基于边界自适应的自动做市商模型

Boundary Adaptation Automatic Market Maker Model

Floralheaven

摘要：为了提升资金的利用率，Uniswap 、Curve 、balancer 选择了三种不同的道路，其实际应用都不同程度导致了 defi 积木建设难度的指数性增大。本文从目前的普遍应用基础出发设计了一种基于边界自适应的自动做市商模型，使 lp 提供者在继续使用 Uniswap V2 形式 lp 的基础上，获得与 Uniswap V3、Curve V2 相当的流动性增益，并保持了系统的简洁性与鲁棒性。

Abstract: In order to improve the utilization rate of funds, Uniswap, Curve, and Balancer have chosen three different paths, and their practical applications have all led to an exponential increase in the difficulty of building Defi blocks in varying degrees. This article proposes a boundary adaptive automatic market maker model based on the current widespread application foundation, which enables LP providers to obtain liquidity gains equivalent to Uniswap V3 and Curve V2 while continuing to use Uniswap V2 form LP, while maintaining the simplicity and robustness of the system.

简介：

Dex 项目的发展历史，是一场以流动性设计为基础创新要素的新兴去中心化基础设施大赛。从 Uniswap【0】 以其著名的「x * y = k」恒定产品池公式为大众普及到 curve【1】加入加法恒等式，为了提升资金的利用率，Uniswap 、Curve 和 Balancer 等产品选择了截然不同的道路。Uniswap V3【2】引入了区间流动性的功能，LP 可以自定义提供流动性的区间，人为优化资金使用率；而 Curve V2【3】在 V1 优化曲线策略基础上，通过增加参数使币种不限定于等价币种，并根据价格和流动性的变化动态调整，做到无需人为接入的自动化调节，提高了用户在非稳定币资产方面的交易体验，且显著减缓了滑点；Balancer【4】则选择了截然不同的方式，他通过内置资产管理者（Asset Manager）的功能，允许被授权的资产管理者从池子中提取一部分资金，将该资金转入许可的（白名单内）第三方协议中产生额外收益，从而提高闲置资金的收益率。例如稳定币的兑换池，一天只需要不到 30%就能使得各稳定币之间几乎无滑点交易，那剩余的 70%资金，就可以转入例如 AAVE，Compound 这样的借贷协议中进行放贷，产生额外的收益。其余类似 Bancor 、DODO 等项目进入了外部预言机，导致系统风险严重依赖于外部预言机，具有不可控风险，并且失去了市场定价权，即放弃了自己成为 Primary Market 的机会；而类似 Mooniswap【5】等项目使用自动根据偏移量逐次构建多条虚拟的曲线，使得套利交易者只能吸收到每一条虚拟曲线所规定的套利上限，而不再是一次性在原始曲线上完成大量套利，此类方法的缺点是需要仔细判别套利机会的出现，一定程度上也需要依赖外部因子；而且虚拟量缩短套利路径的过程需要动态构建大量曲线，对于高并发的系统，此类方法在工程上过于复杂，引入过多不确定性。可以看出，大量的流动性创新设计在近 10 年被提出，而作为原生初级市场，「x * y = k」以其无与伦比的简洁性得到了广泛的应用。我们能否设计一种体验更优秀、流动性可控、滑点可定制的 dex 产品仍旧是目前的研究热点。

本文对兑换的核心原则进行了阐述，并提出了一种基于边界自适应的自动做市商模型，使兑换过程在 Uniswap V3 基本假设下解决了流动性无法进行同质化处理的问题，并制作了 Xunion swap 进行了实验验证，结果表明新的模型可以根据不同币种特点进行不同的初始化设置，使兑换过程的滑点可定制，同时保持流动性使用同质化代币表示、便于 defi 乐高堆积的优良特性。

概念解释：

在文献 6 中作者提出了 Uniswap V3 和 curve V1 的揉合公式的中间具有类似形式的问题，并认为“Curve V1 揉合公式就是 Uni V3 平移公式的一个特殊形态。事实上，若在 Curve V1 揉合公式内再引入一个参数，x+y 的部分调整为 x+py，两者就完全等价了”，但其文章最后说到“Curve V1 揉合公式和 Uni V3 平移公式的相似性，又似乎不过是个不值一提的简单数学巧合罢了。”

