Principles of decentralized finance, June – July 2022 G. Angeris, T. Diamandis

Problem set 4: Advanced results in CFMMs

1 Replicating portfolios with CFMMs

In class, we showed how to replicate a concave, homogeneous, nondecreasing payoff using a CFMM. It turns out, in the two token setting, we can replicate *any* nondecreasing payoff using a CFMM. (There are some basic conditions on the growth of the function which we will see next.) This problem will guide you through how to construct such a CFMM.

Consider a CFMM that has two assets: a risky asset (*e.g.*, Ethereum) and a USD-equivalent (*e.g.*, DAI). Our goal is to create a CFMM such that one side of an LP position always has value $f(p)$ where p is the price of the risky asset in terms of the numeraire. Specifically, 1 ETH $= p$ DAI, and p can be interpreted as the price of 1 ETH token in DAI (or USD as 1 DAI $\approx$ 1 USD).

Our approach will be to construct a two token CFMM (defined by its trading function φ) such that arbitrageurs are incentivized to keep the DAI reserves at $f(p)$ as the price of ETH, p, fluctuates. In essence, we are "outsourcing" portfolio rebalancing to sophisticated players and only assuming these players are profit-maximizing. We assume that f is nonnegative, strictly increasing, and differentiable on its domain; *i.e.*, $f(p) \geq 0$ and $f'(p) > 0$ for $p > 0$. (Note that we do *not* assume that f is convex or concave.)

a) For a given price p, the CFMM must hold $f(p)$ DAI in reserves. Assume that the price of ETH is p_1 and the CFMM holds both $f(p_1)$ DAI and some amount of ETH. If the price changes from p_1 to p_2, show that the amount of ETH the CFMM needs to "buy" (or "sell") is given by

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

Hint: if the price increases from p to $p+h$, the CFMM must sell some ETH to increase its DAI position by $f(p+h) - f(p)$.

If the CFMM trades using this strategy (by incentivizing arbitrageurs to perform said trades), it must have enough ETH in its reserves to buy DAI as the exchange rate goes up. At some price p, it would then need to hold at least

$$g(p) = \int_{p}^{\infty} \frac{f'(q)}{q} dq$$

in ETH to execute this strategy, as p may increase without bound (colloquially, ETH may *moon*) in the future. (Assume that f is such that $g(p)$ is finite for $p \geq 0$.) If the CFMM's reserves contain exactly $f(p)$ DAI and $g(p)$ ETH, their value in DAI is

$$V(p) = f(p) + pg(p).$$

From class, we know that this is the portfolio value function in the case that the first asset is worth exactly 1 DAI.

b) Show that we can equivalently write V as

$$V(p) = V(0) + \int_0^p g(q)dq.$$

c) Show that $V(p)$ is a nonnegative, nondecreasing, concave function on $p > 0$.

Equipped with reserves $(f(p), g(p))$ for a given exchange rate p, it is natural to consider the set of reserves that allow the CFMM to cover its obligation as the price p varies. For this, we will consider an object similar to the epigraph of a function, called the *dominating reserves*, defined as the set

$$S = \{x \in \mathbf{R}^2 \mid x_1 \geq f(p),\ x_2 \geq g(p) \text{ for some } p \geq 0\}.$$

(In finance, we sometimes say that a vector x *dominates* a vector y whenever $x \succeq y$.) We will show that the set S is a convex set and can therefore be easily optimized over.

d) Find a (simple) function φ such that $x_2 \geq \varphi(x_1)$ if, and only if, $x \in S$.

e) Show that φ is convex. Argue that this shows that S is a convex set.

This means that φ, defines a CFMM's trading function with a specific important property: arbitrageurs are incentivized to always keep the reserves at $(f(p),\ g(p))$. (Why?) If we sell of the right to withdraw the first component of the reserves as a contract, then the payoff of that contract, on execution, is $f(p)$, as we wanted to show. (Check out the protocols Primitive[1] and Composite[2], which are applying these ideas in the wild.) Interestingly, this new function φ and the portfolio value function V are intimately related. This relation provides a means to construct a CFMM for a given portfolio value function.

f) Show that φ^{-1} is the conjugate of $-V$ with negated arguments, *i.e.*, $\varphi^{-1}(y) = (-V)^*(-y)$.

(Note that this is a special, simpler to prove, case of the result we showed in class when we have two tokens.)

[1] `https://primitive.xyz`

[2] `https://www.composite.org`