The Geometry of Constant Function Market Makers

Guillermo Angeris* gangeris@baincapital.com
Tarun Chitra tarun@gauntlet.network
Theo Diamandis tdiamand@mit.edu
Alex Evans aevans@baincapital.com
Kshitij Kulkarni ksk@eecs.berkeley.edu

July 2023

Abstract

Constant function market makers (CFMMs) are the most popular type of decentralized trading venue for cryptocurrency tokens. In this paper, we give a very general geometric framework (or 'axioms') which encompass and generalize many of the known results for CFMMs in the literature, without requiring strong conditions such as differentiability or homogeneity. One particular consequence of this framework is that every CFMM has a (unique) canonical trading function that is nondecreasing, concave, and homogeneous, showing that many results known only for homogeneous trading functions are actually fully general. We also show that CFMMs satisfy a number of intuitive and geometric composition rules, and give a new proof, via conic duality, of the equivalence of the portfolio value function and the trading function. Many results are extended to the general setting where the CFMM is not assumed to be path-independent, but only one trade is allowed. Finally, we show that all 'path-independent' CFMMs have a simple geometric description that does not depend on any notion of a 'trading history'.

Introduction

The study of automated market makers has existed for many decades, with roots in the scoring rule literature dating back to at least the 1950s [McC56]. However, these mechanisms only reached mass adoption after being implemented as decentralized exchanges on blockchains. Surprisingly, the types of automated market maker that are most popular in practice bear little resemblance to those proposed prior to the invention of blockchains. Instead, the most popular blockchain-based automated market makers are what are known as the *constant function market makers*, or CFMMs. These market makers are generally simpler than earlier market maker designs, such as those based on the logarithmic scoring

*The authors are listed in alphabetical order.

rule, and provide a means for efficient liquidity aggregation and order routing. But why have these mechanisms succeeded?

One of the main reasons that these mechanisms have been so popular in the cryptocurrency space is that solving the optimal arbitrage problem—the problem of how much to trade in order to equalize prices between CFMMs and other venues—is generally (computationally) 'easy' [AECB22]. This ease comes directly from the fact that CFMMs satisfy a general, very geometric, notion of convexity. Though the initial line of work, which defined CFMMs as a useful class, focused on their geometric properties [AC20], the majority of research on CFMMs has focused on analytic properties of CFMMs that depend on explicit parameterizations [LP21, WM22, MMR23a, SKM23, FPW23, MMR23b, GRGM23].

There are important reasons to examine geometry of CFMMs directly. First, a geometric lens leads to very natural statements for many of the properties of, and operations one can perform on, CFMMs. Second, many 'surprising' decisions made by developers that 'worked in practice' can be explained by understanding the geometry of CFMMs; for example, intuitively, the 'curvature' of a CFMM corresponds to a notion of liquidity [ACE22], which was known by practitioners well before its formalization. Third, the geometric setting for CFMMs is very general and rarely requires notions of differentiability, homogeneity, or other similar properties. Finally, the geometric view of CFMMs allows for reasoning about CFMMs without regards to its particular trading function and/or its representation.

What is a CFMM? CFMMs are relatively simple to describe analytically, which is likely why many researchers and practitioners work with them in this 'analytic' setting. A CFMM consists of two main objects: a trading function $\varphi : \mathbf{R}_+^n \to \mathbf{R}$ (sometimes called an 'invariant') and a vector of reserves $R \in \mathbf{R}_+^n$. A user proposes a trade, represented as a portfolio $\Delta \in \mathbf{R}^n$, and the trade is valid if the trading function, evaluated on the reserves after the trade is completed, has the same value as the function evaluated on the reserves before the trade is completed, *i.e.*, if $\varphi(R - \Delta) = \varphi(R)$. (Hence the name 'constant function market maker'.) If this equality holds, the CFMM then pays out Δ to the user and resulting in new reserves $R - \Delta$. (If the trade is invalid, nothing is paid out or received from the user.) Liquidity providers, who provide the reserves R against which trades are made, earn fees from these trades. The fact that this process is simple to describe and implement, along with having many strong theoretical guarantees, has been part of its reason for success, especially within difficult-to-secure environments such as public blockchains. Despite their simple description, CFMMs have spawned a large amount of research into their financial, arbitrage, and routing properties (*e.g.*, [AC20, DKP21, DRCA23, FMW23, MDP23], among many others).

Analytic vs. geometric properties. Many descriptions of CFMMs focus on a coordinate-dependent (or 'analytic') version of CFMMs, focusing on the representation of φ as an explicit function. For instance, Uniswap is commonly described via the trading function $\varphi(R) = \prod_{i=1}^n R_i$. However, there are a number of equivalent trading functions such as $\tilde{\varphi}(R) = (\prod_{i=1}^n R_i)^c$ for any $c > 0$. While the pricing and behavior is equivalent for these

different representations, the mechanics of many definitions hinge upon the specific representation provided. (Some might demand concavity or monotonicity, for example.) We call any properties that are dependent on the particular representation of the trading function *analytic* properties.

On the other hand, nearly by definition, geometric descriptions of CFMMs are unique and relatively simple to handle. For instance, there is a natural 'addition' operator for CFMMs using a geometric representation. Describing the corresponding operation on trading functions is not obvious and likely has no natural analogue. (We do show that there is another functional representation, given by the portfolio value function, that does have a natural correspondence.) This idea that certain operations such as addition, are 'easy' to perform on CFMMs, when defined geometrically, is one of the reasons that proofs using geometry can be significantly more succinct than those using analytic means.

This paper. In this paper, we focus on representing CFMMs via classical geometric objects such as convex sets and cones, assuming a bare minimum of requirements. Using these objects, we replicate the results of a number of papers for CFMMs without fees (also known as the 'path-independent' CFMMs) and many results in the case of a single trade with no restrictions on the CFMM. The key objects we look at are particular cones which we call the liquidity cones, and their corresponding conic duals. We construct many of the 'usual objects' such as trading functions, portfolio value functions, no arbitrage intervals, and so on, directly from these objects. This leads to a number of interesting results: for example, that every (path-independent) CFMM has a canonical trading function that is nondecreasing, concave, and homogeneous, along with new proofs for older, previously known results. We assume a reasonable amount of familiarity with convex optimization and provide a very short primer on conic duality in appendix A as a refresher.

1 Fee-free constant function market makers

In this section, we consider the general case of constant function market makers that are path-independent. We show the connection between these 'path-independent' or 'fee-free' constant function market makers and 'general' constant function market makers later, in §2.4. We consider this case first as this is the most common case in the literature [AC20, FPW23, GRGM23], and is a good starting point for the more general case.

Section layout. The section begins with a basic set of requirements (sometimes called 'axioms') which are of a different form than the standard assumptions made in many texts. We will show that from these requirements, which are mostly geometric in origin, we can derive many known results and a number of generalizations that, to our knowledge, are not known in the overall literature. For example, one important case is that any CFMM has a canonical trading function that is homogeneous, nondecreasing, and concave. This is usually taken as an assumption in some form (see, *e.g.*, [AEC21, FPW23, SKM23]), but we show here that it is true of any CFMM satisfying some basic properties that are essentially

necessary for a CFMM to be reasonable. (Indeed, these properties are almost always part of a much longer list, or are easy consequences of a subset of assumptions generally made in the literature.) This geometric set up also simplifies a number of known statements in the literature, such as those of [AEC23], by showing that the equivalence of a portfolio value function and a trading function is a special case of conic duality.

1.1 Reachable set

We will define the reachable set of reserves as a set $S \subseteq \mathbf{R}^n$ satisfying certain requirements. This set will represent the valid holdings of a constant function market maker (CFMM). In general, if $R \in S$ are the current reserves of the constant function market maker, then any trader may change the reserves to $R' \in S$ by selling $R' - R$ to the CFMM. The trader would then receive the entries of $R' - R$ which are negative, and tender the entries which are positive to the CFMM. In a certain sense, we may view the reachable set S as the set of valid states available to the contract.

Definition. We say a set S is a *reachable set* (which defines a fee-free, or 'path independent' CFMM) if it satisfies these rules or 'axioms':

1. All reserves are nonnegative; that is, $S \subseteq \mathbf{R}^n_+$
2. The set S is nonempty, closed, and convex
3. The set S is *upward closed*; *i.e.*, if $R \in S$, then any $R' \geq R$ has $R' \in S$

From these three rules, we will recover (and generalize) many of the results known in the literature. In general, while we do not assume that $0 \notin S$, we note that this is a silly case as we would then have $S = \mathbf{R}^n_+$, so this case is often excluded from many of the proofs presented.

High-level interpretation. The first requirement means that a constant function market maker cannot take on debt, or that the position is always solvent. Many, but not all, results hold with some slight modifications, even in the case where this condition is relaxed. The convexity requirement roughly corresponds to the fact that increasing the size of a trade does not result in a better exchange rate for the trader. The nonemptyness of S just means that S is nontrivial, while the closedness is a technical condition. Finally, the 'upwards closed' condition means that, if a CFMM accepts some trade, then it would always accept a different trade that tenders more of any asset. (This condition is not technically necessary: it suffices that, given a nonempty set S satisfying the first condition, the set $\tilde{S} = S + \mathbf{R}^n_+$ satisfies the second condition above. Almost all results shown below hold in this case.) The last condition also lets us interpret the boundary of S as a Pareto-optimal frontier for the possible reserves in the sense that no rational trader would ever trade on the interior of S.

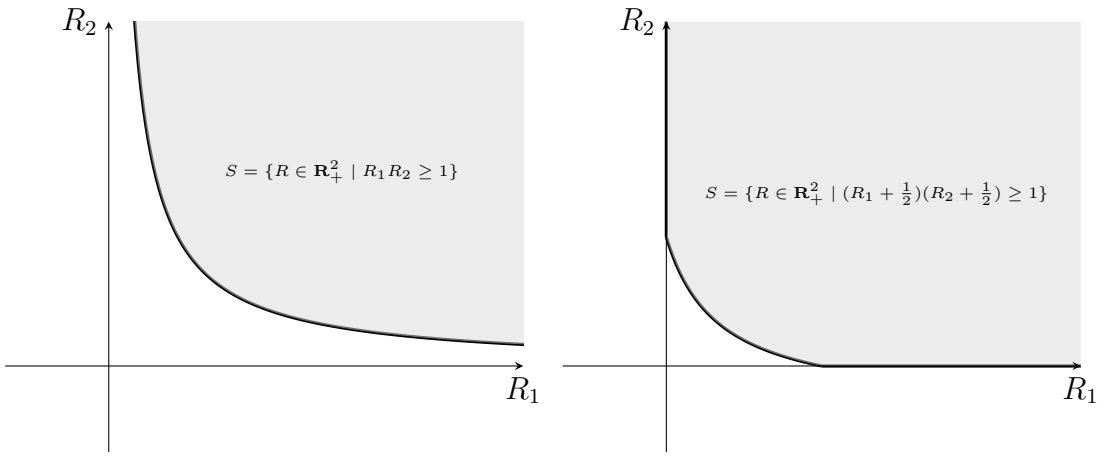

Figure 1: The set of reachable reserves for Uniswap (left) and Uniswap v3 (right).

Examples. One of the canonical examples of a reachable set is that of Uniswap [AZR20], defined

$$S = \{R \in \mathbf{R}_+^2 \mid R_1 R_2 \geq k\},$$

where $k > 0$ is a constant. See figure 1 for an example. Another example is that of a 'tick' in Uniswap v3 [AZS+21], which is defined

$$S = \{R \in \mathbf{R}_+^2 \mid (R_1 + \alpha)(R_2 + \beta) \geq k\},$$

where, again, $k > 0$ is some provided constant.

Quasiconcavity. Note that, in these examples, S is the superlevel set of some quasiconcave, nondecreasing function. In fact, we can show that any nonempty set S defined by

$$S = \{R \in \mathbf{R}_+^n \mid \psi(R) \geq \alpha\}, \tag{1}$$

with quasiconcave, nondecreasing $\psi : \mathbf{R}_+^n \to \mathbf{R} \cup \{+\infty\}$, generates a reachable set satisfying the required conditions. This includes [SKM23] and [FPW23] as a special case, though we do not require homogeneity. (Indeed, homogenity is not needed as an assumption as we will later show that one can always choose ψ to be concave, nondecreasing, and homogeneous for any set S satisfying the reachable set conditions, even when the 'original' function ψ is not.) We may also replace the inequality with an equality and define the set

$$S = \{R' \in \mathbf{R}_+^n \mid R' \geq R, \text{ for some } \psi(R) = \alpha\}.$$

Note that these two definitions are equivalent if ψ is continuous in some neighborhood $\psi^{-1}(N)$ where N is a neighborhood around α.

