Replicating Monotonic Payoffs Without Oracles

Guillermo Angeris   Alex Evans   Tarun Chitra

angeris@stanford.edu   ahe4nc@gmail.com   tarun@gauntlet.network

September 2021

Abstract

In this paper, we show that any monotonic payoff can be replicated using only liquidity provider shares in constant function market makers (CFMMs), without the need for additional collateral or oracles. Such payoffs include cash-or-nothing calls and capped calls, among many others, and we give an explicit method for finding a trading function matching these payoffs. For example, this method provides an easy way to show that the trading function for maintaining a portfolio where 50% of the portfolio is allocated in one asset and 50% in the other is exactly the constant product market maker (*e.g.*, Uniswap) from first principles. We additionally provide a simple formula for the total earnings of an arbitrageur who is arbitraging against these CFMMs.

Introduction

Constant function market makers (CFMMs) continue to be the most used decentralized application, with billions of dollars in daily trading volume. Recently, there has been increased interest in understanding the space of financial products that can be created with CFMMs. The main usage of CFMMs, to date, is as decentralized exchanges, or DEXs for short. When CFMMs are used as DEXs, liquidity providers pool assets into the CFMM contracts with the aim of earning passive yield on their assets, while traders, who wish to swap one asset for another, execute trades against this pool while paying a small fee to the liquidity providers on each trade. To decide which trades to accept, the CFMM contract ensures that a specific function, known as the *trading function*, that depends on the current state of the contract and the traded amounts, is kept constant. An important consequence of this design is that arbitrageurs will always ensure that the price quoted by CFMM stays synchronized with the price of other markets that consist of the same asset pairs [AKC+19, AC20].

Previous work. Another view of a liquidity provider's shares in a CFMM is as a dynamically adjusted portfolio held by liquidity providers. This portfolio is constantly adjusted by arbitrageurs [EAC21] as the price of assets in external markets changes. It has been shown that these portfolios held by liquidity providers can replicate a number of other financial

payoffs [Cla20, AEC21, Cla21]. Evans [Eva20] was the first to show that CFMMs with dynamic trading functions (*i.e.*, where the trading function is allowed to evolve over time) can replicate *any* unlevered payoff function. If leverage is available (*e.g.*, if users are allowed to borrow assets against a liquidity provider's share of the pool) it is possible to replicate a number of bounded convex payoffs [CAEK21]. Furthermore, [AEC21] provides a simple method to construct a CFMM trading function given a desired portfolio value function for liquidity providers. This method depends on the concavity of the payoff function and uses some basic properties of convex functions to construct the desired payoffs. However, the payoffs that can be generated via this method are restricted — one can only construct a CFMM whose liquidity provider shares have a portfolio value function that is concave, nonnegative, nondecreasing, and 1-homogeneous, the so-called 'consistent' portfolio values. In fact, the paper shows that the space of CFMMs and the space of consistent portfolio value functions are equivalent in that every CFMM has a consistent portfolio value function and vice-versa.

Comparisons and this work. The key insight of this work is to note that liquidity providers do not have to sell their entire position, but can instead sell off the right to withdraw individual components of the share. Surprisingly, this small fact allows a much richer set of payoffs to be replicated without leverage, without additional collateral than what is held in a CFMM liquidity provider share, and without requiring an external oracle [ESGC21]. More specifically, we show that any monotonic payoff, in a certain price interval, can be replicated using this technique by constructing an appropriate trading function. In many practical cases, we show that these payoffs also yield explicit formulas for the trading function, and, in some special cases, the total expected arbitrage profit.

Replicating payoffs. Using this method, many of the capped or bounded convex payoffs of [CAEK21] can be replicated without requiring a CFMM lender. Specifically, we show that a number of payoffs such as capped calls, logarithmic payoffs, and the cash-or-nothing call (sometimes called the binary option) can be easily replicated. We also show that one can uniquely derive the most popular trading function, the constant mean market maker [ZCP18, AZR20, MM19, Eva20] of Uniswap and Balancer, by requiring that the user's portfolio have a constant proportion of their total portfolio value in each asset. This illustrates that liquidity providers should be assessing the quality of a CFMM pool by assessing the associated payoffs, rather than just the trading function itself. Provided that a user can construct smart contracts that securitize a subset of the components of the portfolio in the liquidity provider share, it is possible to replicate these payoffs. We note that there are live smart contracts on Ethereum, such as Ondo Finance [All] that allow for liquidity providers to sell a portion of their yield to other market participants.

Summary. In §1, we present all of the mathematical background needed to construct the trading function for a given payoff, conditions under which payoffs that span an infinite interval can be replicated, and a simple formula for the earnings of an arbitrageur for a given price process. We then provide examples of different payoffs that are useful in practice in §2

and discuss some interpretations and extensions in §3.

