these to be zero for any trade, even when $\gamma = 1$.

2.1 The trading set and implications

There are potentially many trading functions φ which are all ‘equivalent’ in some sense or another. One example is to compare the functions φ and $-\varphi$. Clearly, any trade which is feasible in one CFMM is feasible in the other, yet the functions are not equal except when both take on the value 0.

One way of (intuitively) solving this problem is to introduce a set which contains all possible achievable trades at some reserves R ; *i.e.*, all possible pairs of inputs Δ and outputs Λ which can be accepted as valid by the CFMM. This lets us work with the feasible trades without dealing with the specifics of the function φ . On the other hand, because our definition of a CFMM is so general, the function φ could also potentially allow many other trades which a rational agent would never perform. One basic example, when $n = 1$, is that at fixed reserves R , for some fixed input Δ , we could have two feasible trades whose outputs satisfy $\Lambda_1 > \Lambda_2$. In this case, a rational trader would never opt to receive strictly less coin and so would always take Λ_1 instead of Λ_2 , even though both trades are feasible. Under the ‘simple’ definition, then, a CFMM that only allows the first trade (Δ, Λ_1) would have a different set than one which allows both trades, (Δ, Λ_1) and (Δ, Λ_2) , even though no rational agent would ever opt for the latter trade (Δ, Λ_2) .

The trading set. To fix this issue, we introduce the *trading set* $T(R) \subseteq \mathbf{R}_+^n \times \mathbf{R}_+^n$ at reserves R , defined as

$$T(R) = \{(\Delta, \Lambda) \mid \varphi(R, \Delta', \Lambda') = \varphi(R, 0, 0) \text{ for some } \Delta' \leq \Delta, \Lambda' \geq \Lambda\}, \quad (4)$$

where the inequalities are all taken elementwise. Another way of stating this definition is the following: the trade $(\Delta, \Lambda) \in T(R)$ is in the trading set only when there exists a (potentially) cheaper alternative $\Delta' \leq \Delta$, or one with (potentially) higher payoff, $\Lambda' \geq \Lambda$.

The general idea is that no rational agent will ever pick a trade $(\Delta, \Lambda) \in T(R)$ whenever there exists a better trade (Δ', Λ') satisfying $\Delta' \leq \Delta$ and $\Lambda' \geq \Lambda$ with at least one of the elementwise inequalities holding strictly. We also note that this definition of a trading set is similar, though not quite equivalent, to the idea of an epigraph in optimization theory [37, §3.1.7].

The trading set contains all of the important information provided by the trading function φ , for a given CFMM. Because of this, we will often opt to work with the trading set instead of the function φ directly, as working with the set is generally mathematically simpler and more elegant. In many (but not all) cases, the statements for the trading set can easily be translated to statements over the function φ . When this is the case, we will write both statements directly.

Feasibility and equivalence. We will say some trade (Δ, Λ) is *feasible* if $(\Delta, \Lambda) \in T(R)$ and define two CFMMs to be *equivalent* if their trading sets are equal (*i.e.*, if the same trades are feasible in both). The main idea is that the definition of T is essentially unique with respect to the actions that any rational agent would take. More specifically, if two trading sets are not equal $T(R) \neq T'(R)$ for some reserves R , say, then there exists a trade in one set which is not feasible in the other; in other words, at least one trade $(\Delta, \Lambda) \in T(R)$ is not in $T'(R)$ and there exists no trade dominating (Δ, Λ) in either set.

An interesting and surprising consequence of this definition is that, given any trading function φ , we can construct an equivalent CFMM with trading function φ' such that $\varphi'(R, \cdot, \cdot)$ is monotonically nonincreasing in its first argument and nondecreasing in its second. We show this and discuss some additional implications in §A.1.

Equivalence in practice. The trading set for a constant mean market (3) can easily be written as the set of all nonnegative (Δ, Λ) that satisfy

$$\prod_{i=1}^n (R_i + \gamma \Delta_i - \Lambda_i)^{w_i} \geq \prod_{i=1}^n R_i^{w_i}.$$

If we were to take $n = 2$ and $w_1 = w_2 = 1/2$, then the trading set is the set of all nonnegative (Δ, Λ) that satisfy

$$(R_1 + \gamma \Delta_1 - \Lambda_1)^{1/2} (R_2 + \gamma \Delta_2 - \Lambda_2)^{1/2} \geq R_1^{1/2} R_2^{1/2}.$$

Squaring both sides of the inequality, as both quantities are nonnegative, gives exactly the equation for the trading set for the constant product market (2) for any possible reserve vector R and fee $\gamma \leq 1$. This implies that the trading sets are equal, which, in turn, implies the CFMMs are equivalent, as expected.

In fact, this case is the special case where the two trading functions are related by a strictly monotonic transformation, so the two trading sets are obviously equivalent. (More generally, the CFMMs with trading functions φ and $f \circ \varphi$ are equivalent for any invertible transformation $f : \mathbf{R} \rightarrow \mathbf{R}$.) An enlightening exercise is to write two different, but equivalent, trading functions for constant product and constant mean markets for which there exists no invertible transformation mapping one to the other.

2.2 Convexity of the trading set

We will make only one assumption regarding the trading set $T(R)$: for each possible reserve vector R , the set $T(R)$ is a closed convex set.

Discussion. This assumption of convexity has two important consequences. First, the geometry of convex sets is an extremely well-studied and developed field, and many basic results from this field suffice for the mathematical purposes of this paper, while remaining considerably general. The second case is that, when the set $T(R)$ can be written down in a

compact way (*e.g.*, as the intersection of a polynomial number of well-known convex cones), then we can usually solve convex optimization problems over this set in a computationally efficient way [37, §1], even when closed-form solutions aren't guaranteed to exist. As we will show later in §2.4, this implies that agents can easily maximize their payoff by computing an appropriate solution to an optimization problem over the trading set.

Convexity in practice. So far, to the knowledge of the authors at the time of writing, there is no CFMM used in practice whose trading set is nonconvex. For example, constant mean market CFMMs have convex trading sets since the weighted geometric mean function is a concave function, composition with an affine function preserves convexity, and the superlevel sets of a concave function are convex (*cf.*, [37, §3.1] for elementary proofs). This implies that the trading set

$$T(R) = \{(\Delta, \Lambda) \in \mathbf{R}_+^n \times \mathbf{R}_+^n \mid \prod_{i=1}^n (R_i + \Delta_i - \Lambda_i)^{w_i} \geq \prod_{i=1}^n R_i^{w_i}\},$$

is therefore a convex set, for any valid weights $w \geq 0$ with $\mathbf{1}^T w = 1$ and reserves R . (This also immediately shows that constant product markets have convex trading sets, as a special case.)

