Automated Market Making of Trading Pool

ALEX[*]

5 January 2023

Abstract

We introduce a new invariant function associated with generalised mean that underpins the ALEX AMM. ALEX builds DeFi primitives targeting developers looking to build ecosystem on Bitcoin, enabled by Stacks. With a suitable parameterisation, the invariant function supports both risky pairs (i.e. $xy = L$), stable pairs (i.e. $x + y = L$) and any linear combination in-between (i.e. Curve). We also show that our invariant function maps to the liquidity distribution of Uniswap V3.

Introduction

At ALEX, we build DeFi primitives targeting developers looking to build ecosystem on Bitcoin, enabled by Stacks. As such, we focus on trading, lending and borrowing of crypto assets with Bitcoin as the settlement layer and Stacks as the smart contract layer. At the core of this focus is the automated market making ("AMM") protocol, which allows users to exchange one crypto asset with another trustlessly. This paper focuses on technical aspects of AMM.

AMM and Invariant Function

ALEX AMM is built on three beliefs: (i) it is mathematically neat and reflect economic demand and supply and (ii) it is a type of mean, like other AMMs. We will firstly review some desirable features of AMM that ALEX hopes to exhibit.

Properties of AMM

AMM protocol, which provides liquidity algorithmically, is the core engine of DeFi. In the liquidity pool, two or more assets are deposited and subsequently swapped resulting in both reserve and price movement. The protocol follows an invariant function $f(X) = L$, where $X = (x_1, x_2, \ldots, x_d)$ is d dimension representing d assets and L is constant. When $d = 2$, which is the common

---

[*]https://www.alexgo.io; Corresponding author: Chan Ahn (alexd@alexgo.io)

practise by a range of protocols, AMM $f(x_1, x_2) = L$ can be expressed as $x_2 = g(x_1)$. Although it is not always true, g tends to be twice differentiable and satisfies the following

- monotonically decreasing, i.e. $\frac{dg(x_1)}{dx_1} < 0$. This is because price is often defined as $-\frac{dg(x_1)}{dx_1}$. A decreasing function ensures price to be positive.

- convex, i.e. $\frac{d^2 g(x_1)}{dx_1^2} \geq 0$. This is equivalent to say that $-\frac{dg(x_1)}{dx_1}$ is a non-increasing function of x_1. It is within the expectation of economic theory of demand and supply, as more reserve of x_1 means declining price.

Meanwhile, f can usually be interpreted as a form of mean, for example, mStable relates to arithmetic mean, where $x_1 + x_2 = L$ (constant sum formula); one of the most popular platforms Uniswap relates to geometric mean, where $x_1 x_2 = L$ (constant product formula); Balancer, which our collateral rebalancing pool employs, applies weighted geometric mean. Its AMM is $x_1^{w_1} x_2^{w_2} = L$ where w_1 and w_2 are fixed weights. ALEX AMM extends these to create a generalised mean.

ALEX AMM

After extensive research, we consider it possible for ALEX AMM to be connected to generalised mean defined as

$$\left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)^{\frac{1}{p}}$$

where $0 \leq p \leq 1$. The expression might remind readers of p-norm when $x_i \geq 0$. It is however not true when $p < 1$ as triangle inequality doesn't hold.

When $d = 2$ and $p = 1 - t$ ($0 \leq t < 1$) is fixed, the core component of generalised mean is assumed constant as below.

$$x_1^{1-t} + x_2^{1-t} = L$$
$$-\frac{dx_2}{dx_1} = \left(\frac{x_2}{x_1} \right)^t$$

This equation is regarded reasonable as AMM, because (i) function g where $x_2 = g(x_1)$ is monotonically decreasing and convex; and (ii) The boundary value of $t = 0$ and $t = 1$ corresponds to constant sum and constant product formula respectively. When t decreases from 1 to 0, price $-\frac{dg(x_1)}{x_1}$ gradually converges to 1, i.e. the curve converges from constant product to constant sum (see Appendix A for the relevant proofs). Though purely theoretical at this stage, Appendix B maps to the liquidity distribution of Uniswap V3. This is motivated by an independent research from Paradigm.

Trading Formulae

Market transaction, which involves exchange of one crypto asset and another, satisfies the invariant function. Please note the formulae do not account for the fee re-investment, which results in a slight increase of L after each transaction, like Uniswap V2.