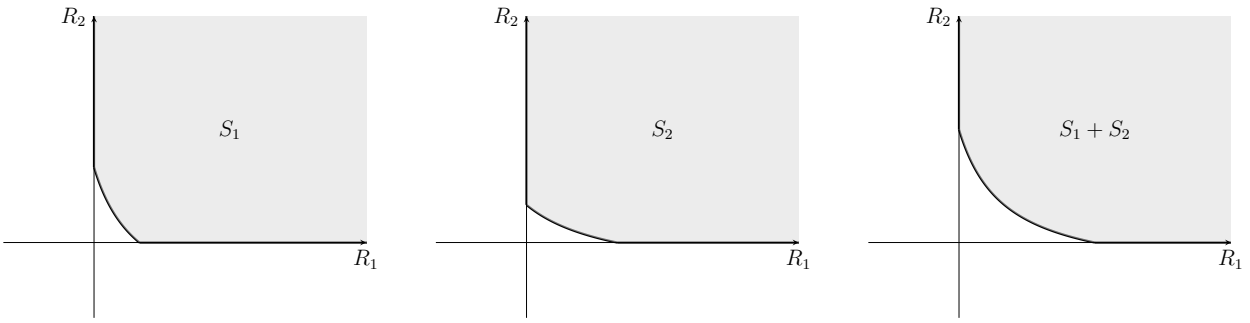

Figure 2: Adding two Uniswap v3 bounded liquidity pools (left, middle) gives us another CFMM (right).

1.2 Composition rules

An interesting consequence of the definition of reachable sets is that reachable sets, and therefore CFMMs, satisfy certain composition rules, some of which were known in the literature under special assumptions [EH21]. These rules follow directly from the calculus of convex sets [BV04, §2.3] and require no additional assumptions than those given in §1.1.

Nonnegative scaling. Given a reachable set S, we may scale the set by $\alpha \geq 0$ to get αS, which is another reasonable reachable set satisfying the conditions. (We will see later in §1.6 that this scaling corresponds to adding or removing liquidity to the CFMM.)

Set addition. We may also add any two reachable sets S and S', which gives another reachable set

$$S + S' = \{R + R' \mid R \in S,\ R' \in S'\}.$$

This set is convex and nonempty, and it is not hard to prove the set is closed since S and S' are both contained in the positive orthant. It is also clear that $S + S'$ is upward closed since each of S and S' are upward closed. These sums have the 'simple' interpretation that $S + S'$ are the possible combined holdings of the two CFMMs. Additionally, this, combined with nonnegative scaling, means that taking nonnegative linear combinations of trading sets always yields another trading set. We provide an example in figure 2.

Nonnegative matrix multiplication. Another important rule is that multiplication by a nonnegative matrix $A \in \mathbf{R}_+^{n\times p}$ and 'upwards closure' of the resulting set gives another reachable set; *i.e.*, the set

$$AS + \mathbf{R}_+^n = \{R' \in \mathbf{R}_+^n \mid R' \geq AR \text{ for some } R \in S\},$$

is a reachable set. This operation can be interpreted when looking at each row $j = 1, \ldots, n$ of A, which we write as $\tilde{a}_j^T$. Given some vector $R \in S$, then $\tilde{a}_j^T R = (AR)_j$. This entry, $(AR)_j$, can then be seen as a type of 'meta-asset', whose value is equal to a weighted basket of assets, where the weights are the entries of $\tilde{a}_j$. This is a reachable set since $AR \in \mathbf{R}_+^n$ for

any $R \in S \subseteq \mathbf{R}_+^n$ and AS is a convex set if S is convex. (The set is clearly upward closed by definition.)

Special case: projection. An important special case is when the matrix A projects all components of a trading set into a larger space. More specifically, let A be a matrix of the form

$$A = \begin{bmatrix} a_1 & a_2 & \cdots & a_k \end{bmatrix}$$

with $a_i \in \mathbf{R}^n$ and $k \leq n$ being all distinct unit basis vectors (*i.e.*, a_i is 0 everywhere except at exactly one entry, where it is 1). We can interpret $AS + \mathbf{R}_+^k$ in the following way: if there is a 'list' of n assets, and the CFMM defined by S trades only k of those assets, then AS is a CFMM which trades these k assets and zero of the remaining possible $n - k$ assets. (The CFMM will happily accept any of the remaining $n - k$ assets, but tender nothing for them: a trade no rational user would want.)

Intersection. Finally, we can take the intersection of reachable sets, which yields another reachable set; *i.e.*, if S and S' are reachable sets then $S \cap S'$ is similarly a reachable set. This corresponds to a CFMM whose reachable reserves can only be those which the individual CFMMs have in common. Though this is not a natural operation for CFMMs which already exist on chain, it is a useful theoretical operation for constructing CFMMs with particular properties. (Indeed, we will see that constructing a CFMM from a portfolio value function, to be presented later, is possible only due to this intersection property.)

Aggregate CFMMs. Combining the previous two rules gives us a very general way of 'combining' CFMMs which trade different (but potentially overlapping) baskets of assets. Assume we have m constant function market makers and a universe of n assets. We will have CFMMs $i = 1, \ldots, m$ with reachable sets $S_i \subseteq \mathbf{R}_+^{n_i}$, each trading a subset tokens of n_i tokens. We introduce matrices $A_i \in \mathbf{R}_+^{n \times n_i}$ which map the 'local' basket of n_i tokens for CFMM i to the global universe of n tokens. We have $(A_i)_{jk} = 1$ if token k in the market's local index corresponds to global token index j, and $(A_i)_{jk} = 0$ otherwise. We note that the ordering of tokens in the local index does not need to be the same as the global ordering. Then the set

$$\tilde{S} = \sum_{i=1}^{m} A_i S_i$$

is a *aggregate CFMM* which corresponds exactly to the set of all possible holdings for every CFMM in the network. Such CFMMs were first implicitly defined for Uniswap v3 [AZS+21], and later used in [CAE21] to prove some basic approximation bounds, while [MMR23a] defined a notion of 'complexity' based on similar ideas, and, finally [DRCA23] defined them as part of the solution method for optimal routing.

Extensions to negative reserves. There are some basic generalizations of some of these conditions in the case where the set S is not contained in the positive orthant. In this case,

the CFMM can take on debt. If the debt is unbounded, it is possible to create sets S and S' such that $S+S'$ is not closed, so the resulting set would not be a reachable set. On the other hand, it is not hard to show that allowing bounded debt (*i.e.*, there exists some $x \in \mathbf{R}^n_+$ such that $x + S \subseteq \mathbf{R}^n_+$) means that an analogous statement does still hold by a nearly identical proof.

1.3 Liquidity cone and canonical trading function

In this subsection we introduce the liquidity cone for a reachable set S. The liquidity cone is a kind of 'homogenized' version of the reachable set defined previously that simplifies a number of later derivations. Its definition will also suggest a canonical trading function: a trading function that corresponds to the reachable set S and is nondecreasing, homogeneous, and concave.

1.3.1 Liquidity cone

The *liquidity cone* for reachable set S is defined as

$$K = \mathbf{cl}\{(R, \lambda) \in \mathbf{R}^{n+1} \mid R/\lambda \in S,\ \lambda > 0\}, \tag{2}$$

where **cl** is the closure of the set. The set K is a cone as $(R, \lambda) \in K$ implies that $(\alpha R, \alpha\lambda) \in K$ for any $\alpha \geq 0$. The name 'liquidity cone' comes from the fact that, if $(R, \lambda) \in K$ then the largest such λ indicates, roughly speaking, the amount of liquidity available from reserves R. (We will see what this means in a later section.)

Basic properties. The liquidity cone K has some important properties we use later in this section. First, the set K is nonempty as S is nonempty and $S \times \{1\} \subseteq K$. We also have that $0 \in K$ as K is nonempty and closed. To see this, if $y \in K$ then $\alpha y \in K$, so $\alpha \downarrow 0$ gives the result. The cone K is also a convex cone as it is the closure of the perspective transform on the convex set $S \times \mathbf{R}_{++}$ (see, *e.g.*, [BV04, §2]).

Upward closedness. The cone K is not upward closed, but is 'almost upward closed' in the following sense: if $(R, \lambda) \in K$ and $R' \geq R$ with $\lambda' \leq \lambda$ then $(R', \lambda') \in K$. In particular, note that the inequality over λ is reversed. Showing this fact is just a definitional exercise.

Positive reachability. We also have that,

$$(\mathbf{R}^n_{++}, 0) \subseteq K. \tag{3}$$

This follows from the fact that the set S is nonempty. To see this, let $R \in S$ and note that, for any strictly positive vector $R' \in \mathbf{R}^n_{++}$ we know that $R'/\lambda \geq R$ for λ small enough, so $(R', \lambda) \in K$. Finally, since $(R', \lambda) \in K$ implies that $(R', \lambda') \in K$ for any $\lambda' \leq \lambda$, then we are done by setting $\lambda' = 0$. Roughly speaking, this corresponds to the intuitive fact that

every nonnegative basket is a feasible set of reserves, at some 'large enough' multiple. This observation is taken as an assumption in [FPW23] and [SKM23], but is a direct consequence of the definition of the reachable set. Additionally, since K is closed we have

$$(\mathbf{R}^n_+, 0) \subseteq K,$$

though this construction is less useful than the previous.

Reachable set. We may, of course recover the reachable set from the liquidity cone in a variety of ways. Perhaps the simplest is to note that, for any $\lambda > 0$ we have

$$S = \{R/\lambda \mid (R, \lambda) \in K\}. \tag{4}$$

This is easy to see as $(R, \lambda) = \lambda(R/\lambda, 1) \in K$, and, since K is a cone, this is if, and only if, $(R/\lambda, 1) \in K$ which is also if, and only if, $R/\lambda \in S$. This will be useful in what follows.

1.3.2 Canonical trading function

Given any liquidity cone K for a reachable set S, we will define a *canonical trading function*,

$$\varphi(R) = \sup\{\lambda \mid (R, \lambda) \in K\}, \tag{5}$$

setting $\varphi(R) = 0$ if the set is empty. (Since K is closed, we may replace the sup with a max if $0 \notin S$, which we assume for the remainder of the section.) In terms of the trading set S, we may write this as

$$\varphi(R) = \sup\{\lambda > 0 \mid R/\lambda \in S\},$$

using the definition of the liquidity cone K. If the reachable set S is written using a nondecreasing, quasiconcave, but not necessarily concave, function as in (1), then we can 'canonicalize' this trading function by writing

$$\varphi(R) = \sup\{\lambda > 0 \mid \psi(R/\lambda) \geq k\}. \tag{6}$$

Note that, if ψ is continuous, this is the same as finding the largest positive root over λ of $\psi(R/\lambda) = k$. If the function is strictly increasing (as is often the case) then the positive root is unique and it suffices only to find it. Figure 3 illustrates this definition for the case of Uniswap.

Computational considerations. It may be the case that the canonical trading function (6) has no closed form solution. From the previous, since we know that computing the value of the canonical trading function at some reserves R corresponds to a root-finding problem, we may do this using efficiently by using bisection (as ψ is assumed to be nondecreasing) or, if ψ is differentiable, using Newton's method for finding the positive root. In either case, computing $\varphi(R)$ can be done efficiently in practice. (As a side note: if bisection is used, it suffices to run it only until the bracketing interval is either fully contained in $[0, 1)$ or $[1, \infty)$. In the former, the reserves are guaranteed to be infeasible, while in the latter they are guaranteed to be feasible.)

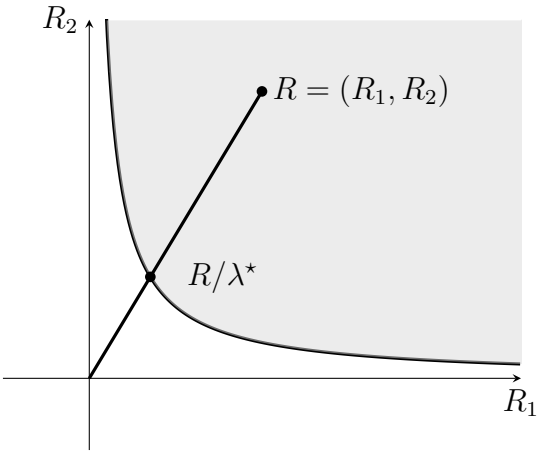

Figure 3: Another interpretation of the canonical trading function (5): we scale along the line segment defined by (R_1, R_2) to $(0, 0)$, with scale factor $1/\lambda$, increasing λ until we hit the reachable set boundary.

Reachable set. From (4) we can recover the set S from this canonical trading function since

$$S = \{R \in \mathbf{R}^n_+ \mid \varphi(R) \geq 1\}.$$

Additionally, note that if $\varphi(R) > 0$, which is always true if $R \in \mathbf{R}^n_{++}$ is strictly positive, from positive reachability (3), then

$$\frac{R}{\varphi(R)} \in S. \tag{7}$$

Concavity. This function is concave, as it is the partial maximization of the concave function

$$f(R, \lambda) = \lambda - I(R, \lambda)$$

over λ, where I is the indicator function of the (convex) set K, defined $I(R, \lambda) = 0$ if $(R, \lambda) \in K$ and $+\infty$ otherwise.