For a more complicated example, we will consider the trading function for Curve [9]:

$$\varphi(R, \Delta, \Lambda) = \alpha \mathbf{1}^T (R + \gamma \Delta - \Lambda) - \beta \prod_{i=1}^n (R_i + \gamma \Delta_i - \Lambda_i)^{-1}, \quad (5)$$

where $\alpha, \beta \geq 0$ are tunable parameters, $(1 - \gamma)$ is the percentage fee, and, as usual, $(\Delta, \Lambda) \in \mathbf{R}_+^n \times \mathbf{R}_+^n$. We can show that the trading set is convex directly, since the function $x \mapsto -(\prod_{i=1}^n x_i)^{-1}$ is a concave function that is increasing in each of its arguments. (A simple proof follows from the fact that $x \mapsto \log \prod_{i=1}^n x_i^{-1}$ is convex as it is the sum of negative logarithms, and a function is convex if it is log-convex [37, §3.5.1].) Therefore, the set of all (Δ, Λ) satisfying

$$\alpha \mathbf{1}^T (R + \gamma \Delta - \Lambda) - \beta \prod_{i=1}^n (R_i + \gamma \Delta_i - \Lambda_i)^{-1} \geq \alpha \mathbf{1}^T R - \beta \prod_{i=1}^n R_i^{-1},$$

is, again, a convex set as it is the superlevel set of the sum of an affine and a concave function.

2.3 Path deficiency and path independence

There are many special CFMMs which, when appropriately generalized, yield a very natural family of trading functions and sets worth studying. One particularly useful property that makes the analysis of some CFMMs simpler is path independence. While practical CFMMs usually don't satisfy path independence (often owing to their fee structure), path independent CFMMs often serve as a good starting point for reasoning about possible CFMMs and many of the special cases we study will be path independent.

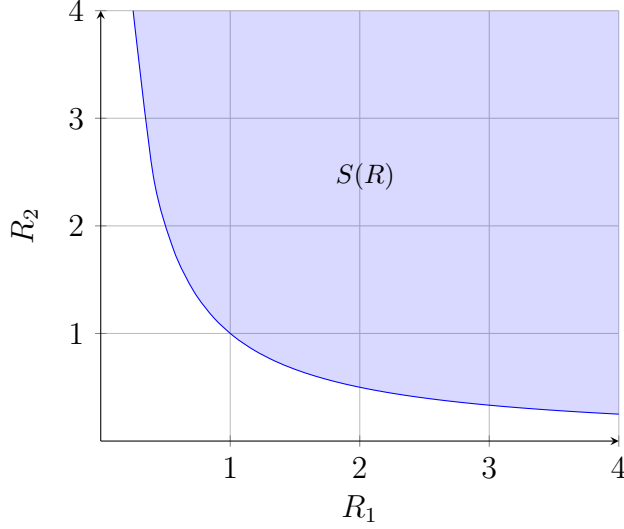


Figure 1: Example reachable set

We note that, unlike in the classical automated market maker literature (where path independence is almost a requirement), almost no CFMMs in practice are path independent. Much of the theory presented here also does not require this property to hold except in specific cases, and we will make explicit note of this when those results are presented. Because of this we will present a slight generalization of path independence, called path deficiency, which retains many of the useful properties but is satisfied by all known CFMMs used in practice.

The reachable reserve set. The definitions of path deficiency and path independence can be phrased in simple ways in terms of the *reachable reserve set*, defined, for fixed reserves $R \in \mathbf{R}_+^n$, as

$$S(R) = \{R + \Delta - \Lambda \mid (\Delta, \Lambda) \in T(R)\}. \quad (6)$$

Equivalently, the reachable reserve set, $S(R)$, is the set of reserves which can be *reached* from the current CFMM reserves by performing a single feasible trade. Note that the set $S(R)$ is also convex as it is the image of $T(R)$ under an affine transformation. The reachable reserve set is shown in figure 1 for the case of constant product markets with reserves satisfying $R_1 R_2 = 1$ and no fees.

2.3.1 Path deficiency

We will say that a CFMM is *path deficient* if, for given reserves R , any reachable reserve $R' \in S(R)$ has a reachable set satisfying $S(R') \subseteq S(R)$. In other words, performing any feasible trade can only make the reachable reserve set no larger than its current one.

This has a very simple implication: any path deficient CFMM initialized with reserves R^0 will always satisfy

$$\mathbf{1}^T R \geq \inf_{R' \in S(R^0)} \mathbf{1}^T R',$$

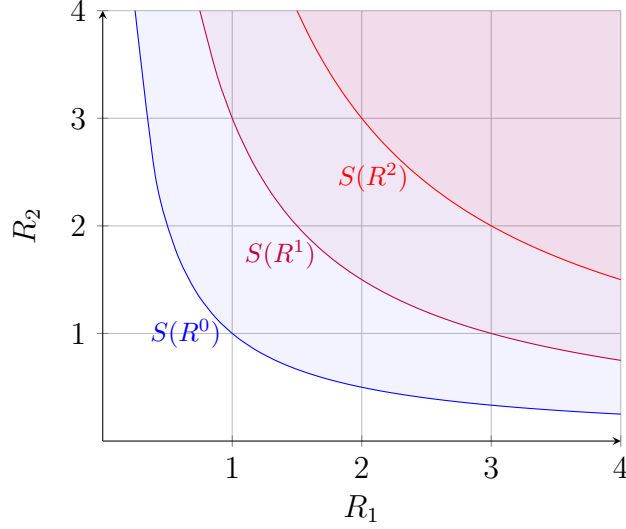


Figure 2: Example reachable sets of a (strictly) path-deficient CFMM after two trades

where R are the reserves after any number of feasible trades have been executed. This follows from the fact that $S(R) \subseteq S(R^0)$, which generalizes the known lower bounds for the total amount of coin in reserves for, *e.g.*, constant product and constant mean market makers [29, §2.3]. In other words, path deficiency guarantees that the reserves are always bounded from below after any set of trades has been performed.

Strict path deficiency. Additionally, we will say that a CFMM is *strictly path deficient* if $R' \in S(R)$ implies that $S(R') \subseteq \mathbf{dint} S(R)$, where $\mathbf{dint} S(R)$ is the dominated interior of $S(R)$, defined as

$$\mathbf{dint} S(R) = \{R' \in S(R) \mid R' \text{ dominates some element in } S(R)\}.$$

For two nonnegative vectors, $x, y \in \mathbf{R}_+^n$, we say x *dominates* y if $x \geq y$ and at least one of the inequalities holds strictly. Clearly, a strictly path deficient CFMM is path deficient, but not vice versa. Additionally, note that $\mathbf{relint} S(R) \subseteq \mathbf{dint} S(R)$, where $\mathbf{relint} S(R)$ is the relative interior [37, §2.1.3] of $S(R)$. See, *e.g.*, figure 2 for an example.

The main idea of strict path deficiency is to note that any agent will always prefer to make a trade such that the new CFMM reserves satisfy $R' \in S(R) \setminus \mathbf{dint} S(R)$ to a trade which changes the CFMM reserves to $R' \in \mathbf{dint} S(R)$, since, by definition, $R' \in \mathbf{dint} S(R)$ implies that the agent either received strictly less output or had to add in strictly more input than at least one possible feasible trade in $S(R)$.