在我看来，AMM 的进化，其实在 Uniswap V3 和 curve V1 的应用说明了：

价格生成机制只要能保证价格生成的鲁棒性并且不触碰到导致系统恶化的边界情况，币种具体的价格曲线并不需要为一条固定曲线，而可以是一种可以定制的曲线簇。

本文的方法在上述想法的指引下，提出了内部交易价格偏离函数概念，对 uniV3 提出的虚拟流动性概念进行了进一步拓展使用，最终使流动性保持了同质化代币形态，兑换过程相比于 curve V2 对流动性具有更高的优化水平，更低的系统复杂度，适用于各种类型的代币兑换，并且大幅降低了流动性的参数设置难度。

下面对本文提出的概念进行解释：

1、自适应区间做市

一种基于 uniswapV3 区间做市的方法，但本文通过对区间的自适应使 lp 不再使用 nft 形式，而是使用 erc20 形式；

2、虚拟流动性

借鉴于 uniV3 的概念，本文拓展了其使用方法，并且增加了参数关联性与自动化系数，使其具有更大的使用价值；

3、价格偏离变量

我们把 lp 对中两个币种数量的真实比值得到的价格与添加虚拟流动性后得到的实际价格进行比较得到的差值称之为价格偏离变量

4、偏离增益衰减函数

本文使用了一种指数函数作为对价格偏离的补偿，我们称其为偏离增益衰减函数

价格生成算法：

本文的算法构建，其基础模型仍然是到目前为止，价格发现能力优秀的 AMM 模型：

$$x \cdot y = K$$

当出现兑换过程时：

$$(x + \Delta x) \cdot (y - \Delta y) = K$$

$$\Delta y = y - \frac{K}{x + \Delta x}$$

此时上述参数 y、K、x、Δx 全为已知参数，就可以通过上式求出Δy。

解出方程后，可以得到此时的价格比值：

$$\frac{value_x}{value_y} = \frac{y - \Delta y}{x + \Delta x}$$

目前对此模型的唯一诟病就是全局流动性适应导致的区间流动性不够集中，使币种兑换时的滑点较大。

UniswapV3 使用了区间流动性概念，把上式改为：

$$(x_{true} + x_{virtual}) \cdot (y_{true} + y_{virtual}) = K$$

此式是对原式的平移，$x_{virtual}$、$y_{virtual}$就是我们人为添加的虚拟流动性，在 V3 中把这两个虚拟流动性与区间挂钩，推导出后续的使用方案。在本文中我们把此流动性与真实流动性进行挂钩，假设初始时虚拟流动性和真实流动性是一个 a 倍的比例关系，方程如下：

$$x_{virtual} = a * x_{true}$$

$$y_{virtual} = a * y_{true}$$

初始时的真实价格与虚拟价格保持一致，因此需要上两式系数都为 a；此系数代表流动性的聚集度的增益度，我们可以从 0~+∞的区间取值，实际取值范围可定为：

$$a \in [1,20]$$

此时前述模型更改为：

$$(x_{true} + a * x_{true}) \cdot (y_{true} + a * y_{true}) = K$$

当出现兑换过程时：

$$(x_{true} + a * x_{true} + \Delta x) \cdot (y_{true} + a * y_{true} - \Delta y) = K$$

$$\Delta y = y_{true} + a * y_{true} - \frac{K}{x_{true} + a * x_{true} + \Delta x}$$

当虚拟流动性为正时，同样的Δx，会使Δy 增大，即兑换出的另一种币种的数量增加。

由此可以看出，通过添加 a 倍虚拟流动性可以使兑换过程的滑点减小，且随着 a 的增大会不断增大。这时我们可以在此基础上定义币对价格比值：

$$\frac{value_x}{value_y} = \frac{y_{true} + a * y_{true} - \Delta y}{x_{true} + a * x_{true} + \Delta x}$$