Homogeneity. The trading function φ is homogeneous for $\alpha > 0$ since

$$\varphi(\alpha R) = \sup\{\lambda \mid (\alpha R, \lambda) \in K\}.$$

Since K is a cone, then $(\alpha R, \lambda) \in K$ if, and only if, $(R, \lambda/\alpha) \in K$. Setting $\bar{\lambda} = \lambda/\alpha$, then we have

$$\varphi(\alpha R) = \sup\{\alpha\bar{\lambda} \mid (R, \bar{\lambda}) \in K\} = \alpha\varphi(R).$$

For $\alpha = 0$ the result follows since $0 \in K$.

Monotonicity. The trading function is nondecreasing from the 'almost upward closed' property mentioned previously. For the remainder of the paper, we will call a function that is nondecreasing, homogeneous, and concave, a *consistent* function.

Marginal prices. Given R with $\varphi(R) = 1$, *i.e.*, the starting reserves are 'reasonable' and φ differentiable at R, then, from concavity,

$$\varphi(R + \Delta) \leq \varphi(R) + \nabla\varphi(R)^T \Delta.$$

(We may replace the gradient with a supergradient for a more general condition.) If the trade Δ is feasible in that $\varphi(R + \Delta) \geq \varphi(R)$ then

$$\nabla\varphi(R)^T \Delta \geq 0.$$

Note that this means that $\nabla\varphi(R)$ is a supporting hyperplane of S at R if $\varphi(R) = 1$. If the trader is trading some amount of asset i for asset j, *i.e.*, $\Delta_i > 0$ and $\Delta_j < 0$ with all other entries zero, we have

$$(\nabla\varphi(R))_j \Delta_j \leq -(\nabla\varphi(R))_i \Delta_i,$$

or, rewriting further,

$$\Delta_j \leq \frac{(\nabla\varphi(R))_i}{(\nabla\varphi(R))_j}(-\Delta_i).$$

Where equality can be achieved in the limit as the trade becomes small. We can therefore interpret the quantity $(\nabla\varphi(R))_i/(\nabla\varphi(R))_j$ as the price of token j with respect to token i, and we can interpret the vector $\nabla\varphi(R)$ as a vector of prices, up to a scaling factor determined by the numeraire.

Discussion. This shows that a number of results which hold 'only' for homogeneous trading functions, such as those of [FPW23, AEC21], are fully general and hold for all CFMMs. Indeed, we do not need to assume homogeneity at all as it may always be derived for a trading set satisfying some basic conditions given above. Additionally, the direct connection to constant function market makers comes from the fact that any trader may change the reserves to some $R' \in \mathbf{R}_+$ so long as

$$\varphi(R') \geq \varphi(R) = 1,$$

where we assume that $\varphi(R) = 1$ is a 'starting condition' on the level set. Of course, no trader would ever take $\varphi(R') > 1$, since otherwise there exists some dominating trade $\tilde{R}' \leq R'$ with at least one inequality holding strictly; *i.e.*, the trader would tender less (or get more) of at least one token and still have a feasible trade. So, in general, we have that, for any 'reasonable' action,

$$\varphi(R') = \varphi(R), \tag{8}$$

where R' is the new set of reserves, after a trade has been made, and R is the original set of reserves. Equation (8) is the defining equation for path-independent constant function market makers, explaining both their name and the direct connection to the reachable set defined here. (See [AAE+22] for more.)

1.3.3 Uniqueness of canonical trading function

We call this trading function *canonical* since it is unique up to a scaling constant. In fact, this function is unique if the function is scaled such that the reachable set corresponds to its 1-superlevel set.

Proof. To see this, let φ and $\tilde{\varphi}$ be two trading functions that are consistent and yield the same reachable set S; *i.e.*,

$$S = \{R \in \mathbf{R}_+^n \mid \varphi(R) \geq \alpha\} = \{R \in \mathbf{R}_+^n \mid \tilde{\varphi}(R) \geq \beta\},$$

where $\alpha, \beta > 0$. (If $\alpha = 0$ then, since φ is homogeneous and nondecreasing, we have that $\varphi(R) \geq 0$, which would imply that its reachable set is all of $\mathbf{R}_+^n$, and similarly for $\tilde{\varphi}$.) This is the same as

$$\{R \mid \varphi(R)/\alpha \geq 1\} = \{R \mid \tilde{\varphi}(R)/\beta \geq 1\},$$

so we will overload notation by writing φ for φ/α and $\tilde{\varphi}$ for $\tilde{\varphi}/\beta$, with the understanding that these differ by a proportionality constant. Now, we will show that $\varphi = \tilde{\varphi}$. To see this, start with the case that R satisfies $\varphi(R) > 0$ and $\tilde{\varphi}(R) > 0$, then

$$\varphi\left(\frac{R}{\varphi(R)}\right) = 1,$$

so $R/\varphi(R) \in S$ and we then have, by definition of $\tilde{\varphi}$,

$$\frac{\tilde{\varphi}(R)}{\varphi(R)} = \tilde{\varphi}\left(\frac{R}{\varphi(R)}\right) \geq 1.$$

Repeating the steps above with φ and $\tilde{\varphi}$ swapped yields

$$\varphi(R) = \tilde{\varphi}(R),$$

when $\varphi(R) > 0$ and $\tilde{\varphi}(R) > 0$. Now, if $\varphi(R) = 0$ then

$$\varphi(tR) = t\varphi(R) = 0,$$

so $tR \notin S$ for any $t > 0$. This means that

$$t\tilde{\varphi}(R) = \tilde{\varphi}(tR) < 1,$$

again by definition of $\tilde{\varphi}$, or, that $\tilde{\varphi}(R) < 1/t$ for any $t > 0$, so $\tilde{\varphi}(R) = 0$. Repeating these steps where φ is swapped with $\tilde{\varphi}$ implies that $\varphi(R) = 0$ only when $\tilde{\varphi}(R) = 0$. This gives the final result that $\varphi = \tilde{\varphi}$, or that the canonical function is unique up to scaling constants.

1.3.4 Examples

In this subsection, we show the canonical trading function for Uniswap and Uniswap v3.

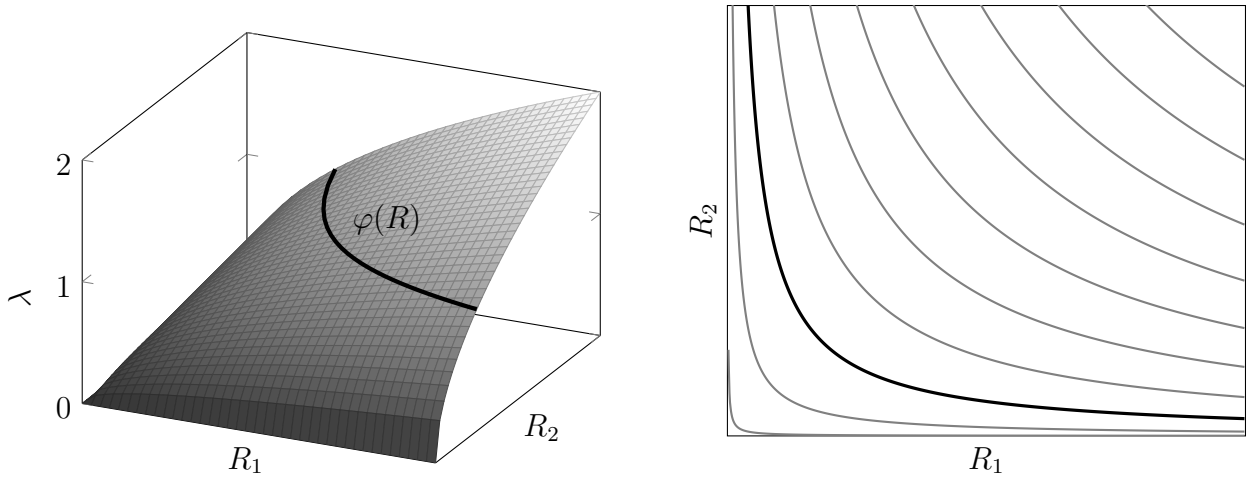

Figure 4: Left: the liquidity cone for Uniswap, with the level set defined by the trading function $\varphi(R) = \sqrt{R_1 R_2} = 1$ shown. Right: each λ-level set of the surface looks like the boundary of the set of reachable reserves (see figure 1). The trading function φ is highlighted.

Uniswap. Starting with the usual example of Uniswap (v1/v2), we have that

$$S = \{R \in \mathbf{R}_+^2 \mid R_1 R_2 \geq k\}.$$

The liquidity cone for Uniswap is given by

$$K = \{(R, \lambda) \in \mathbf{R}^3 \mid R_1 R_2 / \lambda^2 \geq k \in S,\ \lambda > 0\} \tag{9}$$

so, the canonical trading function (6) can be written

$$\varphi(R) = \sup\{\lambda > 0 \mid R_1 R_2 / \lambda^2 \geq k\},$$

when $R \in \mathbf{R}_+^2$ (and zero otherwise). This gives the canonical trading function

$$\varphi(R) = \sqrt{\frac{R_1 R_2}{k}},$$

which is evidently concave, nondecreasing, and 1-homogeneous, with

$$\varphi(R) \geq 1 \quad \text{if, and only if} \quad R_1 R_2 \geq k,$$

as required. The liquidity cone and canonical trading function are shown in figure 4.

Uniswap v3. We can also do the same for Uniswap v3, which has a quasiconcave trading function given by

$$\psi(R) = (R_1 + \alpha)(R_2 + \beta).$$

Since ψ is strictly increasing in the positive orthant, it suffices only to find the (positive) root of

$$(R_1/\lambda + \alpha)(R_2/\lambda + \beta) = k,$$

which is a simple quadratic. The resulting canonical trading function is unfortunately more complicated:

$$\varphi(R) = \frac{1}{2}\left(\frac{\beta R_1 + \alpha R_2 + \sqrt{(\beta R_1 + \alpha R_2)^2 + 4(k - \alpha\beta)R_1 R_2}}{k - \alpha\beta}\right). \tag{10}$$

This function is evidently homogeneous and strictly increasing since $k > \alpha\beta$. Concavity is more difficult due to the square root term, but we show it directly in appendix C. A good exercise is to show that the canonical trading function φ in (10) has $\varphi(R) \geq 1$, if, and only if, $(R_1 + \alpha)(R_2 + \beta) \geq k$.

1.4 Dual cone and portfolio value function

In this section, we will look at an equivalent characterization of the liquidity cone K, called the dual cone. The characterizations are equivalent since the liquidity cone K is convex. Indeed, we will show that this dual cone has a very tight relationship with the portfolio value function, and leads to a simple proof of the equivalence of (consistent) portfolio value functions and (canonical) trading functions in that every portfolio value function has a corresponding trading function, and vice versa, which was originally derived in [AEC23].

1.4.1 Dual cone

The *dual cone* of a cone $K \subseteq \mathbf{R}^{n+1}$ is defined as

$$K^* = \{(c, \eta) \in \mathbf{R}^{n+1} \mid c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in K\}.$$

While this definition holds for any cone K, for the remainder of this section, we will be working with the case that K is the liquidity cone of a CFMM with reachable set S, as defined the previous subsection.

Intuition. In a very general sense, the dual cone K^* is simply another (dual) representation of the original liquidity cone, K, in that the dual of K^*, defined as $(K^*)^* = K$, as K is closed and convex. (For more information on conic duality, we refer the reader to appendix A.) We will use this fact to give a simple proof that the trading function and the portfolio value function (to be introduced later in this section) are two views of the same underlying object.

Basic properties. First, note that K^* is always a closed, convex cone as it can be written as the intersection of closed hyperplanes, and, by definition, we have $0 \in K^*$. Additionally, we have that

$$K^* \subseteq \mathbf{R}^n_+ \times \mathbf{R} \tag{11}$$

since $K \supseteq \mathbf{R}^n_{++} \times \{0\}$, from the previous section. (To see this, use the definition of K^*.) Finally, we may write the dual cone in terms of only the reachable set S. We have that $(c, \eta) \in K^*$ if, and only if,

$$c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in K,$$

by definition. But this latter statement is true if, and only if it is true for all $\lambda > 0$, since K is the closure over the set defined in (2); *i.e.*, $(c, \eta) \in K^*$ if, and only if,

$$c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in K, \ \lambda > 0.$$

Rearranging the inequality gives that $c^T(R/\lambda) + \eta \geq 0$, and note that, by definition of K, we have that $(R, \lambda) \in K$ with $\lambda > 0$ only when $R/\lambda \in S$. This means that $(c, \eta) \in K^*$ if, and only if,

$$c^T \tilde{R} + \eta \geq 0, \text{ for all } \tilde{R} \in S. \tag{12}$$

This particular rewriting of K^* will be useful in what follows.

1.4.2 Portfolio value function

Much in the same way that we defined the trading function, we may define the *portfolio value function* as

$$V(c) = \sup\{-\eta \mid (c, \eta) \in K^*\}. \tag{13}$$

This function has the following interpretation: given an external market with prices $c \in \mathbf{R}^n_+$ (*i.e.*, anyone may trade asset i for asset j for a fixed price c_i/c_j) then $V(c)$ corresponds to the total value of reserves after arbitrage has been performed. In particular, $V(c)$ is the optimal value of the problem,

$$\begin{array}{ll} \text{minimize} & c^T R \\ \text{subject to} & R \in S, \end{array} \tag{14}$$

with variable $R \in \mathbf{R}^n$, where S is the reachable set.