Sufficient condition. A simple but very useful sufficient condition for strict path deficiency is that a CFMM is path deficient if we can write its trading set in the following form:

$$T(R) = \{(\Delta, \Lambda) \in \mathbf{R}_+^n \times \mathbf{R}_+^n \mid \psi(R + \gamma\Delta - \Lambda) \geq \psi(R)\},$$

where $0 \leq \gamma < 1$ and ψ is a quasiconcave function that is strictly increasing in its arguments. (For more information on quasiconcave functions, see, *e.g.*, [38].) A quick sketch of the proof is to note that $R + \Delta - \Lambda$ dominates $R + \gamma\Delta - \Lambda$ in at least one entry if $\Delta \neq 0$. Because the function is strictly increasing, then

$$\psi(R + \Delta - \Lambda) > \psi(R + \gamma\Delta - \Lambda) \geq \psi(R),$$

which gives the result after using the definition of the reachable reserve set (6) and using the fact that $\psi(R') > \psi(R)$ and $R' \geq R$ implies that R' dominates R .

This provides a much simpler proof of path deficiency than the one given in appendix D of [29] for constant product markets, and this sufficient condition covers all of the example trading functions given by equations (3) and (5), whenever $0 \leq \gamma < 1$.

2.3.2 Path independence

In a manner analogous to the classical market making literature, we will say a CFMM is *path independent* if it is path deficient and its reachable reserve set does not change after any feasible trade that is not dominated by another. In other words, a CFMM with reserves R is path independent whenever it is path deficient and $R' \in S(R) \setminus \mathbf{dint} S(R)$ implies $S(R') = S(R)$. By definition, any path independent CFMM is path deficient, but not strictly path deficient.

The main reason why path independence simplifies many of the derivations provided is that, in general, all of its properties can be written only as a function of the reserves the CFMM has at any one point in time, since no rational agent will ever make a trade such that the resulting reserves lie in the dominated interior, $\mathbf{dint}(R)$, as there would exist a feasible trade that would have been strictly better for the agent. We will see in the following sections that this yields a simple approach to finding the marginal price of given assets, among other cases.

Sufficient condition. A simple sufficient condition for path independence is that the set $T(R)$ can be written as

$$T(R) = \{(\Delta, \Lambda) \mid \psi(R + \Delta - \Lambda) \geq \psi(R)\}, \quad (7)$$

where ψ is a nondecreasing quasiconcave function. Since a concave function is quasiconcave, this condition is enough to show that all of the example trading functions, given by equations (3) and (5), are path independent whenever they have no fees ($\gamma = 1$).

2.4 Optimal arbitrage and the marginal price

First, we will look at the no-arbitrage conditions for a given CFMM and show that, in the case of path-deficient CFMMs, these conditions are the best an arbitrageur can hope to do. We will then look at how these conditions imply a specific marginal price for fixed reserves and then explore some important special cases for which the marginal prices are easy to write down.

Optimal arbitrage. In the arbitrage problem, we have a reference market of coins $i = 1, \dots, n$, where each can be sold or purchased at some fixed price given by $c_i > 0$ for each coin i . In this problem, an agent (usually called an arbitrageur) is allowed to borrow Δ_i of coin i for $i = 1, \dots, n$ and use it to trade with both the reference market and the CFMM, with the only condition that the loan is repaid at the end of the trade. The *optimal arbitrage problem* then asks what is the optimal arbitrage trade; *i.e.*, what is the optimal value of the problem

$$\begin{aligned} & \text{maximize} && c^T(\Lambda - \Delta) \\ & \text{subject to} && (\Delta, \Lambda) \in T(R), \end{aligned} \tag{8}$$

with variables $\Delta, \Lambda \in \mathbf{R}^n$, where R specifies the current reserves of the CFMM at the time the trade is to be performed. An equivalent formulation in terms of the reachable set is

$$\begin{aligned} & \text{maximize} && c^T(R - R') \\ & \text{subject to} && R' \in S(R), \end{aligned} \tag{9}$$

with variable $R' \in \mathbf{R}^n$. The equivalence follows by noting that we can write $R' = R + \Delta - \Lambda$ and there exists such a $(\Delta, \Lambda) \in T(R)$ if, and only if, $R' \in S(R)$, by definition. Additionally, note that any optimal point for (9) will always have $R' \in S(R) \setminus \mathbf{dint} S(R)$.

Because both problems are convex problems, it is almost always the case that they can be efficiently solved whenever the set $T(R)$ can be compactly expressed in terms of well-known convex sets. Additionally, the optimality conditions of problem (9) imply that there exists a supporting hyperplane for the set $S(R)$ with slope collinear to c at the optimal point R^* . (For more details, see Corollary 11.5.2 and Theorem 18.8 of [39].)

Path deficiency. In general, it may be possible that solving problem (9) and executing the optimal trade provided is actually not the best possible strategy for a specific arbitrageur. For example, it may be the case that an arbitrageur could somehow have a higher-payoff strategy by breaking up the trade into many smaller trades and performing some complicated trading procedure that results in a better payoff.

In this case, the idea of path deficiency is extraordinarily useful: if a CFMM is path deficient, then there is no strategy by which an arbitrageur could have higher payoff than simply solving problem (8) or (9) and executing the resulting trade. Additionally, if the CFMM is strictly path deficient, then the arbitrageur only does worse by attempting to subdivide the resulting trades.

To show this, we will consider any strategy $\{R^i\}_{i=0}^m$ such that the i th action taken by the arbitrageur changes the reserves from R^i to R^{i+1} and is feasible, *i.e.*, $R^{i+1} \in S(R^i)$. Now, by definition, the price paid by the agent during the i th action is equal to $c^T(R^i - R^{i+1})$. Summing over the prices implies that the total payoff of this strategy is equal to $c^T(R^0 - R^m)$. Since the CFMM is path deficient, the reachable reserve sets satisfy $S(R^{m-1}) \subseteq \dots \subseteq S(R^0)$, so $R^m \in S(R^0)$, which implies that this strategy cannot have higher payoff than the optimal value of (9), since the strategy taking R^0 to R^m in one step is feasible for (9) and has the same payoff.

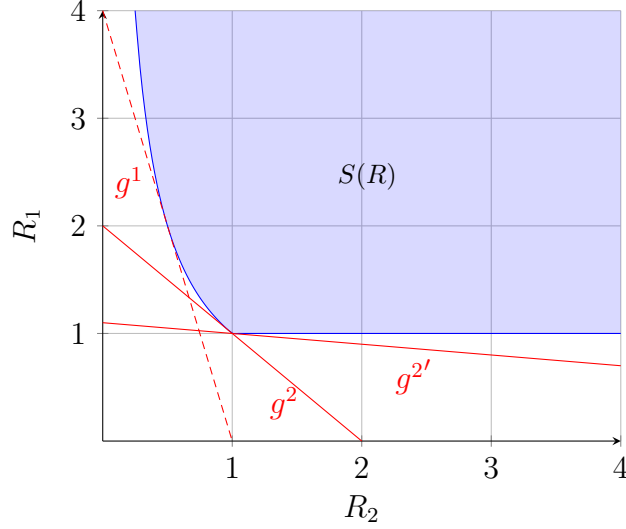


Figure 3: Reported prices for an example CFMM

The case where the CFMM is strictly path deficient is rather similar. If the number of moves taken satisfies $m > 1$, then clearly $R^m \in \mathbf{dint} S(R^0) \subseteq S(R^0)$. But, by definition, R^m is in the dominated interior only when there exists a trade $R' \in S(R^0)$ which dominates R^m . Because R' is feasible for (9), then the optimal value of problem (9) must be strictly larger than the payoff for the original m -step strategy. This, in turn, implies that $m = 1$ and the resulting problem reduces exactly to (9).