1 Replicating payoffs

A *payoff* is a function $f : \mathbf{R}_+ \to \mathbf{R}$ which maps the *price* $p \geq 0$ of some asset, which we will call the risky asset, to a quantity of the numéraire, $f(p)$. A *monotonic payoff* is one where the payoff function f is monotonically nondecreasing; *i.e.*,

$$f(p) \leq f(q),$$

whenever $p \leq q$. In the special case that f is differentiable, this is equivalent to $f'(p) \geq 0$ for all $p \geq 0$. Throughout the rest of this paper, we will be concerned only with the monotonic payoffs that are nonnegative (*i.e.*, satisfy $f(p) \geq 0$) but show some extensions which relax this latter condition. Additionally, for convenience, we will assume that f is differentiable for the rest of this section, but we will present results that apply in much more general settings such as when f is differentiable, except at a countable number of discontinuities, and is lower semicontinuous.

Portfolio interpretation. We can view the monotonic payoff as a user's desired portfolio allocation over two assets: the risky asset and the numéraire, with $f(p)$ denoting how much of the numéraire the user is holding at price p. In this scenario, the user is continually rebalancing the portfolio (*e.g.*, by selling or buying the risky asset) as the market price changes. Using this strategy, if the market price changes from $p_1 > 0$ to $p_2 > 0$, the total amount of risky asset that the user needs to sell is given by:

$$\int_{p_1}^{p_2} \frac{f'(p)}{p} \, dp. \tag{1}$$

A basic argument for this is as follows. Note that, as the price changes from p to $p + h$, the user must buy $f(p + h) - f(p)$ of the numéraire (selling if the quantity is negative). If h is small, this costs approximately $(f(p + h) - f(p))/p$, and, since f is differentiable, we have:

$$\frac{f(p + h) - f(p)}{p} = \frac{f'(p)h}{p} + o(h).$$

Dividing the right hand side by h, taking the limit, and integrating over p gives the desired result. This argument can be made fully airtight, but we omit the details as they are mostly mechanical and unenlightening.

Required risky asset. A natural question is: at some price $\alpha \leq p \leq \beta$ where α, β satisfy $0 \leq \alpha \leq \beta \leq \infty$ (we allow that $\beta = \infty$ for convenience), how much of the risky asset do users need to hold in their portfolios to be able to trade using this strategy? This follows from (1), which gives that

$$g(p) = \int_p^\beta \frac{f'(q)}{q} \, dq.$$

3

Therefore, at any price $\alpha \leq p \leq \beta$, the portfolio under this strategy contains $f(p)$ of the numéraire, and $g(p)$ of the risky asset. Additionally, we note that, since $f' \geq 0$, the function g is nonincreasing and nonnegative. We call $g(p)$ the 'replication cost' at price p.

1.1 Desired portfolios and trading functions

We will define the set of *desired portfolios* as:

$$S = \{(f(p), g(p)) \mid \alpha \leq p \leq \beta\}. \tag{2}$$

In other words, the set S is the set of all possible portfolio allocations within the replication interval $[\alpha, \beta]$.

Portfolio value. A natural question to ask is: what is the portfolio value of S, at some price p? The portfolio value $V(p)$ at price p is defined as the sum of the total value of all assets, in terms of the numéraire, *i.e.*:

$$V(p) = f(p) + pg(p). \tag{3}$$

We can also rewrite V in an equivalent, but very useful way:

$$V(p) = V(\alpha) + \int_\alpha^p g(q)\, dq. \tag{4}$$

To see this, note that:

$$\int_\alpha^p g(q)\, dq = pg(p) - \alpha g(\alpha) - \int_\alpha^p q\, dg(q),$$

where the right hand side follows from integration by parts. Since the last term of this expression is equal to:

$$-\int_\alpha^p q\, dg(q) = \int_\alpha^p q \frac{df(q)}{q} = f(p) - f(\alpha),$$

then (4) follows from a basic rearrangement.

The portfolio value function has several immediate properties. For example, we can see from (3) it is nonnegative since $f(p), g(p) \geq 0$ whenever $0 \leq \alpha \leq p \leq \beta$. On the other hand, using (4), we can see that V nondecreasing since $g \geq 0$, and concave since g is nonincreasing. Putting this all together, we see that the portfolio value V is a nonnegative, nondecreasing, concave function, which implies that there is a constant function market maker with portfolio value function V [AEC21].