To see this, note that $(c, \eta) \in K^*$ if, and only if,

$$c^T R \geq -\eta, \text{ for all } R \in S,$$

from the previous characterization of K^* given in (12). The claim follows by applying the definition of V in (13).

Properties. From the optimization problem formulation (14), we see that V is clearly nonnegative and nondecreasing since for any $R \in S$, we have that $R \geq 0$. The function V is also concave because it is the partial maximization of the concave function

$$f(c, \eta) = -\eta - I(c, \eta),$$

over η, where I is the indicator function of the convex set K^*, defined as $I(c, \eta) = 0$ if $(c, \eta) \in K^*$ and $+\infty$, otherwise. Finally, we see that V is homogenous since for $\alpha > 0$, $V(\alpha c)$ is the optimal value of the problem

$$\begin{array}{ll} \text{minimize} & \alpha c^T R \\ \text{subject to} & R \in S. \end{array}$$

Since α is a constant, this value is clearly $\alpha V(c)$.

Consistency. We say a portfolio value function is *consistent* if it is concave, homogeneous, and nondecreasing, which we know is true for any function V derived from a reachable set S. Of course, every consistent portfolio value function also defines a dual cone:

$$K^* = \{(c, \eta) \mid V(c) + \eta \geq 0\},$$

which can be easily verified to be a convex cone that is contained in $K^* \subseteq \mathbf{R}^n_+ \times \mathbf{R}$ using the fact that V is consistent, so we may convert from portfolio value functions to dual cones directly.

Examples. Using (9), we can write the dual cone for Uniswap

$$K^* = \{(c, \eta) \mid c^T R + \eta\lambda \geq 0, \text{ for all } R_1 R_2 \geq k\lambda^2, \ \lambda > 0\}.$$

We can simplify this expression via a few observations. First, we must have $c \geq 0$, from (11). Second, because $c \geq 0$, if $\eta \geq 0$ then (c, η) is clearly in K^*. The interesting case is then when $c \geq 0$ but $\eta < 0$. In this case, we must have that

$$c^T R \geq (-\eta)\sqrt{\frac{R_1 R_2}{k}},$$

since λ can take any value between 0 and $\sqrt{R_1 R_2/k}$. Rearranging, we have that

$$c_1 x + c_2 x^{-1} \geq (-\eta)/\sqrt{k},$$

where $x = \sqrt{R_1/R_2}$. Minimizing the left hand side over $x > 0$ means that this inequality is true if, and only if,

$$2\sqrt{c_1 c_2} \geq -\eta/\sqrt{k},$$

so the dual cone for Uniswap is

$$K^* = \{(c, \eta) \in \mathbf{R}^2_+ \times \mathbf{R} \mid 2\sqrt{k c_1 c_2} + \eta \geq 0\}.$$

The portfolio value function can almost be read off from the definition:

$$V(c) = 2\sqrt{k c_1 c_2}, \tag{15}$$

which is evidently homogeneous, nondecreasing, and concave.

As a more complicated example, we'll derive the portfolio value function for a Uniswap v3 'tick'. In this case, it's easier to work directly from the optimization problem (14). For convenience, let $c = (p, 1)$ and note that we can recover the general case using the homogeneity of V, as $V(\tilde{c}) = \tilde{c}_2 V(\tilde{c}_1/\tilde{c}_2, 1)$. Then,

$$V(p, 1) = \inf_{R \geq 0} \{pR_1 + R_2 \mid (R_1 + \alpha)(R_2 + \beta) \geq k\}.$$

Any profit maximizing trader will ensure that the inequality holds with equality (*i.e.*, the solution is at the boundary of the set S). After substitution, we have a simple convex

function that is minimized either at a point $R > 0$ with gradient zero or at the boundary. We can conclude that

$$V(p,1) = \begin{cases} pk/\alpha - \beta & p < \beta^2/k \\ 2\sqrt{pk} - (\alpha+\beta) & \beta^2/k \leq p \leq k/\alpha^2 \\ pk/\beta - \alpha & k/\alpha^2 < p. \end{cases}$$

Note the similarity of this expression to the previous (15) when the price is within a particular range. This range corresponds exactly to the 'tick' interval in Uniswap v3 [AZS+21].

1.4.3 Replicating market makers

In this subsection we show how to convert directly between the portfolio value function and a canonical trading function (and vice versa). This shows that, indeed, every canonical trading function has an equivalent consistent portfolio value function, and, in a sense, each of these functions is a different 'view' of the same underlying object.

Trading function to portfolio value. Assuming φ is a canonical trading function, as defined in (5), then we may write the portfolio value function as

$$V(c) = \inf_{R>0} \left(\frac{c^T R}{\varphi(R)} \right).$$

To see this, note that the definition of K^* is that $(c, \eta) \in K^*$ when

$$c^T R + \eta\lambda \geq 0, \text{ for all } (R, \lambda) \in K.$$

Minimizing the left hand side over $\lambda > 0$ gives that $(c, \eta) \in K^*$ only when

$$c^T R + \eta\varphi(R) \geq 0, \text{ for all } R \in \mathbf{R}^n_+,$$

by definition of $\varphi(R)$. Using a basic limiting argument, we may replace $R \in \mathbf{R}^n_+$ with $R \in \mathbf{R}^n_{++}$, which implies that $\varphi(R) > 0$ by positive reachability (3), so we have that

$$-\eta \leq \frac{c^T R}{\varphi(R)}, \text{ for all } R \in \mathbf{R}^n_{++},$$

or, equivalently, that $(c, \eta) \in K^*$ if, and only if,

$$-\eta \leq \inf_{R>0} \left(\frac{c^T R}{\varphi(R)} \right).$$

Applying the definition of $V(c)$, given in (13), gives the final result.

Trading function from portfolio value. It is also possible to show that we can recover a canonical trading function from a given portfolio value function. To see this, note that

$$\varphi(R) = \inf_{c>0} \left(\frac{c^T R}{V(c)} \right), \tag{16}$$

is a concave, nondecreasing, homogeneous trading function. We can easily show that, if K^* corresponds to the dual of a liquidity cone K, and V is the corresponding portfolio value function, then $\varphi(R)$ corresponds to its canonical trading function.

From a nearly-identical argument to the previous, replacing the definition of φ with that of V, we have that $(\tilde{R}, \tilde{\lambda}) \in (K^*)^*$ if, and only if,

$$\tilde{\lambda} \leq \inf_{c>0} \left(\frac{c^T \tilde{R}}{V(c)} \right).$$

Since K is a liquidity cone (by assumption) it is therefore closed and convex, so we have that $(K^*)^* = K$; *cf.*, appendix A. Finally, maximizing over $\tilde{\lambda}$ and using the definition of φ given in (5):

$$\varphi(\tilde{R}) = \inf_{c>0} \left(\frac{c^T \tilde{R}}{V(c)} \right),$$

where φ is the canonical trading function for K.

Example. To complete the cycle, we convert the portfolio value function of Uniswap v2 back to its canonical trading function. From above,

$$\begin{aligned}
\varphi(R) = \inf_{c>0} \left(\frac{c^T R}{V(c)} \right) &= \frac{1}{2\sqrt{k}} \inf_{c>0} \left(\sqrt{\frac{c_1}{c_2}} R_1 + \sqrt{\frac{c_2}{c_1}} R_2 \right) \\
&= \frac{1}{2\sqrt{k}} \inf_{x>0} \left(x R_1 + x^{-1} R_2 \right) \\
&= \sqrt{\frac{R_1 R_2}{k}},
\end{aligned}$$

where we recognized $xR_1 + x^{-1}R_2$ as a convex function and minimized by simply applying the first order optimality conditions.

Interpretation. There is a nice interpretation for equation (16) which is that the quotient $c^T R / V(c)$ denotes the *leverage* or the 'lambda' of the portfolio $R \in \mathbf{R}^n_+$ at price c, where $V(c)$ denotes the true value of the CFMM holdings at this price. We may then view the trading function $\varphi(R)$ as the lowest possible leverage over all possible prices. The inequality $\varphi(R) \geq 1$, which defines the reachable set, says that the leverage must be at least 1 in order for the reserves to lie in the set.

Connection to RMMs. There is a connection to the original result of [AEC23] by noting that the trading function presented there is defined, using the portfolio value function V, as

$$\varphi^0(R) = \inf_{c>0} \left(c^T R - V(c)\right) = -I_{(K^*)^*}(R, 1),$$

where $I_{(K^*)^*}$ is the indicator function for the dual cone of the dual cone, $(K^*)^*$. Since $(K^*)^* = K$ then $\varphi^0(R) \geq 0$ if, and only if, $(R, 1) \in K$, which happens if, and only if, $R \in S$, as required.

Discussion. From the above, we have that every consistent portfolio value leads to a canonical trading function. This method gives a general procedure for going from one to the other. Additionally, since we know $((K^*)^*)^* = K^*$, then we know that, starting from any consistent portfolio value function V, converting it to a trading function φ, and then converting back results in the same V we started with, which shows that the mapping is indeed invertible.

1.4.4 Composition rules

We will denote $S_V \subseteq \mathbf{R}^n_+$ as the reachable set corresponding to the portfolio value function V. (We will see how to construct this explicitly in what follows.)

Composition rules for portfolio value. Given consistent portfolio value functions, there are a number of possible ways these could be 'combined'. The first is by scaling: if V is consistent, then certainly αV is consistent. If both V and V' are consistent, then $V + V'$ is consistent, and, finally if A is a nonnegative orthogonal matrix, and V is consistent, then $V \circ A^T$ is consistent. We will show that these operations correspond to natural operations over the reachable sets corresponding to the portfolio value functions.

Recovering the reachable set. We may recover the reachable set from a given portfolio value function since we know that, for given portfolio value function, its liquidity cone, which we will denote $K_V \subseteq \mathbf{R}^{n+1}$ is

$$K_V = \{(R, \lambda) \in \mathbf{R}^{n+1} \mid c^T R - \lambda V(c) \geq 0 \text{ for all } c \geq 0\}.$$

Clearly, this cone is convex, closed, and satisfies $K_V \subseteq \mathbf{R}^{n+1}_+$ from the fact that V is consistent. Additionally, since we may define a reachable set from a liquidity cone as $S_V = \{R \mid (R, 1) \in K_V\}$, then this is the same as saying

$$S_V = \{R \mid c^T R \geq V(c) \text{ for all } c \geq 0\}. \tag{17}$$

It remains to be verified that S_V is a valid reachable set, but this follows from the properties of K_V outlined above. (Another way to see this is to note that $c^T R \geq V(c)$ if, and only if, $c^T R / V(c) \geq 1$ for all $c > 0$, *i.e.*, $\varphi(R) \geq 1$ using (16). Since φ is a canonical trading function, then S_V is a reachable set.)

Scaling. It is not hard to see that

$$S_{\alpha V} = \alpha S_V,$$

for any $\alpha \geq 0$ by using the definition of S_V and the fact that V is homogeneous.

Addition. Similarly, addition over the portfolio value functions 'commutes' over the reachable sets; *i.e.*,

$$S_{V+V'} = S_V + S_{V'}.$$

The direction $S_{V+V'} \subseteq S_V + S_{V'}$ is easy to show by definition. On the other hand, since $S_{V+V'}$ is a closed convex set, if $R \notin S_{V+V'}$ then there exists a strictly separating hyperplane $c \in \mathbf{R}^n_+$ with

$$c^T R < c^T \tilde{R}, \text{ for all } \tilde{R} \in S_{V+V'}.$$

Taking the infimum of the right hand side and using (14) gives

$$c^T R < (V + V')(c) \leq c^T \tilde{R} + c^T \tilde{R}' \text{ for all } \tilde{R} \in S_V,\ \tilde{R}' \in S_{V'},$$

which means that $R \notin S_V + S_{V'}$. Here, the last inequality follows from the fact that $V(c) \leq c^T \tilde{R}$ for all $\tilde{R} \in S_V$ and similarly for $S_{V'}$. Putting both statements together gives that $S_{V+V'} = S_V + S_{V'}$.

Nonnegative projection. Given some nonnegative matrix $A \in \mathbf{R}^{m\times n}_+$ that is also an orthogonal matrix, *i.e.*, $A^T A = I$, then

$$S_{V\circ A^T} = AS_V + \mathbf{R}^m_+,$$

where $(V \circ A^T)(c) = V(A^T c)$. This follows nearly immediately from the definition of A and (17).