Reported price. The optimality conditions for problem (9) suggest a simple definition for the prices that should be reported by the CFMM, at some reserves R' : the CFMM should report the slope of the supporting hyperplane of $S(R)$ at the point R' , scaled appropriately by the numéraire. In other words, if $g \in \mathbf{R}^n$ is a supporting hyperplane of $S(R)$ at R' , then the reported price should be λg for some $\lambda \geq 0$.

The scaling constant exists since the choice of numéraire is always left to the CFMM designer and does not change the optimality conditions. For example, if coin 1 is chosen as the numéraire, then the designer would choose $\lambda = 1/g_1$ and the CFMM would then report g/g_1 as the prices of all coins, such that the reported price of coin 1 is always $(g/g_1)_1 = 1$, as desired.

We also note that there may be many supporting hyperplanes of $S(R)$ at any one point (cf., g^2 and $g^{2'}$ at reserves $(1, 1)$ in figure 3) in which case there are many no-arbitrage prices implied by these reserves and no unique price can be reported. For example, if there exist two supporting hyperplanes with slopes g and g' , then any convex combination of g and g' is also a supporting hyperplane and therefore a valid price. For convenience, we will assume that all such prices are reported, though this need not be true in practice.

Discussion. By reporting the price at the optimality conditions of the optimal arbitrage problem, we have essentially resolved two issues in one.

First, the definition of the reported prices implies that, given a reference market with prices equal to $c \in \mathbf{R}_+^n$, an arbitrageur is always incentivized to make any one of the prices reported by the CFMM equal to c , since any other trade is strictly suboptimal. In other words, if the price of the CFMM is mismatched to that of a reference market, an agent is able to make what is essentially ‘free money’ by only trading between these markets, which, in turn, would correct the price reported by the CFMM to be the same as the reference market price.

Second, unlike the reported price, there is no guarantee that a marginal price at one specific reserve value is well-defined, since the definition of a marginal price requires the existence of arbitrarily small trades. (One simple example where a marginal price might not exist is to consider any CFMM that requires a fixed, nonzero amount of input before any trade is accepted.) On the other hand, if the CFMM is path independent, then the reported price and the marginal price will always match exactly. We show a proof in §A.2.

Special cases. The reported price can be easily computed in the common case where the trading set can be written in the form of (7), in which case the reachable set is constant after any optimal trade since every optimal trade is never in the dominated interior, which, in turn, implies that an optimal trade always leaves the reachable set unchanged by the definition of path independence. We can then use (7) to write the reachable sets as

$$S(R) = S(R^0) = \{R' \in \mathbf{R}^n \mid \psi(R') \geq \psi(R^0)\},$$

for any $R \in S(R^0) \setminus \mathbf{dint} S(R^0)$, where R^0 are the reserves of the CFMM before the trade was completed. In this case, the first order optimality conditions of (9) would imply that

$$c \in \lambda \partial \psi(R'^*),$$

where $\partial \psi(R'^*)$ are the subgradients of the function ψ at R'^* , that are, by definition, supporting hyperplanes of the epigraph of ψ (see [39, §23]). Here, $\lambda \geq 0$ acts as a scaling constant and depends on the choice of numéraire.

If ψ is differentiable, then we would instead have (see Theorem 25.1 of [39]),

$$c = \lambda \nabla \psi(R'^*),$$

so the reported prices of this CFMM at some reserves R are simply proportional to $\nabla \psi(R)$. In general, when the trading set of a CFMM can be written in the form of (7), we would expect the function ψ to be differentiable since this case corresponds to the existence of exactly one possible price that can be reported for some reserves R .

Practical examples. In the case of constant mean markets (*e.g.*, Balancer), given the reserves R , we can very easily give the reported prices in the fee-less case. In this case, note

that, from (3),

$$\psi(R) = \prod_{i=1}^n R_i^{w_i},$$

so, after taking the gradient, we have:

$$(\nabla\psi(R))_j = \frac{w_j}{R_j} \prod_{i=1}^n R_i^{w_i} = \frac{w_j}{R_j} \psi(R).$$

Therefore, the price of some coin j with respect to some second coin k corresponds to choosing coin k as the numéraire, *i.e.*, choosing $\lambda = 1/(\nabla\psi(R))_k$, we get

$$\lambda(\nabla\psi(R))_j = \frac{(\nabla\psi(R))_j}{(\nabla\psi(R))_k} = \frac{w_j/R_j}{w_k/R_k}.$$

And, because $\gamma = 1$, the CFMM is path independent, the reported price is equal to the marginal price. Note that this result is equal to the original derivation of the marginal price given in the Balancer whitepaper [8, Eq. 7], though it is considerably more concise to derive using this formalism.

It is also not difficult to derive the prices that the Curve CFMM should report. From (5),

$$\psi(R) = \alpha \mathbf{1}^T R - \beta \left(\prod_{i=1}^n R_i \right)^{-1},$$

so

$$(\nabla\psi(R))_j = \alpha + \beta \left(R_j \prod_{i=1}^n R_i \right)^{-1},$$

and, taking coin k as the numéraire, we find the price of coin j as,

$$\frac{(\nabla\psi(R))_j}{(\nabla\psi(R))_k} = \frac{\alpha + \beta (R_j \prod_{i=1}^n R_i)^{-1}}{\alpha + \beta (R_k \prod_{i=1}^n R_i)^{-1}}.$$

2.5 Liquidity providers and returns

An important aspect of CFMMs is the ability for liquidity providers, as described in §2, to add or remove value from the reserves. Because liquidity providers own some explicit percentage of the total amount of coins in reserves, we consider what the current value of the CFMM's total reserves are, under the same assumptions of §2.4: that (a) there exists an external, infinitely liquid reference market and (b) there exists an arbitrageur who is solving the arbitrage problem. The total value in the reserves is then proportional to the value of the position a liquidity provider has, with respect to the CFMM (where the proportionality constant is simply the percentage of the reserves that a liquidity provider is entitled to).

Value in reserves. By definition, the total value of all assets held in reserves, R , by the CFMM is simply $c^T R$, where $c_i > 0$ is the price of currency i given by a reference market. To say what the total value of the reserves is, note that problem (9) is equivalent to the following problem:

$$\begin{aligned} & \text{minimize} && c^T R' \\ & \text{subject to} && R' \in S(R), \end{aligned} \tag{10}$$

with variable $R' \in \mathbf{R}^n$, in the sense that an optimal R' for (9) is optimal for (10) and vice versa. We can see this since the term $c^T R$ in the objective of (9) is a constant in the problem, and we've simply switched maximizing a function with minimizing its negative. Since this is true, then the optimal value of (10) is exactly the total value of the reserves.

Throughout the remainder of this section, we will let $p_R^*(c)$ be the optimal value of problem (10) for a given cost vector c and fixed reserves R . We also note that the function $p_R^*(c)$ can be recognized as the negative of the support function of the set $S(R)$ [39, §13].