4

Trading function. We can construct a trading function for a constant function market maker whose liquidity provider position at price p is equal to $(f(p), g(p))$. (For a general introduction to CFMMs and trading functions, see, *e.g.*, [AAE+21, §2].) To do this, we use a simplification of the results from [AEC21], given in appendix A. This simplification shows that, given the nonnegative, nondecreasing, concave portfolio value function V, we can write a trading function

$$\psi(R_1, R_2) = \inf_{\alpha \leq p \leq \beta} (R_1 + pR_2 - V(p)), \tag{5}$$

whose portfolio value is equal to $V(p)$ at price p, for all $R_1, R_2 \geq 0$. Using (4), then

$$pR_2 - V(p) = \alpha R_2 - V(\alpha) + \int_\alpha^p (R_2 - g(p)) \, dp.$$

Since g is nonincreasing, then it is immediate that this expression is minimized by choosing p to be equal to

$$g^{-1}(R_2) = \sup \{\alpha \leq p \leq \beta \mid g(p) \geq R_2\},$$

if the set is nonempty, and we set $g^{-1}(R_2) = \alpha$, otherwise. To see this, note that the integrand of the term

$$\int_\alpha^p (R_2 - g(p)) \, dp$$

is nonpositive for all $p \leq q$ where q satisfies $g(q) \geq R_2$, and choosing the largest such q, *i.e.*, $q = g^{-1}(R_2)$, as defined previously, minimizes the total integral. We use the suggestive 'inverse' notation since g^{-1} is indeed the inverse of g when g is continuous and R_2 satisfies $g(\beta) \leq R_2 \leq g(\alpha)$, which is a common case in practice.

Plugging this back into (5), the trading function is given by

$$\psi(R_1, R_2) = R_1 + g^{-1}(R_2)R_2 - V(g^{-1}(R_2)). \tag{6}$$

In the common special case that $g(g^{-1}(R_2)) = R_2$ (*i.e.*, $g^{-1}(R_2)$ is the 'true inverse') then this simplifies to:

$$\psi(R_1, R_2) = R_1 - f(g^{-1}(R_2)), \tag{7}$$

which, from the previous discussion happens when, *e.g.*, g is continuous.

Discussion. The function ψ in (5) is increasing and it is concave as it is the infimum over a family of functions that are linear in R_1 and R_2 [BV04, §3.2.3]. Because of this, arbitrageurs are incentivized to arbitrage against a CFMM using ψ as its trading function, in order to make its price match that of an external market. From the previous discussion, this ensures that the liquidity provider's portfolio, when the external market is at price p, is given by $(f(p), g(p))$. We will show a direct proof of this in §1.3 and give a simple expression for the total earnings of arbitrageurs who arbitrage against CFMMs of this form.

There are a few possible implementations of this system, and we present a very simple one. In this implementation, a liquidity provider first mints a share on a CFMM whose trading function is specified above by putting in $(f(p), g(p))$ of the numéraire and risky

assets, respectively, when the market price is p. The liquidity provider then sells off the right to only the numéraire side of the pool, which has value $f(p)$, via some token. This token grants the buyer the following right: when the token is burned, the liquidity provider share is also burned, and the amount of numéraire found in the pool is immediately paid out to the token holder, while the remaining risky asset is paid out to the liquidity provider. The underlying value of the token is at least (but often close to) $f(p)$, as it can always be redeemed for that amount at any point, which is the desired monotonic payoff of the price p.

1.2 Replication costs

In the case that $\beta < \infty$ and $p > 0$, the amount of risky asset needed to replicate the portfolio is always finite when f is finite, but this need not be true as $\beta \to \infty$. We show that the growth of f needs to be at most sublinear in order to be finite, while it suffices to be polynomial of degree $(1 - \varepsilon)$ to be finite, for any $p > 0$.

Necessary conditions. The payoff function f has to exhibit sublinear growth in order to have a finite replication cost. More specifically, if f is not sublinear in that

$$f(p) \geq Cp,$$

for some $C > 0$ and for all $p \geq p_0 \geq \beta$ (*i.e.*, if $f(p) = \Omega(p)$) then, for any p

$$g(p) = \int_p^\beta \frac{f'(p)}{p}\, dp \geq \int_{p_0}^\beta \frac{f'(p)}{p}\, dp \geq \int_{p_0}^\beta \frac{C}{p}\, dp \to \infty,$$

as $\beta \to \infty$. So it is necessary that f grows slower than any linear function in order for the risky side of the portfolio to be finite for any p. In other words, we must have that f is little-oh of p, *i.e.*, $f(p) = o(p)$ as $p \to \infty$. This means that, *e.g.*, it is not possible to replicate a call option with a finite amount of risky asset.