Intersection. There is a natural question then, as to what the intersection of reachable sets corresponds to. Clearly, we have

$$S_V \cap S_{V'} = \{R \mid c^T R \geq V(c) \text{ and } c^T R \geq V'(c)\}.$$

Of course, this implies that

$$S_V \cap S_{V'} = S_{\max\{V,V'\}},$$

where the max is taken pointwise. Note that this does not correspond to a natural operation on the portfolio value functions as the pointwise maximum of two concave functions is not necessarily concave. (Take, for example, $V(p,1) = \sqrt{p}$ and $V'(p,1) = p$.) Let, on the other hand, $\tilde{V}$ be the (pointwise) smallest concave function with $\tilde{V} \geq V$ and $\tilde{V} \geq V'$, then indeed we have

$$S_V \cap S_{V'} = S_{\tilde{V}},$$

and it is not hard to show that $\tilde{V}$ is consistent.

Discussion. This also gives another proof of the composition rules presented for the reachable sets since we may always recover a consistent portfolio value from any reachable set. In this sense, we may think of the portfolio value function and the reachable set as two objects with a 'natural homomorphism' under which scaling, addition, nonnegative projection, and intersection are all preserved.

1.5 Connection to prediction markets

Prediction markets are a type of market which attempts to elicit the beliefs of players about the probability that certain events occur. These markets have a rich academic history, stemming back since at least the 50s [McC56] and, until the relatively recent paper [FPW23], a connection between such markets and CFMMs was not known, except in some very special cases. This section restates and simplifies the results of [FPW23] in this framework. We differ in the notion of 'histories' for path-independent CFMMs which is implicitly included in this framework and discussed later in this paper, as a general result in §2.4.

Cost functions. A *cost function* is defined as a function $C : \mathbf{R}^n \to \mathbf{R} \cup \{+\infty\}$ such that

1. The function C is convex, nondecreasing
2. It is translation invariant, $C(q + \alpha\mathbf{1}) = C(q) + \alpha$
3. It is somewhere finite; *i.e.*, there is at least one q for which $C(q)$ is finite

Note that we do not require the function to be differentiable, only subdifferentiable in its domain. This means that there might be many probabilities which are consistent with the market's predictions, but includes differentiability as the special case where there is only one.

Example. One particular, important example is the logarithmic market scoring rule, or LMSR, which has cost function

$$C(q) = b \log \left(\sum_{i=1}^{n} \exp \left(\frac{q_i}{b} \right) \right),$$

where $b > 0$ is some given constant. This function is clearly nondecreasing and finite. It is also convex as it is a log-sum-exp [BV04, §3.1.5] function with affine precomposition. It is not hard to see that this function is also translation invariant using the definition, which means that this function is, indeed, a reasonable cost function.

Mechanics. The mechanics of a prediction market are that any player may buy any of n possible mutually exclusive outcomes. Every player will be paid a dollar for each share of outcome i they hold if outcome i occurs at some future time. All other outcomes will have a value of zero. A player who wishes to buy $\delta \in \mathbf{R}^n$ shares and must pay a cost of

$C(q+\delta) - C(q)$, where q is the current set of outstanding shares that have been sold to all players. (Negative values of δ_i means that the player is selling back δ_i shares to the market.) The outstanding shares are then updated to $q \leftarrow q + \delta$.

Interpretation. Let's say the prediction market begins with some outstanding shares q_0, and a player has beliefs $p \in \mathbf{R}^n_+$ about the probability of each event such that p_i corresponds to the probability of the ith event occurring. The player can then maximize her expected profit (under her distribution of beliefs) by solving

$$\text{maximize} \quad p^T q - (C(q_0 + q) - C(q_0)),$$

with variable q. We note that the optimal value of this problem, call it $E(p)$ for expected payoff at probabilities p, is tightly related to the Fenchel conjugate of C, since

$$E(p) = C^*(p) + C(q_0) - p^T q_0.$$

The optimality conditions for this problem are that

$$p \in \partial C(q_0 + q^\star),$$

where $q^\star$ is the solution to the optimization problem. This means that, if the market has some outstanding shares given by q_0 then we may interpret $\partial C(q_0)$ as the set of probabilities consistent with the market's belief about the event.

CFMM to cost function. Given a reachable set S, we can construct a cost function:

$$C(q) = \min\{\alpha \geq 0 \mid \alpha \mathbf{1} - q \in S\}. \tag{18}$$

(This was first observed by [FPW23].) We may also define the cost function in terms of the liquidity cone as

$$C(q) = \max\{\beta \geq 0 \mid (\mathbf{1} - \beta q, \beta) \in K\}.$$

This function is a cost function since it is evidently translation invariant by definition, and is nondecreasing since S is upward closed. The function is finite at 0 since S is nonempty: if $R \in S$, then $0 \leq C(0) \leq \max_i R_i$. Additionally, this function is convex as it is the partial minimization of the convex function

$$f(\alpha, q) = \alpha - I(\alpha, q),$$

over $\alpha \in \mathbf{R}$, where $I(\alpha, q) = 0$ if $\alpha \mathbf{1} - q \in S$ and $\alpha \geq 0$, and is $+\infty$ otherwise. (This set indicator is convex as it is the indicator function for the intersection of convex sets.)

Example. Recall that Uniswap has the trading set

$$S = \{R \in \mathbf{R}^2_+ \mid R_1 R_2 \geq k\}$$

Using (18), we have the cost function

$$C(q) = \min\{\alpha \geq 0 \mid (\alpha - q_1)(\alpha - q_2) \geq k\}.$$

The cost function is the positive root of the quadratic over α, the same as was found in [FPW23]:

$$C(q) = \frac{q_1 + q_2}{2} + \frac{1}{2}\sqrt{(q_1 - q_2)^2 + k}.$$

We can easily verify that this function is finite, translation invariant, and convex (by noting that the square root term can be expressed as the ℓ_2 norm of the vector $(q_1 - q_2, \sqrt{k})$). The fact that it is nondecreasing can be seen by showing that its gradient is everywhere nonnegative.

Cost function to CFMM. Any cost function C defines a CFMM by defining its reachable set as,

$$S = \{R \in \mathbf{R}^n_+ \mid C(-R) \leq 0\}. \tag{19}$$

This S is indeed a reachable set as (a) the function C is nondecreasing by assumption, so S is upward closed, (b) it is convex as C is convex, and (c) it is nonempty since $C(q)$ is finite for some $q \in \mathbf{R}^n$, so $C(q - C(q)\mathbf{1}) = 0$ by translation invariance, and therefore $C(q)\mathbf{1} - q \in S$. We may write its canonical trading function using (6):

$$\varphi(R) = \sup\{\lambda > 0 \mid C(-R/\lambda) \leq 0\}.$$

Equivalence. If the cost function C is constructed from a CFMM with reachable set S, as in (18), then it is not hard to show that (19) yields exactly this set S. To see this, note that, by definition (18), we have that $C(-R) \leq 0$, if, and only if, $\alpha\mathbf{1} + R \in S$ for all $\alpha \geq 0$; letting $\alpha = 0$ gives that $R \in S$. On the other hand, if $R \in S$ then, $R + \alpha\mathbf{1} \in S$ for every $\alpha \geq 0$, by upward closedness, so $C(-R) \leq 0$ and the sets are equivalent.

Example. The logarithmic market scoring rule (LMSR) has the cost function

$$C(q) = b \log\left(\sum_{i=1}^{n} \exp\left(\frac{q_i}{b}\right)\right).$$

We may define its trading set, using (19), as

$$S = \left\{ R \in \mathbf{R}^n_+ \;\middle|\; \sum_{i=1}^{n} \exp(-R_i/b) \leq 1 \right\}.$$

The corresponding canonical trading function is

$$\varphi(R) = \sup\left\{\lambda > 0 \;\middle|\; \sum_{i=1}^{n} \exp(-R_i/\lambda b) \leq 1\right\}$$

This function has no closed form solution but can be solved numerically as a univariate root-finding problem. Since C is strictly increasing, the positive root is unique and can be found efficiently using the methods discussed in §1.3.2.

1.6 Liquidity provision

As in [AAE+22], we discuss liquidity provision in the case where the trading function φ is homogeneous. This is, of course, fully general as we may assume that φ is a consistent trading function.

Liquidity providers. An agent, called a *liquidity provider* can add or remove assets from the CFMM's reserves R. When an agent adds liquidity, she adds a basket $\Psi \in \mathbf{R}^n_+$ to the reserves, resulting in the updated reserves $R^+ = R + \Psi$. When an agent removes liquidity, she removes a basket $\Psi \in \mathbf{R}^n_+$ with $\Psi \leq R$ from the reserves, resulting in the updated reserves $R^+ = R - \Psi$. When adding (or removing) to reserves, the agent receives (tenders) an IOU. This IOU gives the agent a pro-rata share of the reserves based on the amount of value the agent added and the total amount of value in the pool. We describe the exact mechanism for liquidity addition (and removal) below.

Liquidity change condition. The main condition for adding and removing liquidity is that the asset prices must not change after the removal, or addition, of liquidity. More specifically, we must have that the prices, as given in §1.3.2, at the new reserves, $R^+ \in \mathbf{R}^n_+$, must be equal, up to a scalar multiple, to those at the original reserves, $R \in \mathbf{R}^n_+$. Written out, this gives the following condition:

$$\nabla\varphi(R^+) = \alpha\nabla\varphi(R),$$

where φ is the canonical trading function and $\alpha > 0$ is some positive constant. Since φ is homogeneous, we have that, for any $\alpha > 0$, $\nabla\varphi(\alpha R) = \alpha\nabla\varphi(R)$. We conclude that $\Psi = \nu R$ for $\nu > 0$ is a valid liquidity change for any $\nu > 0$ (where $\nu < 1$ corresponds to liquidity removal and $\nu > 1$ corresponds to the addition of liquidity). Note that scaling R to αR corresponds exactly to scaling the reachable set by α.

Liquidity provider share weights. The CFMM additionally maintains a table of all liquidity providers and their corresponding share weights, representing the fraction of the reserves that each liquidity provider owns. We denote these weights as $w \in \mathbf{R}^N_+$, where N is the number of liquidity providers, and enforce that they sum to one, *i.e.*, $\sum_{i=1}^{N} w_i = 1$. These weights are updated whenever a liquidity provider adds or removes liquidity, or when the number of liquidity providers N changes.

Value of the reserves. Let $V = p^T R$ be the value of the CFMM reserves at price p. After adding liquidity νR, the value of the reserves is now

$$V^+ = p^T R^+ = (1+\nu)p^T R = (1+\nu)V.$$

For removing liquidity, we replace ν with $-\nu$. The fractional change in reserve value is

$$(V^+ - V)/V^+ = \nu/(1+\nu).$$

Liquidity provider share update. When liquidity provider j adds or removes liquidity, all the share weights are adjusted pro-rata based on the change of value of the reserves, which is the value of the basket she adds or removes. The fractional change in reserve value is $\nu/(1+\nu)$. Thus, after adding liquidity, the change in share weights is

$$w_i^+ = \begin{cases} w_i/(1+\nu) + \nu/(1+\nu) & i = j \\ w_i/(1+\nu) & i \neq j. \end{cases}$$

For removing liquidity, we replace ν with $-\nu$ and add the constraint that $\nu \leq w_j$.

Portfolio value. We note that, since liquidity providers own a pro-rata share with weight w_i of the total pool value, we may view each liquidity provider's position as 'independent'. In particular, there is no distinction between many liquidity providers pooling their assets together into a single CFMM versus every liquidity provider having their own CFMM instance and owning all of the assets of their particular instance. (There may be practical differences, however, owing to the fact that users may prefer to trade with a subset of these for a variety of reasons, such as gas fees.)

2 Single trade

We consider in this section the general CFMM case, which potentially includes fees and is therefore not necessarily path-independent. (We show the connection to the previous fee-free case later in the section.)

2.1 Trading set

Much in the same way as the previously-defined reachable set, we will define the *trading set* $T \subseteq \mathbf{R}^n$, which is any set T satisfying the following properties:

1. The set T is closed and convex
2. The zero trade is included, $0 \in T$
3. The set T is downward closed; *i.e.*, if $\Delta \in T$ and $\Delta' \leq \Delta$ then $\Delta' \in T$

An additional requirement that will be useful in the composition rules presented later, but is not strictly required for most of the statements below is that: there exists $R \in \mathbf{R}^n_+$ such that

$$R - T = \{R - \Delta \mid \Delta \in T\} \subseteq \mathbf{R}^n_+. \tag{20}$$

This corresponds to the statement that the CFMM can only tender a finite amount of some asset (in 'usual' CFMMs, this would be the available reserves) which is upper bounded by the quantity $R \geq 0$. One could imagine a mechanism that is allowed to mint unbounded amounts of tokens may violate (20).

Set up. In this set up, we have a trader who wishes to trade with the CFMM. This trader can suggest to trade a basket of tokens $\Delta \in \mathbf{R}^n$, where positive values denote what the trader receives from the CFMM and negative values denote what the trader tenders to the CFMM. The CFMM accepts this trade (and tenders or receives the stated amounts) only when $\Delta \in T$. (If $\Delta \notin T$, the trader receives and tenders nothing to the CFMM.) The state of the CFMM is then updated based on the accepted trade Δ (and a rejected trade does not change the state), but, for now, we will only consider the single-trade case and elide discussion of this state update until later. We assume only that the trading set at the current state is known and accessible to the trader.