Path deficiency. An important consequence of path deficiency with respect to the total reserve value is that, in general, the total value of the reserves never decreases for a fixed cost vector. In particular, if R are the reserves at some (initial point) and R' are the reserves at some future point (after any number of trades have been performed), then, by definition of path deficiency, we have $S(R') \subseteq S(R)$. This immediately implies that $p_{R'}^*(c) \geq p_R^*(c)$, since problem (10) with reserves R contains all of the same feasible points of problem (10) with reserves R' , so its optimal value can be no higher. It is not difficult to prove that strict path deficiency implies that this value is, instead, strictly increasing—the idea follows from the fact that all optimal points of (10) with reserves R will always lie in $S(R) \setminus S(R')$ and that $S(R')$ is a closed set.

The dual function. If we can write the reachable reserve set as,

$$S(R) = \{R' \in \mathbf{R}^n \mid \psi(R') \geq \psi(R)\},$$

for some concave, increasing function ψ , then the Lagrangian [37, §5.1.1] of problem (10) is

$$\mathcal{L}(R', \lambda) = c^T R' - \lambda(\psi(R') - \psi(R)),$$

which lets us write the dual function $g(\lambda) = \inf_{R'} \mathcal{L}(R', \lambda)$ for $\lambda \geq 0$. This function, written in terms of ψ is

$$g(\lambda) = \lambda\psi(R) + \inf_{R'} (c^T R' - \lambda\psi(R')) = \lambda\psi(R) - \sup_{R'} ((-c)^T R' - \lambda(-\psi)(R')).$$

If $\lambda > 0$, we have that the last term is equal to

$$\sup_{R'} ((-c)^T R' - \lambda(-\psi)(R')) = \lambda \sup_{R'} ((-c/\lambda)^T R' - (-\psi)(R')) = \lambda(-\psi)^* \left(-\frac{c}{\lambda}\right),$$

where $(-\psi)^*$ is the Fenchel conjugate [37, §3.3] of $-\psi$ and is known for a very large number of convex functions. We also note that this operation is just the perspective transform of $(-\psi)^*$

(sometimes called epi-multiplication [39, §5]) and is well defined even when $\lambda = 0$, though we will continue to write the term as is for simplicity. Combining the resulting statements, we get

$$g(\lambda) = \lambda\psi(R) - \lambda(-\psi)^*\left(-\frac{c}{\lambda}\right),$$

for $\lambda \geq 0$.

By weak duality [37, §5.2.2], we know that $\sup_{\lambda \geq 0} g(\lambda) \leq p_R^*(c)$, so picking any $\lambda \geq 0$ will suffice to give a lower bound on the total value of the reserves. Additionally, since ψ is concave, then strong duality holds [37, §5.2.3] and we have that

$$p_R^*(c) = \sup_{\lambda \geq 0} g(\lambda) = \sup_{\lambda \geq 0} \left(\lambda\psi(R) - \lambda(-\psi)^*\left(-\frac{c}{\lambda}\right) \right), \quad (11)$$

instead. This construction gives us a way of computing total reserve values by solving a single-variable convex optimization problem (since g is always a convex function [37, §5.1.2]) and, in some important cases, gives closed form expressions for the total reserve value.

Constant mean reserve values. Using the constant mean trade function with $\gamma = 1$, given in (3), we can write

$$\psi(R) = \prod_{i=1}^n R_i^{w_i}.$$

We will write, for convenience, $k = \psi(R^0)$ at the initial reserves R^0 . Note that, since this CFMM is path independent, the reachable reserve set does not change and we may assume that the reachable reserve set is simply $S(R) = \{R' \in \mathbf{R}^n \mid \psi(R') \geq k\}$ for any reachable reserves R .

From [37, prob. 3.36], we have that, for any cost vector $c \in \mathbf{R}_+^n$:

$$(-\psi)^*(-c) = \begin{cases} 0 & \prod_{i=1}^n c_i^{w_i} \geq 1/n \\ \infty & \text{otherwise.} \end{cases}$$

As before, the current value of the reserves is given by (11):

$$\sup_{\lambda \geq 0} \left(\lambda k - \lambda(-\psi)^*\left(-\frac{c}{\lambda}\right) \right).$$

Now, note that

$$\lambda k - \lambda(-\psi)^*\left(-\frac{c}{\lambda}\right) = \begin{cases} \lambda k & (\prod_i c_i^{w_i})/\lambda \geq 1/n \\ -\infty & \text{otherwise,} \end{cases}$$

which we can easily maximize by choosing the largest possible λ , *i.e.*, $\lambda = n \prod_i c_i^{w_i}$, since $k > 0$, yielding

$$\sup_{\lambda \geq 0} \left(\lambda k - \lambda(-\psi)^*\left(-\frac{c}{\lambda}\right) \right) = nk \prod_{i=1}^n c_i^{w_i}. \quad (12)$$

Using the special case of $n = 2$ and $w_1 = w_2 = 1/2$, we can recover the total reserve value of Uniswap with zero fees, derived via a different method in [29, §2.3]. To see this, set $c_1 = 1$ (*i.e.*, coin 1 is the numéraire) such that c_2 is the market price of coin 2 with respect to coin 1. Then, we can write the total value in reserves as,

$$p^* = 2k\sqrt{c_2},$$

where the square root difference between the expression in [29, §2.3] and this one comes from the fact that k here is the *square root* of the product constant, *i.e.*, $k = \sqrt{R_1 R_2}$. (See [29, §3].)

Lower bounds for Curve. We suspect that there is no analytical solution to the total reserve value for the Curve CFMM, given in (5). We will, instead, derive some lower bounds to the total reserve value by appropriately choosing $\lambda \geq 0$, where the function we consider is

$$\psi(R) = \alpha \mathbf{1}^T R - \beta \left(\prod_{i=1}^n R_i \right)^{-1},$$

which means the CFMM's reachable set is $S(R) = \{R \in \mathbf{R}^n \mid \psi(R) \geq k\}$, where $k = \psi(R^0)$ and this CFMM is path independent.

First, for $\lambda \geq 0$,

$$\lambda(-\psi)^* \left(-\frac{c}{\lambda} \right) = -(n+1)(\lambda\beta)^{1/(n+1)} \prod_{i=1}^n (c_i - \lambda\alpha)^{1/(n+1)},$$

if $c_i - \lambda\alpha \geq 0$ for each $i = 1, \dots, n$ and $+\infty$, otherwise (see §A.3). The dual function, $g : \mathbf{R} \rightarrow \mathbf{R}$, is then

$$g(\lambda) = \lambda k + (n+1)(\lambda\beta)^{1/(n+1)} \prod_{i=1}^n (c_i - \lambda\alpha)^{1/(n+1)},$$

if $c_i - \lambda\alpha \geq 0$ for each $i = 1, \dots, n$ and $-\infty$, otherwise. Some simple lower bounds come from considering λ as large as possible, which is somewhat tight if k is very large relative to $(\beta \prod_{i=1}^n c_i)^{1/(n+1)}$. We can do this by choosing $\lambda = \min_i c_i / \alpha$, giving the following lower bound for the total reserve value:

$$p_R^*(c) \geq \left(\frac{k}{\alpha} \right) \min_i c_i.$$

Though we suspect that, in general, the exact value of $p_R^*(c)$ cannot be given in closed form, we note that the resulting problem of optimizing g is a one-parameter convex optimization problem that is, in practice, easy to solve numerically.