Sufficient condition. In order to have finite replication cost for all prices $p > 0$, it suffices for the payoff function f to have $\alpha > 0$ and a growth of at most

$$f(p) \leq Cp^{1-\varepsilon},$$

for some $C > 0$, $\varepsilon > 0$ and for all $p \geq p_0$. The proof is nearly identical to the previous, since, for any $p > 0$,

$$g(p) \leq \int_p^{p_0} \frac{f'(p)}{p}\, dp + \int_{p_0}^\beta \frac{f'(p)}{p}\, dp \leq D + C(1-\varepsilon) \int_{p_0}^\beta p^{-(1+\varepsilon)}\, dp \to D + C(1-\varepsilon)\frac{1}{p_0^\varepsilon \varepsilon},$$

where $D = \int_p^{p_0} f'(p)/p\, dp$ is finite since $p > 0$, and we assume $\varepsilon < 1$ for convenience. (If $\varepsilon \geq 1$ in the original statement, then we can always choose $\varepsilon < 1$ as it is a strictly worse bound.)

1.3 Arbitrageur earnings

From §1.1, we know that, because the portfolio given by $(f(p), g(p))$ yields a concave payoff, then arbitrageurs will be incentivized to arbitrage against it and will make the price of the CFMM match that of an external market (see, *e.g.*, [AC20]). We prove this directly here, using a slightly different method.

More specifically, given that the arbitrageur is able to choose any q which leads to a portfolio allocation of $(f(q), g(q))$ for the liquidity provider, we show that, if an external market has price $\alpha \leq p \leq \beta$, then p is an optimal choice for the portfolio allocation in that it maximizes the arbitrageur's earnings.

Maximum profit. Arbitrageurs seek to maximize their own profit and therefore minimize the portfolio value of the liquidity provider. This is expressed by the following problem:

$$\text{minimize} \quad f(q) + pg(q), \tag{8}$$

with variable $\alpha \leq q \leq \beta$. Taking the derivative of the objective and using the definition of g, this can be written

$$f'(q) + pg'(q) = f'(q) - p\frac{f'(q)}{q} = f'(q)\left(1 - \frac{p}{q}\right).$$

Note that, since $f' \geq 0$ by definition, then the objective is unimodal as its derivative changes signs at most once. Additionally, the first order optimality condition,

$$f'(q)\left(1 - \frac{p}{q}\right) = 0,$$

implies that choosing $p/q = 1$ (that is, $p = q$) is a solution with portfolio value $f(p) + pg(p)$, when the market price is p.

Nonnegativity of profit. The profit of an arbitrageur is the negative of the change in the portfolio value when the price changes from p to p', which is

$$p'(g(p) - g(p')) + f(p) - f(p'). \tag{9}$$

Because p is a feasible point for the original problem (8), then we have that

$$f(p') + p'g(p') \leq f(p) + p'g(p),$$

which yields, after rearrangement:

$$p'(g(p) - g(p')) + f(p) - f(p') \geq 0.$$

Total earnings. Given a sequence of price changes $p_0, p_1, \ldots, p_n$, the total earnings, using (9), are

$$\sum_{i=1}^{n} p_i(g(p_{i-1}) - g(p_i)) + f(p_{i-1}) - f(p_i) = f(p_0) - f(p_n) - \sum_{i=1}^{n} p_i(g(p_i) - g(p_{i-1})).$$

Taking limits, we find that the total earnings are

$$W = f(P_0) - f(P_T) - \int_0^T P_t \, dg(P_t),$$

where P_t is a price process with $0 \leq t \leq T$, and the integral is to be interpreted in the Itô sense. Integrating by parts, we can write this as the slightly more interpretable form:

$$W = V(P_0) - V(P_T) + \int_0^T g(P_t) \, dP_t, \tag{10}$$

where V is the portfolio value function described in (3). From the previous discussion, we know that the total arbitrageur profit is nonnegative, $W \geq 0$, for any price process P_t.

Discussion. We can interpret the individual terms in the arbitrageur's total earnings, equation (10), in a simple way. The first term, $V(P_0) - V(P_T)$ is the negative of the payoff to the liquidity provider, which is received from having the underlying portfolio rebalanced as the price of the asset changes from time $t = 0$ to time $t = T$. The second term, $\int_0^T g(P_t) \, dP_t$, is a 'path-dependent' term that comes from the arbitrageur performing arbitrage at each time period.

2 Examples

In this section, we provide a few useful examples of payoffs which can easily be implemented in practice using the methods presented in the previous section.

2.1 Cash-or-nothing call

The simplest monotonic function which can be replicated is perhaps the *cash-or-nothing call*, which has payoff:

$$f(p) = \begin{cases} 0 & p \leq p_0 \\ 1 & p > p_0, \end{cases}$$

for some $p_0 > 0$ and all $p \geq 0$ (*i.e.*, $\alpha = 0$ and $\beta = \infty$). The amount of risky asset is given by:

$$g(p) = \int_p^\infty \frac{df(q)}{q} = \frac{1 - f(p)}{p_0}.$$

(This integral can be interpreted in many ways, as the derivative of f doesn't exist at $p = p_0$, with perhaps the simplest being a Riemann–Stieltjes integral since f is monotonic and $1/p$ is differentiable.)