Interpretation. The conditions imposed on the trading set all have relatively simple interpretations. The convexity of the trading set means that, as users trade more of a token, they receive marginally less (or, at least, no more) than they otherwise would by trading less. The fact that the zero trade is included means that a user is allowed to not trade. Finally, the downward-closedness of the set means that the CFMM will accept more of a given token, all else being equal; *i.e.*, a trader is allowed to 'overpay' for a given trade, and this new trade is still valid. The final optional condition can be interpreted as: a CFMM has a finite amount of assets that it is allowed to tender. While not strictly a requirement, we will need it for a technical condition we present later.

Example. A basic example of a trading set is Uniswap v2 with fees. In this particular case, the current state of the CFMM is given by some reserves $R \in \mathbf{R}^2_+$, and the trading set is

$$T = \{\Lambda - \Delta \mid (R_1 + \gamma\Delta_1 - \Lambda_1)_+(R_2 + \gamma\Delta_2 - \Lambda_2)_+ \geq R_1R_2,\ \Delta, \Lambda \in \mathbf{R}^n_+\},$$

where $0 \leq \gamma \leq 1$ is the fee parameter and is set by the CFMM at creation time. We show this set in figure 5. This writing is bit verbose and difficult to parse, but the construction is very similar to the original, given in the fee-free case above. Because of this, it is often nicer to work directly with a functional form, which we describe below.

Quasiconcavity and fees. Given any nondecreasing, quasiconcave function, with non-negative domain $\psi : \mathbf{R}^n_+ \to \mathbf{R}$ (much like the previous) we can define a trading set with fee

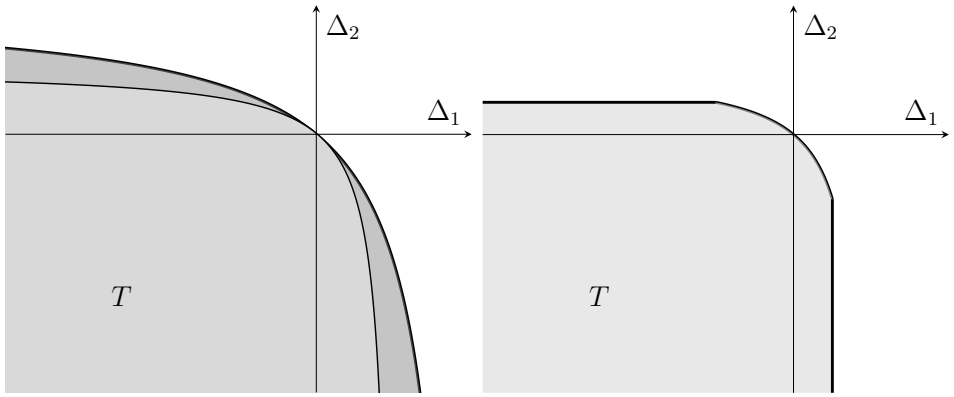

Figure 5: Left: the trading set for Uniswap (without fees) for $R = (1, 1)$ (light gray) and $R = (2, 2)$ (dark gray). Right: the trading set for Uniswap v3.

$0 \leq \gamma \leq 1$ and reserves $R \in \mathbf{R}^n_+$,

$$T = \{\Lambda - \Delta \mid \psi(R + \gamma\Delta - \Lambda) \geq \psi(R),\ \Delta, \Lambda \in \mathbf{R}^n_+\}. \tag{21}$$

(We will, by convention, let the function ψ take on $-\infty$ for values outside of its domain.) Clearly $0 \in T$ and T is downward closed as ψ is nondecreasing. The set is evidently convex as it is an affine transform of the set

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

which is a convex set by the quasiconcavity of ψ. Closedness is trickier, but follows from the fact that the valid choices of Λ are in some compact set, $0 \leq \Lambda \leq R$.

Composition rules. The composition rules are nearly identical in both statement and proof to those of the reachable set. Given trading sets $T, T' \subseteq \mathbf{R}^n_+$

1. Trading sets may be added; *i.e.*, $T + T'$ yields a trading set
2. Trading sets may be scaled, so αT is a trading set for any $\alpha > 0$
3. Taking the intersection $T \cap T'$ preserves the trading set property
4. Applying a nonnegative linear transformation $A \in \mathbf{R}^{k\times n}_+$ and adding all dominated trades,
$$AT - \mathbf{R}^k_+,$$
preserves the trading set property

These composition rules similarly lead to the notion of an aggregate CFMM mentioned previously, in the single-trade case, which is especially useful in the case of Uni v3 as we will show later. The only technical condition appears when adding trading sets: to ensure that the resulting trading set is closed, it suffices to ensure that all CFMMs can tender only a finite amount of assets, as in condition (20).

2.2 Trading cone and dual

Much in the same way as we have defined the liquidity cone, we define the *trading cone* as

$$K = \mathbf{cl}\{(\Delta, \lambda) \in \mathbf{R}^{n+1} \mid \Delta/\lambda \in T,\ \lambda > 0\}.$$

This cone plays a similar role to the liquidity cone, except in the single trade case. Indeed, many of the constructions we have shown previously for the liquidity cone will apply in a similar form to the trading cone. (We have overloaded notation as we will make no further reference to the liquidity cone.)

Trading function. From a nearly identical argument to the previous we may define a homogeneous, nondecreasing, but *convex* (instead of concave) trading function

$$\varphi(\Delta) = \min\{\lambda \geq 0 \mid (\Delta, \lambda) \in K\},$$

or, equivalently,

$$\varphi(\Delta) = \inf\{\lambda > 0 \mid \Delta/\lambda \in T\}. \tag{22}$$

such that

$$T = \{\Delta \in \mathbf{R}^n \mid \varphi(\Delta) \leq 1\}.$$

(Here, we define the min and inf of an empty set to be $+\infty$ for convenience.) The difference in sign from the definition in the path independent case in §1.3.2 comes from the fact that the set T is downward (rather than upward) closed, since we are taking the perspective of the trader, rather than the CFMM or its liquidity providers. In this case, the function φ is similarly canonical and rational traders will always tender trades Δ such that

$$\varphi(\Delta) = 1,$$

hence, again, the name 'constant function market maker.'

Example. Perhaps the simplest example of this type of function is, unsurprisingly, Uniswap v2. Using the quasiconcave function definition (21) of the trading set, we have, for $R \in \mathbf{R}^2_+$,

$$\psi(R_1, R_2) = R_1 R_2$$

with some fee $0 \leq \gamma \leq 1$. For a given proposed trade, $\tilde{\Delta} \in \mathbf{R}^n$, we can decompose $\tilde{\Delta}$ into its positive and negative parts $\tilde{\Delta} = \Lambda - \Delta$ with $\Delta, \Lambda \geq 0$ and disjoint support $\Delta_i \Lambda_i = 0$ for each $i = 1, 2$. Using the definition of the trading function, we look for the smallest $\lambda \geq 0$ such that

$$\left(R_1 + \gamma\frac{\Delta_1}{\lambda} - \frac{\Lambda_1}{\lambda}\right)\left(R_2 + \gamma\frac{\Delta_2}{\lambda} - \frac{\Lambda_2}{\lambda}\right) \geq R_1 R_2.$$

With some basic rearrangements, we find

$$\varphi(\tilde{\Delta}) = \frac{(\Lambda_1 - \gamma\Delta_1)(\Lambda_2 - \gamma\Delta_2)}{R_1(\gamma\Delta_2 - \Lambda_2) + R_2(\gamma\Delta_1 - \Lambda_1)}.$$

This trading function is homogeneous since the numerator is a homogeneous quadratic while the denominator is homogeneous. We can similarly verify that, as expected from the previous discussion, it is convex and nondecreasing by writing it in the following form:

$$\varphi(\tilde{\Delta}) = \frac{1}{-(R_1/(\gamma\Delta_1 - \Lambda_1) + R_2/(\gamma\Delta_2 - \Lambda_2))}.$$

Since the denominator is nonnegative, concave, and nonincreasing (in Λ), then φ must be nonnegative, convex, and nondecreasing (in Λ). Since $\tilde{\Delta} = \Lambda - \Delta$, directly verifying fact that φ is nondecreasing and convex in $\tilde{\Delta}$ requires one more step, which we leave to the reader as a useful exercise. (Of course, we know that both of these already follow from the construction of the trading function in (22) and the fact that ψ is quasiconcave and nondecreasing, as is the case for all such trading functions.)

Bounded liquidity. in a similar way to the previous section, we know that, since $0 \in T$, then

$$(-\mathbf{R}^n_+, 0) \subseteq K.$$

We say the trading set has *bounded liquidity in asset* i if the supremum

$$\sup\{\Delta_i \mid \Delta \in T\} = \Delta_i^\star,$$

is achieved at some $\Delta^\star \in T$. This has the interpretation that there is a finite basket of assets such that we receive all possible amount of asset i from the CFMM. We say a trading set has *bounded liquidity* if it has bounded liquidity for each asset $i = 1, \ldots, n$. Examples of bounded liquidity CFMMs include Uniswap v3 (see figure 5) and those with linear trading functions. These bounded liquidity CFMMs are useful since arbitrage can be easily computed in many important practical cases; see [DRCA23, §3] for more.

Arbitrage cone. In a similar way to the previous, we will define the dual cone for the trading cone $K \subseteq \mathbf{R}^{n+1}$ as

$$K^* = \{(c, \eta) \mid c^T\Delta + \eta\lambda \geq 0, \text{ for all } (\Delta, \lambda) \in K\}.$$

By downward closedness and the fact that $0 \in T$, it is not hard to show that $K^* \subseteq (-\mathbf{R}_+)^n \times \mathbf{R}_+$. Minimizing over the left hand side of the inequality gives another definition, based on the trading function:

$$K^* = \{(c, \eta) \mid c^T\Delta + \eta\varphi(\Delta) \geq 0, \text{ for all } \Delta \in \mathbf{R}^n\}.$$

Some care has to be taken when interpreting this expression if $\varphi(\Delta) = \infty$ when $\eta = 0$, based on the original definition of K, but this is an informative exercise for the reader.

Relation to arbitrage. Much like the portfolio value function, we write the *arbitrage function*, $\mathbf{arb} : \mathbf{R}^n \to \mathbf{R}$, for the trading set T as

$$\mathbf{arb}(c) = \sup\{c^T\Delta \mid \Delta \in T\}. \tag{23}$$

Note that if $c_i < 0$ for any i then $\mathbf{arb}(c) = +\infty$ by the downward-closedness of T, so we may generally assume that $c \geq 0$. This function has the following interpretation: if there is an external market with prices $c \in \mathbf{R}^n_+$, this is the maximum profit that an arbitrageur could derive by trading between the external market and the CFMM. This function is convex (as it is the supremum of a family of functions that are affine in c), nondecreasing over $c \geq 0$, and homogeneous. We may write this function in terms of the dual cone as

$$\mathbf{arb}(c) = \inf\{\eta \mid (-c, \eta) \in K^*\},$$

by a nearly-identical argument to that of the portfolio value function in §1.4.2. This function will be very useful in the routing problem that follows. Additionally, from a very similar argument to §1.4.3, the arbitrage function and the trading function are equivalent representations in that we may derive one from the other by setting

$$\varphi(\Delta) = \sup_{\mathbf{arb}(c)>0} \left(\frac{c^T\Delta}{\mathbf{arb}(c)} \right),$$

and

$$\mathbf{arb}(c) = \sup_{\varphi(\Delta)>0} \left(\frac{c^T\Delta}{\varphi(\Delta)} \right).$$

From before, note the suprema in this equation, versus the infima in the previous. For examples of such arbitrage functions for some common constant function market makers, see [DRCA23, app. A].

Marginal prices. We can view the supporting hyperplanes of T at some Δ as the set of *marginal prices* at trade Δ. We write this set as

$$C(\Delta) = \bigcap_{\Delta' \in T} \{\nu \in \mathbf{R}^n \mid \nu^T(\Delta' - \Delta) \leq 0\}. \tag{24}$$

Note that this set is a closed convex cone as it is the intersection of closed convex cones and is always nonempty as $0 \in C(\Delta)$. We can write the cone $C(\Delta)$ using the trading function as

$$C(\Delta) = \bigcup_{\lambda \geq 0} \lambda \partial(\varphi(\Delta)), \tag{25}$$

whenever $\varphi(\Delta) = 1$ and the subdifferential is defined. As we will soon see, the cone $C(0)$ will be called the *no-trade cone*. This is a generalization of the *no-trade interval* [DRCA23] in the case where $n \geq 2$. We show this cone for Uniswap in figure 6.