但是这一过程结束后，此时币对中两币种的真实数量如下：

$$x_{true} = x_{true} + \Delta x$$

$$y_{true} = y_{true} - \Delta y$$

基于 uniV3 的推导可知，由于更改后的曲线会与 x、y 轴相交，此兑换将会被限制到一定区间。我们把上述初始状态：

$$x_{virtual} = a * x_{true}$$

$$y_{virtual} = a * y_{true}$$

作为稳定态，不满足上述方程的状态称为非稳定态。

可以看出，实际过程中其实都是非稳定状态。当偏离稳定状态后，进行兑换时，我们已知如下参数：$\frac{value_x}{value_y}$、x_{true}、y_{true}、a；我们以上述参数构建新的流动性公式：

$$(x_{true} + b) \cdot (y_{true} + a * y_{true}) = K$$

通过 value 值，我们有如下等式：

$$\frac{value_x}{value_y} = \frac{y_{true} + a * y_{true}}{x_{true} + b}$$

由此式可以推导出 b：

$$b = \frac{value_y * (y_{true} + a * y_{true})}{value_x} - x_{true}$$

$$\Delta y = y_{true} + a * y_{true} - \frac{K}{(x_{true} + b + \Delta x)}$$

由此即可计算出非稳定状态的Δy；

可以看出，此时我们以 y 值为中心，把流动性进行了重新分配。但是我们同时又知道，真实数量比值和价格比值偏离度越大，我们的流动性越小，此时我们需要减弱我们的流动性增益。为此，我们对参数 a 进行了重新设计。

我们定义稳定态时此参数为a_0；

偏离稳态后：

$$a_t = a_0 * f(pd)$$

$f(pd)$为偏离增益衰减函数，此函数定义为：

$$f(pd) = \frac{1}{1 + pd * pd}$$

pd 为内部存储量价格比值与外部价格比值的差值绝对值（Price deviation）与两个价格比值中小值的比值：

$$pd = \left|\frac{value_{x_{true}}}{value_{y_{true}}} - \frac{value_x}{value_y}\right| / \min\left(\frac{value_{x_{true}}}{value_{y_{true}}}, \frac{value_x}{value_y}\right)$$

$$pd = \left|\frac{y_{true}}{x_{true}} - \frac{value_x}{value_y}\right| / \min\left(\frac{y_{true}}{x_{true}}, \frac{value_x}{value_y}\right)$$

此函数取值区间为 0 到+∞，并且是对相对价格比值敏感，并且此函数在 0 到+∞区间内为单调递减函数，并且在：

$pd = 0$ 时，$f(x) = 1$

$pd = 1$ 时，$f(x) = 0.5$

$pd = +\infty$时，$f(x) = 0$

可以看出此函数符合我们对衰减的尺度要求。

$$a_t = a_0 * f(pd)$$

此时我们把流动性等式改写为：

$$(x_{true} + b_t) \cdot (y_{true} + a_t * y_{true}) = K$$

$$(x_{true} + b_t) \cdot (y_{true} + a_0 * f(pd) * y_{true}) = K$$

由此式可以推导出 b：

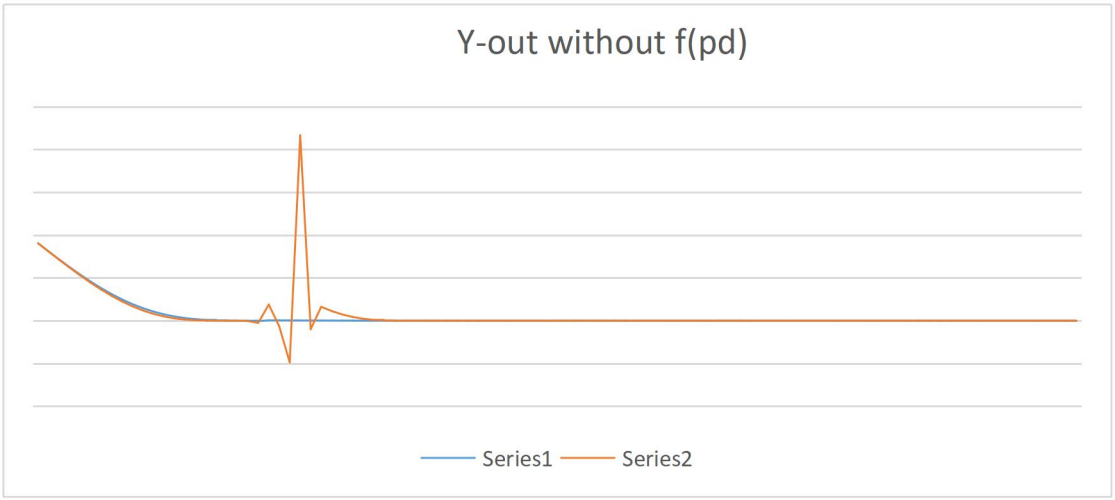
$$b_t = \frac{value_y * (y_{true} + a_0 * f(pd) * y_{true})}{value_x} - x_{true}$$