Out-Given-In

In order to purchase Δy amount of token Y from the pool, the buyer needs to deposit Δx amount of token X. Δx and Δy satisfy the following

$$(x + \Delta x)^{1-t} + (y - \Delta y)^{1-t} = x^{1-t} + y^{1-t}$$

After each transaction, balance is updated as below: $x \to x + \Delta x$ and $y \to y - \Delta y$. Rearranging the formula results in

$$\Delta y = y - \left[x^{1-t} + y^{1-t} - (x + \Delta x)^{1-t} \right]^{\frac{1}{1-t}}$$

When transaction cost exists, the actual deposit to the pool is less than Δx. Assuming $\lambda \Delta x$ is the actual amount and $(1 - \lambda)\Delta x$ is the fee, above can now be expressed as

$$(x + \lambda \Delta x)^{1-t} + (y - \Delta y)^{1-t} = x^{1-t} + y^{1-t}$$

$$\Delta y = y - \left[x^{1-t} + y^{1-t} - (x + \lambda \Delta x)^{1-t} \right]^{\frac{1}{1-t}}$$

To keep L constant, the updated balance is: $x \to x + \lambda \Delta x$ and $y \to y - \Delta y$.

In-Given-Out

This is the opposite case to above. We are deriving Δx from Δy.

$$\Delta x = \frac{1}{\lambda} \left[x^{1-t} + y^{1-t} - (y - \Delta y)^{1-t} \right]^{\frac{1}{1-t}} - x$$

In-Given-Price

Sometimes, trader would like to adjust the price, perhaps due to deviation of AMM price to the market value. Define p' the AMM price after rebalancing the token X and token Y in the pool

$$p' = \left(\frac{y - \Delta y}{x + \lambda \Delta x} \right)^t$$

Then, the added amount of Δx can be calculated from the formula below

$$(x + \lambda \Delta x)^{1-t} + (y - \Delta y)^{1-t} = x^{1-t} + y^{1-t}$$

$$1 + \left(\frac{y}{x}\right)^{1-t} = \left(1 + \lambda \frac{\Delta x}{x}\right)^{1-t} + (\frac{y - \Delta y}{x})^{1-t}$$

$$1 + p^{\frac{1-t}{t}} = \left(1 + \lambda \frac{\Delta x}{x}\right)^{1-t} + p'^{\frac{1-t}{t}} \left(1 + \lambda \frac{\Delta x}{x}\right)^{1-t}$$

$$\Delta x = \frac{x}{\lambda} \left[\left(\frac{1 + p^{\frac{1-t}{t}}}{1 + p'^{\frac{1-t}{t}}}\right)^{\frac{1}{1-t}} - 1 \right]$$

Appendix

A   Generalised Mean when d=2

ALEX's invariant function is $f(x_1, x_2; p) = x_1^p + x_2^p = L$. It can be rearranged as $x_2 = g(x_1) = (L - x_1^p)^{\frac{1}{p}}$. x_1 and x_2 should both be positive meaning the liquidity pool contains both tokens.

Theorem

When $0 < p < 1$, $g(x_1)$ is monotonically decreasing and convex.

Proof

This is equivalent to prove $\frac{dg(x_1)}{dx_1} < 0$ and $\frac{d^2 g(x_1)}{dx_1^2} \geq 0$.

$$\frac{dg(x_1)}{dx_1} = \frac{1}{p}(L - x_1^p)^{\frac{1}{p}-1} \left(-px_1^{p-1}\right) = -\left(\frac{L - x_1^p}{x_1^p}\right)^{\frac{1-p}{p}} < 0$$

$$\frac{d^2 g(x_1)}{dx_1^2} = -\frac{1-p}{p} \left(\frac{L - x_1^p}{x_1^p}\right)^{\frac{1-2p}{p}} \left[\frac{-px_1^{p-1}x_1^p - (L - x_1^p)px^{p-1}}{x_1^2 p}\right]$$

$$= L(1 - p) \left(\frac{x_2}{x_1}\right)^{1-2p} x_1^{-p-1} \geq 0$$

The last inequality holds because each component is positive.

When $p = 1$, it is straightforward to see that the invariant function is constant sum. To show that the invariant function converges to constant product when $p = 0$, we will show and prove an established result in a generalised d dimensional setting.