The proof of the equivalence (25) can be shown in two steps, one for the forward inclusion, and one for the reverse. From the statement, we have Δ with $\varphi(\Delta) = 1$. Now let $g \in \partial\varphi(\Delta)$, then

$$\varphi(\Delta) + g^T(\Delta' - \Delta) \leq \varphi(\Delta'),$$

by definition of the subgradient g. Letting $\Delta' \in T$ means that $\varphi(\Delta') \leq 1$ by definition and $\varphi(\Delta) = 1$ by the previous, so

$$g^T(\Delta' - \Delta) \leq \varphi(\Delta') - 1 \leq 0,$$

for every $\Delta' \in T$, which means that $g \in C(\Delta)$. Multiplying both sides of this inequality by $\lambda \geq 0$ then means that $\lambda g \in C(\Delta)$, or that

$$\bigcup_{\lambda \geq 0} \lambda\partial(\varphi(\Delta)) \subseteq C(\Delta).$$

For the other direction, using the definition of C in (24), note that $g \in C(\Delta)$ if, and only if, Δ is a maximizer of the following optimization problem:

$$\begin{array}{ll} \text{maximize} & g^T\Delta' \\ \text{subject to} & \varphi(\Delta') \leq 1, \end{array}$$

with variable $\Delta' \in \mathbf{R}^n$. Using the optimality conditions of this problem, we know that Δ is a maximizer if, and only if, there exists some $\lambda \geq 0$ such that

$$0 \in -g + \lambda\partial\varphi(\Delta),$$

or, equivalently, if, and only if, $g \in \lambda\partial\varphi(\Delta)$ for some $\lambda \geq 0$, which shows the reverse inclusion. It also shows that

$$C(\Delta) \subseteq \mathbf{R}^n_+,$$

since φ is nondecreasing, so it subgradients must be nonnegative. The optimality conditions are necessary and sufficient since $\varphi(-\mathbf{1}) = 0 < 1$ and $-\mathbf{1}$ is in the interior of the domain of φ.

Marginal price composition. Given $\Delta_i \in T_i$ for $i = 1, \ldots, m$, we have that

$$C\left(\sum_{i=1}^m \Delta_i\right) = \bigcap_{i=1}^m C_i(\Delta_i), \tag{26}$$

where C_i is the cone of marginal prices for CFMM i while C is the cone of marginal prices for the aggregate CFMM

$$\tilde{T} = \sum_{i=1}^m T_i.$$

This is easy to see from the definitions of C and $\tilde{T}$.

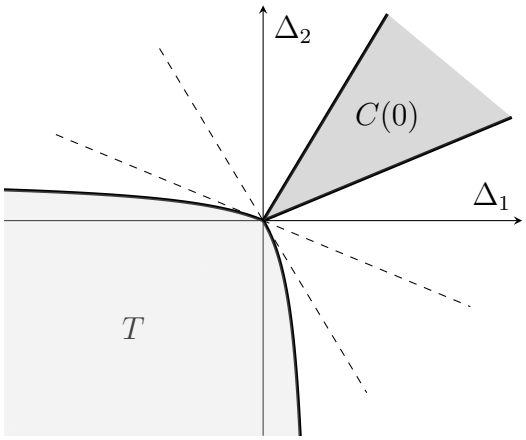

Figure 6: The trading set for Uniswap with fees (notice that the set is kinked at 0) and the corresponding no-trade cone.

Connection to arbitrage. Note that Δ is a solution to the arbitrage problem at price c, *i.e.*, $c^T\Delta = \mathbf{arb}(c)$ if, and only if,

$$c \in C(\Delta),$$

which follows by using the definition of **arb** and C. In other words, the arbitrage problem is solved at any trade which changes the prices to match those of the external market with prices $c \in \mathbf{R}^n_+$. We say there is *no arbitrage at price* c if the zero trade is a solution, *i.e.*,

$$c \in C(0).$$

Equivalently, we may view this as the case where the CFMM's prices are consistent with those of the external market. Alternatively, there is a direction connection between the marginal prices, arbitrage, and the dual cone K^*:

$$c \in C(\Delta), \text{ if, and only if, } (-c, c^T\Delta) \in K^*.$$

We can see this since $c \in C(\Delta)$ if, and only if, for all $\Delta' \in T$, we have

$$c^T\Delta' \leq c^T\Delta.$$

But $(\Delta', \lambda') \in K$ with $\lambda' > 0$ if and only if $\Delta'/\lambda' \in T$ so

$$\frac{c^T\Delta'}{\lambda'} \leq c^T\Delta.$$

Multiplying both sides by $\lambda' > 0$ and using a limiting argument shows that this is true, if, and only if, for all $(\Delta', \lambda') \in K$ we have

$$c^T\Delta' \leq \lambda' c^T\Delta,$$

which is the same as saying $(-c, c^T\Delta) \in K^*$.

2.3 Routing problem

The routing problem takes a number of possible CFMMs $i = 1, \ldots, m$, each trading a subset of n_i tokens out of the universe of n tokens, and seeks to find the best possible set of trades, *i.e.*, those maximizing a given utility function $U : \mathbf{R}^n \to \mathbf{R} \cup \{-\infty\}$. We assume that U is concave and increasing (*i.e.*, we assume all assets have value with potentially diminishing marginal returns). We use infinite values of U to encode constraints; a trade Ψ such that $U(\Psi) = -\infty$ is unacceptable to the trader. See [AECB22, §5.2] for examples, including liquidating or purchasing a basket of tokens and finding arbitrage.

We denote the trade we make with the ith CFMM by Δ_i and this CFMM's trading cone by $K_i \subseteq \mathbf{R}^{n_i+1}$. We also introduce matrices $A_i \in \mathbf{R}^{n \times n_i}$ which map the 'local' basket of n_i tokens for CFMM i to the global universe of n tokens. This construction is similar to the construction of aggregate CFMMs in §1.2, but here we focus on the trade vectors and not the trading sets. The net trade is then

$$\Psi = \sum_{i=1}^{m} A_i \Delta_i.$$

The optimal routing problem is then the problem of finding a set of valid trades with each market that maximize the trader's utility:

$$\begin{array}{ll} \text{maximize} & U(\Psi) \\ \text{subject to} & \Psi = \displaystyle\sum_{i=1}^{m} A_i \Delta_i \\ & (\Delta_i, 1) \in K_i, \quad i = 1, \ldots, m. \end{array}$$

The variables here are the net trades $\Psi \in \mathbf{R}^n$ and the trades $\Delta_i \in \mathbf{R}^{n_i}$. Note that, by definition of the trading cone K_i, we have that $\Delta_i \in T_i$ if, and only if, $(\Delta_i, 1) \in K_i$.

Other interpretations. If $A_i = I$, *i.e.*, if all CFMMs trade the same tokens, then this problem is equivalent to

$$\begin{array}{ll} \text{maximize} & U(\tilde{\Delta}) \\ \text{subject to} & \tilde{\Delta} \in \tilde{T}, \end{array}$$

where $\tilde{T} = \sum_{i=1}^{m} T_i$, which is another trading set, by the composition rules given in §2.1. While this rewriting seems silly, it tells us that we may consider routing through a network of CFMMs as trading with one 'large' CFMM. The optimality conditions for this problem are that

$$0 \in \partial(-U)(\tilde{\Delta}^\star) + \tilde{C}(\Delta^\star),$$

and $\tilde{\Delta}^\star \in \tilde{T}$. From (26) we know that $\tilde{C}$ is the intersection of each individual price cone, so, using the definition of $\tilde{T}$, we get

$$0 \in \partial(-U)\left(\sum_{i=1}^{m} A_i \Delta_i^\star\right) + \bigcap_{i=1}^{m} C_i(\Delta_i^\star),$$

and $\Delta_i^\star \in T_i$, which are exactly the optimality conditions we would get from considering the original routing problem. The case where A_i are general nonnegative orthogonal matrices is slightly more involved, but is ultimately very similar.

Dual problem. From conic duality, we know that the dual problem can be written as

$$\begin{array}{ll} \text{minimize} & \bar{U}(\nu) + \mathbf{1}^T\eta \\ \text{subject to} & (-A_i^T\nu, \eta_i) \in K_i^*, \quad i = 1, \ldots, m, \end{array}$$

where the variables are $\nu \in \mathbf{R}^n$ and $\eta \in \mathbf{R}^m$. Partially minimizing over each η_i and using the definition of the optimal arbitrage function, we have that this problem is equivalent to

$$\text{minimize} \quad \bar{U}(\nu) + \sum_{i=1}^m \mathbf{arb}_i(A_i^T\nu),$$

where $\mathbf{arb}_i$ is the optimal arbitrage function for the ith trading set. This is exactly the dual problem used in the decomposition method of [DRCA23]. This problem has a beautiful interpretation: the optimal trades are exactly those which result in a price vector ν that minimizes the total arbitrage that the user would receive if we interpret $\bar{U}(\nu)$ as the maximum utility that could be received by trading with an external market with price ν.

2.4 Path independence

In this subsection, we show the connection between the path-independent CFMMs, presented in the previous section, and the 'general' CFMMs presented in this one.

Mechanics of trading. In a CFMM, as stated previously, we have some state, which is given by the reserves $R \in \mathbf{R}_+^n$. The current trading set, defined as $T(R) \subseteq \mathbf{R}^n$ has the same properties given at the beginning of this section. (We implicitly included the relationship between the trading set and the reserves in the previous section as the reserves could be considered fixed for a single trade.) The CFMM then accepts or rejects any proposed trade $\Delta \in \mathbf{R}^n$ based on whether $\Delta \in T(R)$. If this is the case, then the CFMM accepts the trade, updating its reserves to $R \to R - \Delta$ (as it pays out Δ_i to the trader from its reserves for $\Delta_i > 0$ and vice versa) and making the new trading set $T(R - \Delta)$. If the trade is rejected then the reserves are not updated and the trading set remains as-is.

Sequential feasibility. From before, we say a trade Δ is feasible if $\Delta \in T(R)$. We say a sequence of trades $\Delta_i \in \mathbf{R}^n$ for $i = 1, \ldots, m$ is *(sequentially) feasible* if

$$\Delta_i \in T(R - (\Delta_1 + \cdots + \Delta_{i-1})).$$

for each $i = 1, \ldots, m$.

Reachability. We say some reserves R' are *reachable* from some initial set of reserves R if there is a sequence of feasible trades $\Delta_i \in \mathbf{R}^n$, for $i = 1, \ldots, m$, such that

$$R' = R - (\Delta_1 + \cdots + \Delta_m).$$

In other words, R' is reachable from R if there is a sequence of feasible trades that takes us from reserves R to reserves R'

Path independence. We say a CFMM is *path independent* if, for any reserves R and for any trade Δ satisfying $\Delta \in T(R)$, we have

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta + \Delta' \in T(R). \tag{27}$$

In English: a CFMM is path independent if there is no difference between performing trades sequentially versus in aggregate, if the trades are sequentially feasible. (We may apply induction to this definition to get the more 'general-seeming' case that applies to any finite sequence of feasible trades.)

Reachable set. If the CFMM is path independent, there exists a fixed set $S \subseteq \mathbf{R}^n$ (which, as we will soon see, corresponds exactly to the reachable set of §1.1) such that every trading set $T(R')$ can be written as

$$T(R') = R' - S, \tag{28}$$

for any reachable R', starting from some reserves R. (Here, $R' - S = \{R' - \tilde{R} \mid \tilde{R} \in S\}$.)

Proof. We will show that, whenever the CFMM is path independent, then we will have that, for any reachable R', $R - T(R) = R' - T(R')$. Setting $S = R - T(R)$ will then suffice to satisfy (28). Note that it suffices to consider only R' which are reachable in 1 step, since the result follows by induction. That is, we will consider the case where $R' = R - \Delta$ for $\Delta \in T(R)$ and the general case follows by induction.

We can rewrite the path independence condition (27) as

$$\Delta' \in T(R - \Delta) \quad \text{if, and only if,} \quad \Delta' \in T(R) - \Delta,$$

or, equivalently,

$$T(R - \Delta) = T(R) - \Delta.$$

The proof is then nearly obvious after this:

$$R' - T(R') = (R - \Delta) - T(R - \Delta) = R - \Delta - T(R) + \Delta = R - T(R).$$

We may then set $S = R' - T(R') = R - T(R)$, such that (28) is satisfied for any R' reachable from R.

Conditions. Note that the conditions on $T(R)$ will imply some conditions on S. Indeed, since $T(R)$ is a closed convex set, then S must also be. Similarly, since $0 \in T(R)$ then $R \in S$, so S is nonempty, and, since we must have $R - \Delta \geq 0$ for any $\Delta \in T(R)$ then $S = R - T(R) \subseteq \mathbf{R}^n_+$. Finally, since $T(R)$ is downward closed, then S must be upward closed, hence S must be a reachable set as defined in §1.1.

Equivalence. This is, of course, a bijection. We know that any path independent CFMM with trading set $T(R)$ may be written as

$$T(R) = R - S,$$

so long as $R \in S$. Additionally, if S is a reachable set, then we must have that $0 \in T(R)$, that $T(R)$ is closed and convex, and that $T(R)$ is downward closed, making it a reasonable trading set. It is also bounded (20) since $S \subseteq \mathbf{R}^n_+$ so $R - T(R) \subseteq \mathbf{R}^n_+$.