Interpretation. In fact, because the cash-or-nothing call is so simple, the functions f and g can be intuited and proven without needing the explicit formula given in (1). Since every nonnegative, monotonic function can be written as the limit of the sum of a number of cash-or-nothing calls, we can recover (1) using only this reasoning. This provides an alternative method for recovering most of the results provided in this paper and is very similar in spirit to the Carr–Madan replication method in finance [CM01, App. 1].

Trading function. Because g is not continuous, there is no guarantee that there exists a $p \geq 0$ such that $g(p) = R_2$, even when $0 \leq R_2 \leq 1/p_0$, so the simplification in (7) does not apply. On the other hand, it is not hard to show that

$$g^{-1}(R_2) = \begin{cases} p_0 & R_2 > 0 \\ +\infty & \text{otherwise,} \end{cases}$$

and therefore that $V(g^{-1}(R_2)) = 1$ for any $R_2 \geq 0$. The resulting trading function is then

$$\psi(R_1, R_2) = R_1 + p_0 R_2 - 1,$$

where we have defined $0 \cdot \infty = 0$ for convenience. Note that this is just the linear market maker, defined in [AAE$^+$21, §2.4].

2.2 Capped call

Another example of a payoff is that of the *capped call*, whose payoff function is defined as

$$f(p) = \begin{cases} 0 & p \leq p_0 \\ p - p_0 & p_0 < p \leq p_1 \\ p_1 - p_0 & p > p_1, \end{cases}$$

where $0 < p_0 \leq p_1$ are user-defined constants. In this case, we have that

$$g(p) = \begin{cases} \log(p_1/p_0) & p \leq p_0 \\ \log(p_1/p) & p_0 < p \leq p_1 \\ 0 & p > p_1. \end{cases}$$

Trading function. The trading function for a capped call can be easily computed using the simplification provided in (7), because the function g is continuous. Using the definition of g, we have

$$g^{-1}(x) = p_1 e^{-x}$$

whenever $0 \leq x \leq \log(p_1/p_0)$. The trading function can then be written

$$\psi(R_1, R_2) = R_1 - f(g^{-1}(R_2)) = R_1 + p_0 - p_1 e^{-R_2},$$

when $0 \leq R_2 \leq \log(p_1/p_0)$, and the reserves are otherwise invalid.

2.3   Black-Scholes cash-or-nothing call

The preceding examples give conditions for the terminal payoffs of binary and capped calls, respectively. As discussed in [AEC21], it is often more useful to work with the price of a derivative contract under a parametric model. This typically requires significantly lower collateral to achieve a similar terminal payoff. One such model is that of Black-Scholes. Here we derive the payoff the a binary call under this model. In this case the payoff is defined as

$$f(p) = \Phi(d(p))$$

where $\Phi(\cdot)$ is the normal CDF and

$$d(p) = \frac{\log(p/K) - \tau\sigma^2/2}{\sigma\sqrt{\tau}}.$$

Here, $\tau > 0$ is the time to maturity, $K \geq 0$ is the strike price and $\sigma \geq 0$ is the implied volatility (we assume zero interest rates to minimize notation).

Integral simplification.   There is a simple but very useful 'trick' to evaluate payoffs of the form

$$f(p) = r(s(p)),$$

where s is a monotonically increasing function. Given that we want to evaluate g, then:

$$g(p) = \int_p^\infty \frac{r'(s(q))s'(q)}{q} \, dq = \int_{s(p)}^{s(\infty)} \frac{r'(u)}{s^{-1}(u)} \, du,$$

where the last equality follows by using the u-substitution $u = s(q)$.

Replication cost.   Using this trick, we have that the amount of risky asset is given by:

$$g(p) = \frac{1}{K} \int_{d(p)}^\infty \frac{\phi(u)}{\exp(\sigma\sqrt{\tau}u + \tau\sigma^2/2)} du = \frac{1}{K} \left(1 - \Phi(d(p) + \sigma\sqrt{\tau}) \right),$$

where $\phi(q) = \Phi'(q) = \exp(-q^2/2)/\sqrt{2\pi}$. As before, we may use (7), because the function g is continuous. Using the definition of g, we have

$$g^{-1}(x) = Ke^{\sigma\sqrt{\tau}\Phi^{-1}(1-Kx)-\tau\sigma^2/2}$$

From (7), after some cancellations we have

$$\psi(R_1, R_2) = R_1 - \Phi(\Phi^{-1}(1 - KR_2) - \sigma\sqrt{\tau})$$

which coincides with the trading function derived in [AEC21] for a covered call under Black-Scholes. (As noted in [AEC21], replicating in this manner requires additional capital as the portfolio value function is pointwise strictly decreasing in the time to maturity, τ. This 'gain' as $\tau \downarrow 0$ is sometimes called "theta" in finance.)