Theorem

$$\lim_{p \to 0} \left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)^{\frac{1}{p}} = \left(\prod_{i=1}^{d} x_i \right)^{\frac{1}{d}}$$

Proof

$\left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)^{\frac{1}{p}} = \exp \left[\frac{\log \left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)}{p} \right]$ Applying L'Hospital rule to the exponent, which is 0 in both denominator and nominator when $p \to 0$, we have

$$\lim_{p \to 0} \frac{\log \left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)}{p} = \lim_{p \to 0} \sum_{i=1}^{d} \frac{\log(x_i)}{\sum_{j=1}^{d} \left(\frac{x_j}{x_i} \right)^p} = \frac{\sum_{i=1}^{d} \log(x_i)}{d}$$

Therefore

$$\lim_{p \to 0} \left(\frac{1}{d} \sum_{i=1}^{d} x_i^p \right)^{\frac{1}{p}} = \lim_{p \to 0} \exp \frac{\sum_{i=1}^{d} \log(x_i)}{d} = \left(\prod_{i=1}^{d} x_i \right)^{\frac{1}{d}}$$

Corollary

When d = 2,

$$x_1 x_2 = \lim_{p \to 0} \left[\frac{1}{2} (x_1^p + x_2^p) \right]^{\frac{2}{p}}$$

Proof of the corollary is trivial, as it is a direct application of the theorem. It shows that generalised mean AMM implies constant product AMM when $p \to 0$.

B   Liquidity Mapping to Uniswap v3

As Uniswap v3 is able to simulate liquidity curve of any AMM, we are interested in exploring the connection between ALEX's AMM and that of Uniswap's. Interesting questions include: what is the shape of the liquidity distribution? Which point(s) has the highest liquidity? We acknowledge that the section is more of a theoretical study for now.

Uniswap V3 AMM can be expressed as a function of invariant constant L with respect to price p, $L_{\text{Uniswap}} = \frac{dy}{d\sqrt{p}}$. For us, the difference in the invariant function means we can write price as $p = e^{rt}$ (or, equivalently, $r = \frac{1}{t} \ln p$) and we have

$$L_{\text{Uniswap}} = \frac{dy}{d\sqrt{p}} = \frac{2}{t} e^{-\frac{1}{2}rt} \frac{dy}{dr}$$

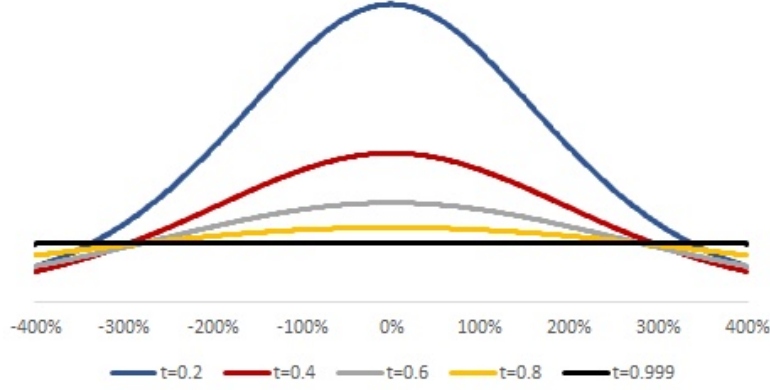Based on the previous sections, we can then express y as

Figure B.1: Liquidity mapping to Uniswap v3

$$y = \left[\frac{L}{1 + e^{-(1-t)r}}\right]^{\frac{1}{1-t}}$$

Therefore

$$\frac{dy}{dr} = L^{\frac{1}{1-t}} \frac{e^{-(1-t)r}}{\left(1 + e^{-(1-t)r}\right)^{\frac{2-t}{1-t}}}$$

$$L_{\text{Uniswap}} = \frac{2}{t} L^{\frac{1}{1-t}} \left(e^{\frac{r(1-t)}{2}} + e^{\frac{-r(1-t)}{2}}\right)^{\frac{-2+t}{1-t}}$$

$$= \frac{2}{t} L^{\frac{1}{1-t}} \left\{2\cosh\left[\frac{r(1-t)}{2}\right]\right\}^{\frac{-2+t}{1-t}}$$

Figure B.1 plots L_{Uniswap} against r (which is proportional to p) regarding various levels of t. When $0 < t < 1$, L_{Uniswap} is symmetric around 0% at which the maximum reaches . This is because

1. $\cosh\left[\left(\frac{r(1-t)}{2}\right)\right]$ is symmetric around $r = 0\%$ with minimum at 0% and the minimum value 1;

2. x^z is a decreasing function of x when x is positive and power z is negative. In our case, we have $z = \frac{-2+t}{1-t} < -1$. Therefore, it is the maximum rather than minimum that L_{Uniswap} achieves at 0.

Furthermore, the higher the t, the flatter the liquidity distribution is. When t approaches 1, i.e. AMM converges to the constant product formula, the liquidity distribution is close to a flat line. When t approaches 0, the distribution concentrates around 0%.

6