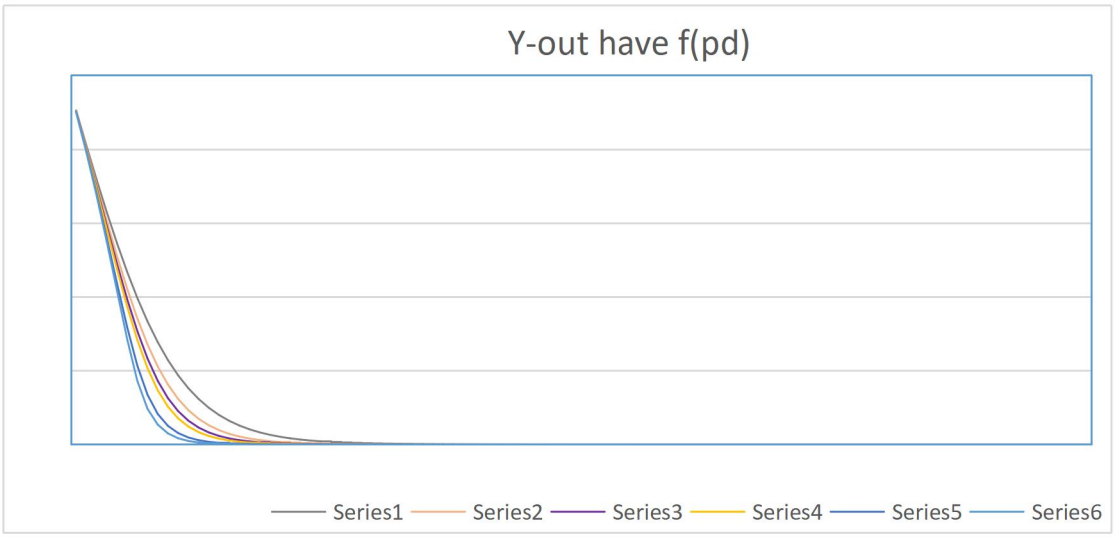
这样就使内部实际价格偏离真实价格时会自动降低流动性的集中度，然后我们即可解出后续待定参量。

上述说明可以看出此过程确实可以有效在一定流动性环境下进行兑换操作，但我们仍要保证最后一个需求，就是在实际价值确定时，随着交易的产生，会不会自动把我们的资金池耗尽？只有不耗尽我们的资金库的算法，才能用于实际交易过程。

为此，我们进行如下数值模拟测试：

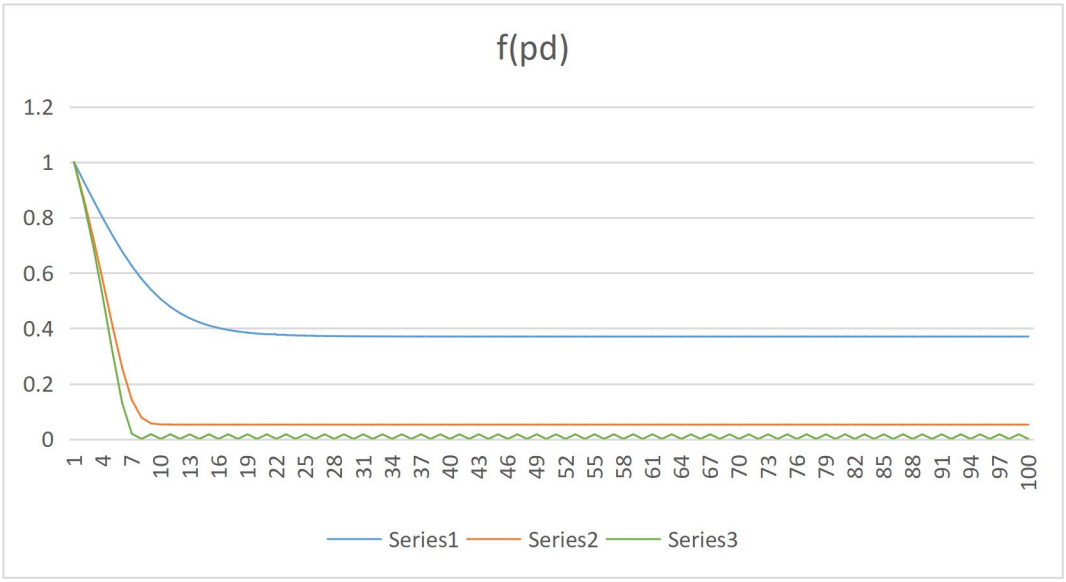
假设首次交易时，两种资产的数量一致，我们根据边界性限制，每次最多兑换出存储池10%资产；同时我们不断抛售其中一种资产，测试在边界条件下，兑换过程会不会耗尽另一种资产，测试了不带 f(pd)和带 f(pd)两种情况，测试结果曲线如下：