3 Extensions and future work

There are several important applications and essentially immediate extensions of the current conditions and definitions that are interesting to study in their own right. We discuss some basic examples here.

3.1 Trading fees

We can easily introduce trading fees to any given CFMM. A simple but effective approach is to introduce fees on the input trade. Given a trading function φ for a CFMM, we can then write a new trading function φ_f with some fee constant $0 < \gamma \leq 1$ defined as

$$\varphi_f(R, \Delta, \Lambda) = \varphi(R, \gamma\Delta, \Lambda),$$

for all reserves R , inputs Δ , and outputs Λ where $(1 - \gamma)$ is the percentage fee required. Equivalently, we can write this in terms of a new trading set $T_f(R)$ as

$$T_f(R) = \{(\Delta, \Lambda) \mid (\gamma\Delta, \Lambda) \in T(R)\},$$

for each reserve R .

In this case, the trader is required to put in $1/\gamma$ more of input Δ for a trade to be feasible. Additionally, this will turn path independent CFMMs into path deficient ones (strictly path deficient, if $\gamma < 1$). Because the resulting CFMM is path deficient, this method also has the nice property that the total reserve values are always bounded from below by the solution to (10).

There are several more possible methods, some of which may include variable input and/or output fees which vary in such a way as to keep other desirable properties of the CFMMs on a case-to-case basis. We suspect that there are many approaches for charging trading fees, each with their own useful properties, but leave the possibility of finding a suitable class of these trading fees that is good to study for future work.

3.2 Comparison to scoring rules

While it is tempting to ask about potential comparisons or equivalences to classic algorithmic game theory automated market makers and scoring rules such as Hanson's LMSR or the more general constant utility market makers for prediction markets provided in [40], we note that this is likely not possible using only the no-arbitrage framework used in this paper. A simple thought experiment shows why this might be the case.

Given an infinitely liquid reference market with a fixed price p_1 from time $[0, T)$, where $T > 0$, and price $p_2 > p_1$ at time T (known by all agents), then the reported price of a prediction market which seeks to predict the price of the asset at time T and the reported price of a given CFMM will always diverge by $p_2 - p_1$. Rational agents will always be incentivized to correctly report the (known) future price p_2 for the prediction market, while arbitrageurs will always make positive payoff from any CFMM which diverges from the

current market price p_1 at all times $[0, T)$, by setting the reported price to be p_1 . Sending $p_2 - p_1 \rightarrow \infty$ then shows that these two AMMs can diverge by any desired amount.

The idea here is that any framework which can compare the two will require assumptions about the market price dynamics, *i.e.*, what the current market price might say about the future market price, which we do not assume at any point in this presentation. We leave this potentially very interesting research avenue of finding a suitable framework for comparison for future work.

3.3 Optimization over possible CFMMs

Note that the given conditions define a family of CFMMs which are likely to be useful in practice. This implies that, for any performance metric (*e.g.*, average total reserve value for a given market model) that a market maker designer wishes to optimize, one could find an (approximately) optimal CFMM to accomplish this task. The problem is likely to be computationally difficult to solve exactly in most important cases, but we suspect that many commonly-used heuristics will likely find good results. Though this approach is unlikely to be feasible except when n is small, we imagine that the very useful case of $n = 2$ can be quickly optimized on modern hardware for many useful performance metrics.

Additionally, if the trading function φ is parametrized by a small number of parameters (for example, the parameters α, β in (5)), it is possible to at least approximately optimize these parameters to maximize or minimize some desired objective function of the trading sets or the reachable sets.

3.4 Time-dependent CFMMs and other generalizations

Note that the conditions and definitions above can be very easily extended to the cases where the trading function φ depends on exogenous variables such as time. In particular, we may assume that arbitrage happens instantaneously or nearly instantaneously. This, in turn, would imply that some (but not all) of our analysis on general CFMMs holds even in this scenario.

There are still several interesting questions to answer in this case. One such question is: what is a natural generalization of the reachable set when the trading function (or, equivalently, the reachable set) is also time-dependent? A simple (but likely woefully incomplete) answer is that, if the reachable set depends on time, say $S_t(R)$, where $t \geq 0$ is a time variable, we additionally have $S_{t'}(R) \subseteq S_t(R)$ for all R and $t' \geq t$. This retains some of the given properties, such as the lower bounds on the total reserve values given in (11), but is likely to be too strong of a condition to be useful in practice.

Another natural question is, are there good restrictions on how liquidity providers should add liquidity to reserves? One could imagine that, in some scenarios, allowing agents to add coins to reserves in an arbitrary way could lead to large losses for liquidity providers. An even more fundamental question, which we do not cover at all is: can liquidity provision easily be included in a similar framework? We suspect so, but even this is not clear at the moment and is likely to be a good avenue for future exploration.

4 Conclusion

The increase in usage and participation in automated market makers has led to a vast set of new scoring rules and pricing mechanisms. Analyzing these mechanisms, which range from LMSR style market makers and CFMMs to scoring rules for rates [41], from the perspective of optimization provides insight into why certain mechanisms are more popular than others and work well in practice. In particular, we show that CFMMs provide an easy optimization problem for arbitrageurs to synchronize off-chain and on-chain pricing data, along with several useful conditions that often hold in practice, which imply that CFMMs are likely to be very well behaved. This generalization encompasses all live CFMMs [7, 8, 27, 9] and provides guidance on how one can design CFMMs that are better for certain asset types and volatilities, based on liquidity provider returns. This construction also gives a way of studying CFMMs from first principles, which may be of use as a starting point for new and interesting applications and generalizations of CFMMs.

Acknowledgements

We would like to thank John Morrow and Tim Roughgarden for feedback on this paper and Alex Evans for feedback and pointing out that the current CFMM analysis extends to the case where the trading function is time dependent. We would also like to thank the reviewers for helpful comments and suggestions, many of which we have incorporated in the text.

References

- [1] A. Othman, D. M. Pennock, D. M. Reeves, and T. Sandholm, “A practical liquidity-sensitive automated market maker,” *ACM Transactions on Economics and Computation (TEAC)*, vol. 1, no. 3, pp. 1–25, 2013.
- [2] R. Hanson, “Combinatorial information market design,” *Information Systems Frontiers*, vol. 5, no. 1, pp. 107–119, 2003.
- [3] Google, “google/arithmancer,” May 2017.
- [4] N. Bene, “Getting to the core,” Apr 2018.
- [5] A. Othman and T. Sandholm, “Automated market-making in the large: the Gates Hillman prediction market,” in *Proceedings of the 11th ACM conference on Electronic commerce*, pp. 367–376, 2010.
- [6] M. Chakraborty, S. Das, A. Lavoie, M. Magdon-Ismael, and Y. Naamad, “Instructor rating markets,” in *Twenty-Seventh AAAI Conference on Artificial Intelligence*, 2013.
- [7] Y. Zhang, X. Chen, and D. Park, “Formal specification of constant product ($xy=k$) market maker model and implementation,” 2018.