2.4 Logarithmic payoff

It is also possible to replicate more complicated payoffs. One such example is the *logarithmic payoff* which is given by

$$f(p) = \begin{cases} 0 & p < p_0 \\ \log(p/p_0) & p \geq p_0. \end{cases}$$

Using the above, then the replication cost at p is:

$$g(p) = \begin{cases} 1/p_0 & p < p_0 \\ 1/p & p \geq p_0. \end{cases}$$

Note that the total amount to cover goes to infinity as $p_0 \downarrow 0$.

Trading function. The trading function is also an exercise in algebra, since the function g is continuous and we can use (7):

$$\psi(R_1, R_2) = R_1 + \log(p_0 R_2),$$

where the range of valid reserves is $0 \leq R_2 \leq 1/p_0$.

Arbitrageur earnings. Using equation (10), we can find how much an arbitrageur should expect to earn when the price of the risky asset follows a geometric Brownian motion with stochastic differential

$$dP_t = P_t \sigma dW_t,$$

where W_t is a standard Brownian motion. The true portfolio value function is given by

$$V(p) = \begin{cases} p/p_0 & p < p_0 \\ 1 + \log(p/p_0) & p \geq p_0. \end{cases}$$

This portfolio value function is difficult to handle directly, so we will consider the following portfolio value function:

$$V(p) = 1 + \log(p/p_0),$$

which is 'approximately' equal to the true portfolio value function when p_0 is small. Using this latter approximation, we then have:

$$W = \log[P_0/P_T] + \int_0^T \sigma dW_t.$$

Taking expectations gives

$$E[W] = \frac{1}{2}\sigma^2 T.$$

In other words, the arbitrageur's expected payoff (approximately) matches that of a variance swap [Neu94]. Loosely speaking, the right to arbitrage a no-fee CFMM with a logarithmic payoff may be used to replicate a variance swap without an oracle. Of course, in practice, the above argument is impractical as it requires unbounded capital (as $p_0 \downarrow 0$ is required), but we expect that finite reserve amounts will suffice to provide similar payoffs.

2.5 Capped power payoffs

Given any power, we can find the market maker for the payoff

$$
f(p) = \begin{cases} 0 & p < p_0 \\ p^\alpha - p_0^\alpha & p_0 \le p \le p_1 \\ p_1^\alpha - p_0^\alpha & p > p_1, \end{cases}
$$

where $0 \le p_0 \le p_1 \le \infty$ and $\alpha \in \mathbf{R}$ is a real number. It is an exercise in integration to show

$$
g(p) = \frac{\alpha}{\alpha - 1}(p_1^{\alpha-1} - p^{\alpha-1}),
$$

if $p_0 \le p \le p_1$, while $g(p) = g(p_0)$ if $p < p_0$ and $g(p) = 0$, otherwise. Note that $p_1 < \infty$ is necessary if $\alpha \ge 1$ in order to have a finite replication cost. This portfolio generalizes that of the the capped call presented in §2.2 as the special case when $\alpha = 1$.

Trading function. We can write

$$
g^{-1}(x) = \left(p_1^{\alpha-1} + \frac{1-\alpha}{\alpha}x \right)^{1/(\alpha-1)},
$$

with domain $0 \le x \le g(p_0)$. Because g is continuous, we can use the simplification in (7), so the trading function can be written as:

$$
\psi(R_1, R_2) = R_1 + p_0^\alpha - \left(p_1^{\alpha-1} + \frac{1-\alpha}{\alpha}R_2 \right)^{\alpha/(\alpha-1)},
$$

where the reserves are valid only when $0 \le R_2 \le g(p_0)$.

2.6 Constant proportion portfolios

What happens if a liquidity provider is seeking a constant proportion of their wealth to be in one asset or the other? As is well known from the literature, this is done by the class of constant mean market makers [MM19, AZR20], but we can also easily recover this from first principles using this framework.

Requirements. In this problem, a user wishes to have a portfolio allocation $(f(p), g(p))$ of the numéraire and risky assets at each price p such that $0 < w < 1$ of the portfolio value is in the numéraire, while $(1-w)$ of the portfolio value is in the risky asset; in other words, f and g must satisfy

$$
wf(p) = (1-w)pg(p).
$$

Dividing by p, taking the derivative of both sides, and using the definition of g, we have:

$$
pf'(p) = wf(p),
$$

12

after some simplifications. It is a standard exercise to show that the unique family of solutions f to this problem is given by

$$f(p) = Cp^w,$$

where $C \geq 0$ is a constant that determines the total portfolio value. This implies that the function g is given by:

$$g(p) = C \frac{w}{1-w} \frac{1}{p^{1-w}}.$$

Note that g is a continuous function on the positive reals.