Discussion. In general, it is tempting to deal with histories of trades among other objects when discussing CFMMs as these are dynamic systems with some internal state that changes as trades are performed. The above shows that, in the special case that the CFMM is path independent, we only need to consider the reachable set, as this contains all properties needed to completely describe the object in question. Indeed, the proof above shows that a CFMM is path-independent if, and only if, it is completely described by a reachable set meeting the conditions outlined in §1.1.

3 Conclusion

In this paper, we have shown that a general geometric perspective on constant function market makers is relatively fruitful. Indeed, assuming only a small number of 'intuitive' conditions on sets, we have derived a number of results—some known already, some not—which follow from almost purely geometrical considerations. In some cases, we show that assumptions made in the literature actually are unnecessary, and indeed are consequences of a subset of the assumptions made. Examples of these include the homogeneity of [AEC21], [SKM23], and [FPW23]. In others, we derive a new form of a known result such as [AEC23] or [FPW23]. We suspect that there are a number of useful 'geometric' interpretations to other known results in the literature, but leave these for future work.

References

[AAE+22] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant function market makers: Multi-asset trades via convex optimization. In *Handbook on Blockchain*, pages 415–444. Springer, 2022.

[AC20] 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.

[ACE22] Guillermo Angeris, Tarun Chitra, and Alex Evans. When Does The Tail Wag The Dog? Curvature and Market Making. *Cryptoeconomic Systems*, 2(1), jun 13 2022. https://cryptoeconomicsystems.pubpub.org/pub/angeris-curvature-market-making.

[AEC21] Guillermo Angeris, Alex Evans, and Tarun Chitra. A Note on Privacy in Constant Function Market Makers, March 2021.

[AEC23] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers. *Digital Finance*, pages 1–21, 2023.

[AECB22] Guillermo Angeris, Alex Evans, Tarun Chitra, and Stephen Boyd. Optimal routing for constant function market makers. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 115–128, 2022.

[AZR20] Hayden Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core. *URL: https://uniswap.org/whitepaper.pdf*, 2020.

[AZS+21] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. *Tech. rep., Uniswap, Tech. Rep.*, 2021.

[BV04] Stephen P. Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, UK; New York, 2004.

[CAE21] Tarun Chitra, Guillermo Angeris, and Alex Evans. How liveness separates cfmms and order books. 2021.

[DKP21] Vincent Danos, Hamza El Khalloufi, and Julien Prat. Global order routing on exchange networks. In Matthew Bernhard, Andrea Bracciali, Lewis Gudgeon, Thomas Haines, Ariah Klages-Mundt, Shin'ichiro Matsuo, Daniel Perez, Massimiliano Sala, and Sam Werner, editors, *Financial Cryptography and Data Security. FC 2021 International Workshops*, pages 207–226, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg.

[DRCA23] Theo Diamandis, Max Resnick, Tarun Chitra, and Guillermo Angeris. An efficient algorithm for optimal routing through constant function market makers. *arXiv preprint arXiv:2302.04938*, 2023.

[EH21] Daniel Engel and Maurice Herlihy. Composing networks of automated market makers. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*. ACM, sep 2021.

[FMW23] Masaaki Fukasawa, Basile Maire, and Marcus Wunsch. Weighted variance swaps hedge against impermanent loss. *Quantitative Finance*, 23(6):901–911, 2023.

[FPW23] Rafael Frongillo, Maneesha Papireddygari, and Bo Waggoner. An axiomatic characterization of cfmms and equivalence to prediction markets. *arXiv preprint arXiv:2302.00196*, 2023.

[GRGM23] Mohak Goyal, Geoffrey Ramseyer, Ashish Goel, and David Mazières. Finding the right curve: Optimal design of constant function market makers. In *Proceedings of the 24th ACM Conference on Economics and Computation*, pages 783–812, 2023.

[LP21] Alfred Lehar and Christine A Parlour. Decentralized exchanges. *Available at SSRN 3905316*, 2021.

[McC56] John McCarthy. Measures of the value of information. *Proceedings of the National Academy of Sciences*, 42(9):654–655, 1956.

[MDP23] Bruno Mazorra and Nicolás Della Penna. Towards optimal prior-free permissionless rebate mechanisms, with applications to automated market makers & combinatorial orderflow auctions. *arXiv preprint arXiv:2306.17024*, 2023.

[MMR23a] Jason Milionis, Ciamac C. Moallemi, and Tim Roughgarden. Complexity-approximation trade-offs in exchange mechanisms: Amms vs. lobs, 2023.

[MMR23b] Jason Milionis, Ciamac C. Moallemi, and Tim Roughgarden. A myersonian framework for optimal liquidity provision in automated market makers, 2023.

[SKM23] Jan Christoph Schlegel, Mateusz Kwaśnicki, and Akaki Mamageishvili. Axioms for constant function market makers, 2023.

[WM22] Mike Wu and Will McTighe. Constant power root market makers, 2022.

A A primer on conic duality

This appendix is intended as a (very short) primer on conic duality. We assume basic familiarity with convex sets and the separating hyperplane theorem. For far more, see [BV04, §2.6].

Cones. A *cone* is a set $K \subseteq \mathbf{R}^n$ such that, if $x \in K$ then, for any $\alpha \geq 0$, we have $\alpha x \in K$. A *convex cone* is, as one would expect, a cone that is convex. More generally, convex cones are closed under nonnegative scalar multiplication, *i.e.*, if $x, y \in K$ and $\alpha, \beta \geq 0$, then

$$\alpha x + \beta y \in K.$$

Basic examples of convex cones include the nonnegative real elements $\mathbf{R}^n_+$ and the norm cones, given by

$$K_{\|\cdot\|} = \{(x,t) \in \mathbf{R}^{n+1} \mid \|x\| \leq t\}.$$

Properties. If K is closed and nonempty then $0 \in K$. The intersection of convex cones is a convex cone and scaling a convex cone results in a convex cone. Finally, the (Cartesian) product of two convex cones is again a convex cone.

Dual cone. The *dual cone* K^* of a cone K is defined as

$$K^* = \{y \in \mathbf{R}^n \mid y^T x \geq 0, \text{ for all } x \in K\}.$$

In other words, the dual cone of K is the set of all vectors which have nonnegative inner product with every element in K. Since we can write

$$K^* = \bigcap_{x \in K} \{y \in \mathbf{R}^n \mid y^T x \geq 0\},$$

then we can see that K^* is a closed convex cone (even when K is not). For example, the dual cone of $\mathbf{R}^n_+$ is $\mathbf{R}^n_+$, while the norm cone is

$$K^*_{\|\cdot\|} = \{(y,r) \in \mathbf{R}^{n+1} \mid \|y\|_* \leq r\},$$

where $\|y\|_*$ is the dual norm of y, defined

$$\|y\|_* = \sup\{y^T x \mid \|x\| \leq 1\}.$$

Properties. By definition $0 \in K$, and, since K^* can be written as an intersection over K, then if $K' \subseteq K$, we have

$$K^* \subseteq K'^*.$$

Additionally note that

$$(K + K')^* = K^* \cap K'^*,$$

and

$$(K \times K')^* = K^* \times K'^*,$$

all of which are simple exercises and follow from the definition of the dual cone above.

Duality. In a certain sense, we may view the dual cone K^* as a collection of *certificates* that an element is not in K. More specifically, if we have any $x \in \mathbf{R}^n$ and we are given some $y \in K^*$ such that $y^T x < 0$, then we are guaranteed that, indeed $x \notin K$, by definition of K^*. Conic duality gives the following guarantee for a nonempty, closed convex cone K: for any $x \in \mathbf{R}^n$, either $x \in K$, or there exists $y \in K^*$ with $x^T y < 0$, but not both. In other words, either some given point x it either belongs in the cone, or we can furnish a certificate, using the dual cone, that it does not.

The reverse implication follows from the previous argument. (Note that this implication requires no assumptions on K.) The forward implication will make use of the convexity of K to furnish a certificate. To see this, let $x \notin K$, then, since K is convex closed, there exists a strict separating hyperplane with slope $y \in \mathbf{R}^n$ such that

$$x^T y < z^T y, \text{ for all } z \in K.$$

Since, for any $t \geq 0$ and $z \in K$, we have $tz \in K$, we therefore know that, for any $z \in K$,

$$x^T y/t < z^T y,$$

and sending $t \to \infty$ we then know

$$z^T y \geq 0 \text{ for any } z \in K,$$

so $y \in K^*$. Finally, since K is closed, then $0 \in K$ so

$$x^T y < 0,$$

completing the proof.

Dual of the dual. Because of the previous, we now have the following result: K is exactly the set of vectors $x \in \mathbf{R}^n$ such that x has nonnegative inner product with every element of K^*; *i.e.*, for which we cannot furnish a certificate that $x \notin K$. But, the set of vectors which have nonnegative inner product with every element of K^* is exactly the dual cone of K^*, written $(K^*)^* = K^{**}$. This gives the following beautiful relation for a nonempty, closed, and convex cone K:

$$K^{**} = K.$$

Conic duality in optimization. Most convex optimization problems can be cast as conic optimization problems. The general form of such a problem is, for some convex objective function $f : \mathbf{R}^n \to \mathbf{R} \cup \{\infty\}$

$$\begin{array}{ll} \text{minimize} & f(x) \\ \text{subject to} & Ax = b \\ & x \in K, \end{array}$$

where the variable is $x \in \mathbf{R}^n$, and the problem data are the closed nonempty convex cone $K \subseteq \mathbf{R}^n$, the matrix $A \in \mathbf{R}^{m \times n}$, and the constraint vector $b \in \mathbf{R}^m$.

Conic duality tells us that, if there exists any point in the interior of K, *i.e.*, $\mathbf{int}\, K \neq \varnothing$, then this problem and the following problem, called the *dual problem*, have the same optimal value

$$\begin{array}{ll} \text{maximize} & \bar{f}(A^T y) + b^T y \\ \text{subject to} & -A^T y \in K^*, \end{array}$$

with variable $y \in \mathbf{R}^n$, where

$$\bar{f}(z) = \inf_x (f(x) - x^T z),$$

is sometimes known as the *concave conjugate*. As we only use this fact once in the main text, we do not derive it in detail, but see [BV04, §5.9] for reference.

B Curve

In this section, we derive the canonical trading function for a two-asset Curve pool. Recall that the trading set for this market is given by [AC20]

$$S = \left\{ R \;\middle|\; R_1 + R_2 - \frac{\alpha}{R_1 R_2} \geq k \right\}.$$

From (6), we can write the trading function as

$$\varphi(R) = \sup \left\{ \lambda > 0 \;\middle|\; \frac{R_1 + R_2}{\lambda} - \frac{\alpha \lambda^2}{R_1 R_2} \geq k \right\}.$$

Rewriting, we have that

$$\varphi(R) = \sup \left\{ \lambda > 0 \;\middle|\; -\alpha\lambda^3 - kR_1R_2\lambda + R_1R_2(R_1 + R_2) \geq 0 \right\}.$$

The solution is given by the largest positive root of the cubic polynomial in λ:

$$\lambda^\star = \frac{\sqrt[3]{c_1 + \sqrt{c_2}}}{3\sqrt[3]{2}\alpha} - \frac{\sqrt[3]{2}kR_1R_2}{\sqrt[3]{c_1 + \sqrt{c_2}}}$$

where $c_1(R) = 27\alpha^2 R_1^2 R_2 + 27\alpha^2 R_1 R_2^2$ and $c_2(R) = 108\alpha^3 k^3 R_1^3 R_2^3 + c_1^2$. Plugging this back in, we have the canonical trading function

$$\varphi(R) = \frac{R_1 + R_2}{k\lambda^\star} - \frac{\alpha(\lambda^\star)^2}{kR_1R_2},$$

which can (painfully) be verified to be homogeneous.

C Proof of concavity of Uniswap v3

The main difficulty in showing that (10) is concave is the square root term

$$\sqrt{(\beta R_1 + \alpha R_2)^2 + 4(k - \alpha\beta)R_1R_2}.$$

Its concavity follows from the fact that the set

$$Q = \{(x, y, t) \in \mathbf{R}_+^3 \mid \|(\sqrt{\eta}(x - y), t)\|_2 \leq \sqrt{1 + \eta}(x + y)\}$$

is convex when $\eta \geq 0$, where $\|\cdot\|_2$ denotes the Euclidean norm. (To see this, note that norms are convex and affine functions are convex. Sets of the form $\{z \mid f(z) \leq 0\}$ are convex when f is convex, and affine precomposition preserves convexity.) Expanding the inequality gives the following equivalent characterization of the set:

$$Q = \{(x, y, t) \in \mathbf{R}_+^3 \mid t \leq \sqrt{(x + y)^2 + 4\eta xy}\},$$

which means that the function

$$\sqrt{(x+y)^2+4\eta xy} = \sup\{t \geq 0 \mid (x,y,t) \in Q\},$$

is concave in (x, y). Finally, setting $\eta = (k-\alpha\beta)/\alpha\beta$, $x = \beta R_1$ and $y = \alpha R_2$ shows that the function

$$\sqrt{(\beta R_1 + \alpha R_2)^2 + 4(k-\alpha\beta)R_1 R_2},$$

is concave in R_1 and R_2.