可以看出，不带衰减函数的系统在极端条件会耗尽另一种币种的储备，而带 f(pd)的系统则能在很广的初始增益范围内保持稳定。

同时我们在 a0=1、10、100 情况下 f(pd)的衰减值如下：



可以看到 f(pd)确实起到了很好的抑制效果，并且在 100 倍增益情况下仍然有效。

资金存储算法：

本文的 dex 所有 tokens 都存储在一个 vault 合约里，这样会导致不同 lp 里同样的币种只能通过记账方式进行处理。但如果使用实际出入库真实数额的记账方式，无法处理各种 balance 会自动变化的币种，例如类似 steth 的不断增长或 AMPL 增减不可控的币种，我们必须找到一种应对这些币种的处理方式。

为此，本文使用了一种在借贷项目中常见的以可变上限的测度计数方式，把绝对数值记录改成 vault 池相对量计数，完美解决了可变数量币种问题。

这里，我们需假设所有币种的增加和减少都是同比例缩放。假设 vault 中某一币种的总量为 a，此时假设其测度上限为 b，单位量为：a/b。此时此币种获得一个增加量 c，我们把他转换为

标准量 d=c/(a/b)，此时 vault 中此币种的总量为 a+c，测度上限为 b +c/(a/b)=b+bc/a=b(1+c/a)=b/a(a+c)=(a+c)/(a/b)，

这样换算后，新增或减少币种存储只要改变其测度上限和某种 lp 中的相对比例即可，不用改变其他 lp 中的记账数量。

结论：

本文从目前的普遍应用基础出发设计了一种基于边界自适应的自动做市商模型，使 lp 提供者在继续使用 Uniswap V2 形式 lp 的基础上，获得与 Uniswap V3、Curve V2 相当的流动性增益，并保持了系统的简洁性与鲁棒性。在此基础上对资金池的计算进行了改进，使之可用于各种数量会发生变化、但比例不会变化的币种，使统一型资金池的适应性得到了加强。

同时本文赞同如下观点：“如果一个系统只依赖自己，那么它的安全边界就是自己，是可以计算的；如果一个系统依赖了外部因子，它的安全边界理论上是不可估算的，如同一个拜占庭分布式系统一样，没有任何经验观察甚至形式化数学可以估算覆盖到所有潜在 fault（故障）路径。”，因此没有使用外部预言机干预价格形成过程。

免责声明：

本文仅供参考，它不构成投资建议或购买或出售任何投资的建议或邀请，也不应用于评估做出任何投资决定的优点。不应将其作为会计、法律或税务建议或投资建议的依据。本文反映了作者的当前意见，并非代表 X-UNION、CFXs 或其附属公司发表，也不一定反映 X-UNION 与其相关的个人的意见。

本文的设计在实际产品中可能会发生变化，最终设计方案以代码为主。

【0】Formal Specification of Constant Product (x × y = k) Market Maker Model and Implementation

【1】StableSwap - efficient mechanism for Stablecoin liquidity

【2】Uniswap v3 Core March 2021

【3】Automatic market-making with dynamic peg Michael Egorov, Curve Finance (Swiss Stake GmbH) June 9, 2021

【4】A non-custodial portfolio manager, liquidity provider, and price sensor. Fernando Martinelli Nikolai Mushegian v2019-09-19

【5】https://mooniswap.exchange/docs/MooniswapWhitePaper-v1.0.pdf

【6】https://mp.weixin.qq.com/s/2JGl1XMs800hyd5wBBFixA