Trading function. Using the definition of g above, we can write

$$g^{-1}(x) = \left(\frac{1-w}{w} \frac{x}{C} \right)^{-\frac{1}{1-w}},$$

which implies

$$\psi(R_1, R_2) = R_1 - f(g^{-1}(R_2)) = R_1 - \left(\frac{R_2}{C} \frac{1-w}{w} \right)^{-\frac{w}{1-w}}.$$

By multiplying both sides of the equation by the right-most term and taking the $(1-w)$th power, we can write the equivalent trading function:

$$\tilde{\psi}(R_1, R_2) = R_1^{1-w} R_2^w - C',$$

where $C' = (Cw/(1-w))^{w/(1-w)}$. The trading functions are equivalent in the sense that R_1 and R_2 satisfy $\psi(R_1, R_2) \geq 0$ if, and only if, $\tilde{\psi}(R_1, R_2) \geq 0$. This is the classic trading function for constant mean market makers.

3 Further discussion

In this section, we share some further thoughts and (nearly immediate) extensions of the method presented above.

Staking. Proof of Stake (PoS) protocols allow a user to lock a digital asset into a pool (a process known as *staking*) in order to provide a service to the network. In return, the network distributes block rewards (a form of subsidy) and collected fees to stakers. The most popular usage of PoS networks is executing consensus algorithms of replicating state machines, such as blockchains. Many CFMMs exist as contracts whose state updates and execution are maintained by a decentralized PoS network.

A number of protocols such as Osmosis [AO21] and Penumbra [dV21] allow users to stake not only the underlying staking asset but the liquidity provider shares that contain the staking asset to receive consensus rewards. For instance, if a network uses a risky asset A

for staking, such networks would allow users to stake any A-numéraire LP share to receive rewards. One reason a network might want to incentivize such a pool is to ensure that there is sufficient on-chain liquidity to purchase asset A with the numéraire, regardless of external market liquidity. The rewards earned by liquidity provider share stakers would be lower than those earned by those staking the base asset. However, liquidity providers would effectively be compounding their returns as they get both CFMM fees and staking rewards.

A PoS system with liquidity provider share staking also can be used to construct staking derivatives, which allows for improved capital efficiency. This capital efficiency comes from allowing liquidity providers to borrow against their locked shares, provided that price of the underlying is above a certain threshold. Staking derivatives can be constructed as capped monotone payoffs [CE20] and the construction of monotone replication in §1.1 can be enforced by a consensus protocol. In particular, while the right to execute the option to liquidate an LP share and realize a position of $f(p)$ unit of numéraire is only bounded below by $f(p)$ in general, it can be made to exactly equal $f(p)$ when a consensus protocol buys the right to execute an LP share liquidation. This is because a consensus protocol controls when the precise liquidation occurs and if added as a consensus rule, will only happen *exactly* when the portfolio value dropped below a threshold. This suggests that staking derivatives are natural consumers of monotone replication.

Continuous liquidation interpretation. Another interpretation of monotone replication via a token that allows for one side of the LP share to be liquidated is as a loan that is being continuously liquidated as the price changes. More specifically, suppose that an LP share is created with $(f(p_0), g(p_0))$ units of the risky asset and numéraire, respectively. Further, suppose that rights to the numéraire portion of the pool are sold (as in §1.1). Now, if the price changes from p_0 to p_1 over a time interval of length h, then holding share through the price change is the same as selling the option for $g(p_0)$ units of numéraire, having it executed at p_1, and using the proceeds to mint a new share which has the allocation $(f(p_1), g(p_1))$. If we take $h \to 0$, then this equivalence can be viewed as saying that holding the liquidity provider share is equivalent to continuously rebalancing by selling numéraire rights and using the proceeds upon execution to recreate another share and resell numéraire rights.

Negative reserves. Note that we do not require that f be nonnegative at any point in the presentation except to assert that the portfolio value function is nonnegative. We can, instead, allow $f(p)$ to be negative in so far as the portfolio value function is nonnegative at all times. This idea corresponds to the fact that the portfolio is allowed to short an asset, so long as the position remains solvent, *i.e.*, so long as the portfolio value function is nonnegative. We can relax this further by requiring only that the portfolio position is nonnegative in an interval of prices, while making sure that the portfolio holder's collateral is liquidated when the price leaves this interval.

4 Conclusion

We have shown how to replicate nonnegative, monotonic payoff functions (somewhat generalizing the result of [AEC21]) by allowing liquidity providers to sell the rights to a specific component of their portfolio, rather than their entire portfolio. This generalization allows us to realize a number of payoffs that were previously thought to require explicit leverage to replicate with CFMM liquidity provider shares. Such a replication increases the space of unlevered structured products that can be created with liquidity provider shares which don't require additional collateral. Our results are likely best implemented in proof-of-stake (PoS) systems that interact with liquidity provider shares to construct simple staking derivatives. Here, the PoS network is the buyer of numéraire exposure. Possible future work directions include adding the effect of fees on monotone replications and computing expected liquidity provider profits in different fee regimes after selling a component of the underlying portfolio.