- [8] F. Martinelli and N. Mushegian, “Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor,” 2019.
- [9] M. Egorov, “StableSwap - efficient mechanism for Stablecoin liquidity,” p. 6.
- [10] N. Koblitiz and A. J. Menezes, “The random oracle model: a twenty-year retrospective,” *Designs, Codes and Cryptography*, vol. 77, no. 2-3, pp. 587–610, 2015.
- [11] J. Peterson and J. Krug, “Augur: a decentralized, open-source platform for prediction markets,” *arXiv preprint arXiv:1501.01042*, 2015.
- [12] D. Mohanty, “Advanced programming in Oraclize and IPFS, and best practices,” in *Ethereum for Architects and Developers*, pp. 151–179, Springer, 2018.
- [13] Provable Data Team, “A scalable architecture for on-demand, untrusted delivery of entropy,” Mar 2019.
- [14] S. Wolfram, “Did Stephen Wolfram’s knowledge engine just become a quantum neural blockchain AI?,” Apr 2018.
- [15] M. Team, “The Dai stablecoin system,” *URL: <https://makerdao.com/whitepaper/DaiDec17WP.pdf>*, 2017.
- [16] R. O’Donnell, *Analysis of boolean functions*. Cambridge University Press, 2014.
- [17] X. Chen, C. Papadimitriou, and T. Roughgarden, “An axiomatic approach to block rewards,” in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pp. 124–131, 2019.
- [18] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, “Astraea: A decentralized blockchain oracle,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1145–1152, IEEE, 2018.
- [19] H. Lambur, A. Lu, and R. Cai, “Uma data verification mechanism: Adding economic guarantees to blockchain oracles,” Jul 2019.
- [20] W. Warren and A. Bandeali, “0x: An open protocol for decentralized exchange on the Ethereum blockchain,” 2017.
- [21] A. Juliano, “dydx: A standard for decentralized derivatives,” 2017.
- [22] D. Pulse, “DeFi pulse: The DeFi leaderboard: Stats, charts and guides.”
- [23] Dune Analytics, “Dune analytics decentralized exchange dashboard,” Jan 2020.

- [24] C. Decker and R. Wattenhofer, “Bitcoin transaction malleability and MtGox,” in *European Symposium on Research in Computer Security*, pp. 313–326, Springer, 2014.
- [25] D. Shane, “A crypto exchange may have lost \$145 million after its CEO suddenly died,” *CNN Business*, <https://edition.cnn.com/2019/02/05/tech/quadriga-gerald-cotten-cryptocurrency/index.html>, 2019.
- [26] I. Kaminska, “Bitcoin Bitfinex exchange hacked: The unanswered questions,” *Financial Times*, vol. 4, 2016.
- [27] E. Hertzog, G. Benartzi, and G. Benartzi, “Bancor protocol,” 2017.
- [28] H. Adams, “Uniswap birthday blog - v0,” Nov 2019.
- [29] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, “An analysis of Uniswap markets,” *Cryptoeconomic Systems*, to appear.
- [30] S. Kamvar, M. Olszewski, and R. Reinsberg, “Celo: A multi-asset cryptographic protocol for decentralized social payments,” 2017.
- [31] S. Higgins, “Decentralized exchange protocol 0x raises \$24 million in ICO,” Aug 2017.
- [32] F. Haga, “2019 DEX summary stats,” 2019.
- [33] F. Haga, “Bancor monthly volumes, 2019-2020,” 2020.
- [34] Y. Cheng, “0x developers release liquidity aggregation tool for Ethereum-based exchange protocol,” Jan 2020.
- [35] S. Nace, “Topic: Exchange traded funds.”
- [36] G. L. Gastineau, “An introduction to exchange-traded funds (ETFs),” *Journal of Portfolio Management and Economics*, vol. 27, no. 3, pp. 88–96, 2001.
- [37] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK ; New York: Cambridge University Press, 2004.
- [38] A. Agrawal and S. Boyd, “Disciplined Quasiconvex Programming,” *arXiv:1905.00562 [cs, math]*, June 2019.
- [39] R. T. Rockafellar, *Convex Analysis*, vol. 28. Princeton university press, 1970.
- [40] A. Othman and T. Sandholm, “Automated Market Makers That Enable New Settings: Extending Constant-Utility Cost Functions,” in *Auctions, Market Mechanisms, and Their Applications* (P. Coles, S. Das, S. Lahaie, and B. Szymanski, eds.), vol. 80, pp. 19–30, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. Series Title: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.

- [41] T. Chitra, “Competitive equilibria between staking and on-chain lending,” *arXiv preprint arXiv:2001.00919*, 2019.

A Miscellaneous Proofs

A.1 An equivalent monotonic trade function

Given some trade function φ , we will write an equivalent CFMM with trading function $\varphi'(R, \cdot, \cdot)$ that is monotonically nonincreasing in its first argument and monotonically non-decreasing in its second, for each possible reserves R .

First, define the squared distance-to-set function for some set $U \subseteq \mathbf{R}^n$ and point $x \in \mathbf{R}^n$ as

$$d(x, U) = \inf_{y \in U} \|x - y\|_2^2.$$

Then the following function

$$\varphi'(R, \Delta, \Lambda) = d((\Delta, \Lambda), T(R)),$$

suffices. In this case, $\varphi'(R, \cdot, \cdot)$ measures the squared distance of a given trade to the trade set.

Equivalence. First we will show that the trading sets of φ and φ' are equivalent. If $\varphi'(R, \Delta, \Lambda) = \varphi'(R, 0, 0)$ then we have that

$$d((\Delta, \Lambda), T(R)) = d((0, 0), T(R)) = 0,$$

so $(\Delta, \Lambda) \in T(R)$, since $T(R)$ is a closed set. Conversely, if $\varphi'(R, \Delta, \Lambda) \neq \varphi'(R, 0, 0)$ then $\varphi'(R, \Delta, \Lambda) > 0 = \varphi'(R, 0, 0)$. So the distance between (Δ, Λ) and the set is strictly positive $d((\Delta, \Lambda), T(R)) > 0$, and, in turn, we have $(\Delta, \Lambda) \notin T(R)$. This implies that the function φ' has trading set $T(R)$ and is therefore equivalent to φ . (As a second useful note, if the set $T(R)$ is convex, then $\varphi'(R, \cdot, \cdot)$ is also convex in its arguments [37, §3.2.5].)

Monotonicity. Since monotonicity of φ' is defined elementwise, it suffices to prove monotonicity for distance functions from general sets $Q \subseteq \mathbf{R} \times \mathbf{R}^n$ of the form

$$Q = \{(t, q) \mid (t', q) \in W \text{ for some } t' \leq t\},$$

for some nonempty closed set $W \subseteq \mathbf{R} \times \mathbf{R}^n$. (Note that the set Q is closed if the set W is.)

We will show that the squared distance-to-set function, $d(\cdot, Q)$, is decreasing with respect to the first element of its first argument. Consider some pair $(t, q) \in \mathbf{R} \times \mathbf{R}^n$ and let $(t^*, q^*) \in \mathbf{R} \times \mathbf{R}^n$ minimize $d(t, q)$, which exists since the set is closed. Now, for any $t' \in \mathbf{R}$ with $t' \geq t$, either $t' \geq t^*$, in which case

$$d(t', q) \leq \|q - q^*\|_2^2 \leq d(t, q)$$

since $(t', q^*) \in Q$ by definition of Q , or $t' < t^*$, which implies that $t \leq t' < t^*$ so clearly,

$$d(t', q) \leq (t' - t^*)^2 + \|q - q^*\|_2^2 < (t - t^*)^2 + \|q - q^*\|_2^2 = d(t, q),$$

which shows that $d(t', q) \leq d(t, q)$ for every $t' \geq t$.