References

[AAE+21] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant function market makers: Multi-asset trades via convex optimization. *arXiv preprint arXiv:2107.12484*, 2021.

[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*, AFT '20, page 80–91, New York, NY, USA, 2020. Association for Computing Machinery.

[AEC21] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers. *arXiv preprint arXiv:2103.14769*, 2021.

[AKC+19] Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and Tarun Chitra. An analysis of Uniswap markets. *Cryptoeconomic Systems*, 2019.

[All] Nathan Allman. Ondo Vault.

[AO21] Sunny Agrawal and Dev Ojha. Vision for Osmosis, May 2021.

[AZR20] Hayden Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core. 2020.

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

[CAEK21] Tarun Chitra, Guillermo Angeris, Alex Evans, and Hsien-Tang Kao. A note on borrowing constant function market maker shares. 2021.

[CE20] Tarun Chitra and Alex Evans. Why stake when you can borrow? *Available at SSRN 3629988*, 2020.

[Cla20]   Joseph Clark. The replicating portfolio of a constant product market. *Available at SSRN 3550601*, 2020.

[Cla21]   Joseph Clark. The replicating portfolio of a constant product market with bounded liquidity. *Available at SSRN 3898384*, 2021.

[CM01]   Peter Carr and Dilip Madan. Towards a theory of volatility trading. *Option Pricing, Interest Rates and Risk Management, Handbooks in Mathematical Finance*, pages 458–476, 2001.

[dV21]   Henry de Valence. Sealed-bid batch auctions, 2021.

[EAC21]   Alex Evans, Guillermo Angeris, and Tarun Chitra. Optimal fees for geometric mean market makers. *arXiv preprint arXiv:2104.00446*, 2021.

[ESGC21]   Shayan Eskandari, Mehdi Salehi, Wanyun Catherine Gu, and Jeremy Clark. SoK: Oracles from the ground truth to market manipulation. *ACMAdvances in Financial Technology*, 2021.

[Eva20]   Alex Evans. Liquidity provider returns in geometric mean markets. *arXiv preprint arXiv:2006.08806*, 2020.

[MM19]   Fernando Martinelli and Nikolai Mushegian. Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor. 2019.

[Neu94]   Anthony Neuberger. The log contract. *The Journal of Portfolio Management*, 20(2):74–80, 1994.

[ZCP18]   Yi Zhang, Xiaohong Chen, and Daejun Park. Formal specification of constant product $xy = k$ market maker model and implementation. 2018.

A   RMMs simplification

In [AEC21], it is shown that, given a portfolio value function $U : \mathbf{R}_+^2 \to \mathbf{R}$ which is nonnegative, nondecreasing, concave, and 1-homogeneous, the trading function defined as

$$\psi(R_1, R_2) = \inf_{c_1, c_2} (c_1 R_1 + c_2 R_2 - U(c_1, c_2))$$

has U as its portfolio value function. Additionally, given a scalar portfolio value function V, that is nonnegative, nondecreasing, concave, and depends only on the relative price p of asset 1 to asset 2, it can be turned to a 1-homogeneous function U that depends on the prices of both assets, by use of the perspective transform:

$$U(c_1, c_2) = c_1 V(c_2/c_1)$$

where we assume that $U(0,0) = 0$ and $U(0, c_2) = -\infty$ for $c_2 > 0$. So, we can write:

$$\psi(R_1, R_2) = \inf_{c_1, c_2} \left(c_1 R_1 + c_2 R_2 - c_1 V(c_2/c_1) \right).$$

Noting that

$$\psi(R_1, R_2) = \inf_{c_1} c_1 \left(\inf_{c_2} \left(R_1 + (c_2/c_1) R_2 - V(c_2/c_1) \right) \right)$$

and letting $p = c_2/c_1$ we get

$$\psi(R_1, R_2) = \inf_{c_1} c_1 \left(\inf_{p} \left(R_1 + p R_2 - V(p) \right) \right) = \begin{cases} 0 & \inf_p \left(R_1 + p R_2 - V(p) \right) \geq 0 \\ -\infty & \text{otherwise.} \end{cases}$$

It is nearly immediate that

$$\tilde{\psi}(R_1, R_2) = \inf_{p} \left(R_1 + p R_2 - V(p) \right),$$

is equivalent to ψ in that $\psi(R_1, R_2) \geq 0$ if, and only if, $\tilde{\psi}(R_1, R_2) \geq 0$. The proof holds throughout even if p is constrained to lie in the interval $[\alpha, \beta]$ for $0 \leq \alpha \leq \beta \leq +\infty$.