The complete proof then follows from the fact that we can apply this proof elementwise to the function $\varphi'(R, \cdot, \cdot)$.

Discussion. In general, the fact that we can always write a monotonic trade function for any trade set implies that problem (8) and the following ‘relaxed’ problem are equivalent (for fixed reserves R),

$$\begin{aligned} & \text{minimize} && c^T(\Lambda - \Delta) \\ & \text{subject to} && \varphi'(R, \Delta, \Lambda) \leq 0. \end{aligned} \tag{13}$$

Here, the variables are $\Lambda, \Delta \in \mathbf{R}^n$ and the problem data are R and c .

To see this, first note that, any trade (Δ, Λ) that is feasible for problem (8) is clearly feasible for this problem since, by definition of φ' , $\varphi'(R, \Delta, \Lambda) = 0$, so the optimal objective value is no larger than that of (8). Additionally, no optimal point (Δ^*, Λ^*) for problem (13) will ever satisfy $\varphi'(\Delta^*, \Lambda^*) < 0$. We can see this since the function φ' is continuous, which implies that the set of all (Δ, Λ) satisfying $\varphi'(\Delta, \Lambda) < 0$ is an open set. This, in turn, implies that, for any trade (Δ, Λ) satisfying $\varphi'(\Delta, \Lambda) < 0$ there always exists a trade (Δ', Λ') satisfying $\Delta' < \Delta$ and $\Lambda' > \Lambda$ (since there always exists such a pair (Δ', Λ') in some neighborhood around (Δ, Λ) , for a nonempty open set) which clearly has strictly lower objective value, so (Δ, Λ) cannot be optimal for (13). So, $\varphi'(R, \Delta^*, \Lambda^*) = 0$ and, therefore, that we also have $(\Delta^*, \Lambda^*) \in T(R)$, so any optimal point for (13) is also feasible for (8), implying that both problems have the same optimal value.

Because $\varphi'(R, \cdot, \cdot)$ is convex if $T(R)$ is, then problem (13) is additionally a convex optimization problem whenever $T(R)$ is convex.

A.2 Marginal price for path independent CFMMs

First, we define the price of performing a trade as the minimal cost of receiving a desired output of Λ , where the value of coin i is given by $c_i > 0$:

$$p(R, c, \Lambda) = \inf\{c^T \Delta \mid R + \Delta - \Lambda \in S(R)\}. \tag{14}$$

Now, under the scenario given in problem (9), we have that the reported price, c is a supporting hyperplane of $S(R)$ at the point $R' = R + \Delta^* - \Lambda^*$ where (Δ^*, Λ^*) is the optimal arbitrage trade, and that $S(R') = S(R)$, since the CFMM is path independent. We can then define the marginal price of a desired output Λ , after the optimal trade is completed, as the limit:

$$\lim_{\varepsilon \downarrow 0} \frac{p(R', c, \varepsilon \Lambda)}{\varepsilon}.$$

By definition, since c is a supporting hyperplane of $S(R)$ at R' , we have that

$$c^T(R'' - R') \geq 0, \text{ for all } R'' \in S(R),$$

which implies that

$$c^T(\Delta - \Lambda) \geq 0,$$

for all Δ, Λ satisfying $R' + \Delta - \Lambda \in S(R) = S(R')$, which can easily be rewritten as $c^T \Delta \geq c^T \Lambda$. Using this inequality with the definition of the marginal price (14), we find:

$$\frac{p(R', c, \varepsilon \Lambda)}{\varepsilon} \geq \frac{1}{\varepsilon}(\varepsilon c^T \Lambda) = c^T \Lambda.$$

but the inequality is, in fact, an equality since $\Delta = \varepsilon \Lambda$ is a feasible point for (14) as $R' \in S(R) = S(R')$. Since the definition of the marginal price of coin i is the average price of buying an infinitesimally small quantity of coin i ; *i.e.*,

$$\lim_{\varepsilon \downarrow 0} \frac{p(R', c, \varepsilon e_i)}{\varepsilon} = c_i,$$

where e_i is the i th unit vector, then the price reported matches the marginal price at reserves R' , as required.

A.3 Conjugate of reciprocal product

We show here that the convex function given by

$$f(x) = \left(\prod_{i=1}^n x_i \right)^{-1},$$

has a Fenchel conjugate given by

$$f^*(y) = \begin{cases} -(n+1) (\prod_{i=1}^n (-y_i))^{1/(n+1)} & y \leq 0 \\ +\infty & \text{otherwise.} \end{cases}$$

The proof is mostly mechanical. The definition of the Fenchel conjugate of the function f is given by

$$f^*(y) = \sup_x (y^T x - f(x)),$$

where $f(x)$ is extended in the natural way (*i.e.*, $f(x) = +\infty$ if $x_i \leq 0$ for any i). First, we show that if $y_i > 0$ for some i , then $f^*(y) = +\infty$. To do this, note that we can set $x_i = t$ and $x_j = 1$ for every j with $j \neq i$. Then sending $t \rightarrow \infty$, we get that $y^T x \rightarrow \infty$, while $f(x) \rightarrow 0$, implying the result.

Now we consider the case where $y \leq 0$. First, note that, in this case

$$y^T x - f(x) \leq 0,$$

for any x , since $x > 0$ and therefore $f(x) \geq 0$ (otherwise, if $x \not> 0$, we have $f(x) = +\infty$ by definition, so the claim is always satisfied). Now, if there exists some i with $y_i = 0$, then we can achieve this bound by setting $x_i = t^n$ and $x_j = 1/t$ for $j \neq i$. Sending $t \rightarrow \infty$ yields the result since $y^T x \rightarrow 0$ and $f(x) \rightarrow 0$.

The remaining case is when $y < 0$. Here, we can write the first order optimality conditions over x (which are sufficient and necessary by convexity and differentiability) after some simplifications:

$$x_i^* y_i = - \left(\prod_{j=1}^n x_j^* \right)^{-1}, \quad i = 1, \dots, n,$$

or, equivalently, that

$$x_i^* \prod_{j=1}^n x_j^* = \frac{1}{-y_i}, \quad i = 1, \dots, n.$$

This implies that x is collinear with the negative reciprocal of y , *i.e.*, that $x_i^* = \lambda/(-y_i)$, and, since $x^* \geq 0$, we must have $\lambda \geq 0$. This implies

$$\lambda^{n+1} = \prod_{i=1}^n (-y_i),$$

and therefore,

$$x_i^* = \frac{1}{-y_i} \left(\prod_{i=1}^n (-y_i) \right)^{\frac{1}{n+1}},$$

which implies that

$$y^T x^* - f(x^*) = -(n+1) \left(\prod_{i=1}^n (-y_i) \right)^{\frac{1}{n+1}},$$

completing the proof.