Smooth Swap Protocol - An Efficient Protocol for Swapping Tokens with Same-Backed Asset

Qi Zhou

August 8, 2020

1 Problem Statement

Consider a liquidity pool maintains a basket of tokens that are backed by the same assets (such as USDT, USDC, TUSD, etc). For each token, the pool has x_i tokens with

$$\sum_i^n x_i = m, \tag{1}$$

where m is the total number of tokens and n is the number of different types of the tokens of the basket.

If a user wants to swap dx_i amount of token i to another token j for amount dx_j, a user can resort to Uniswap with the following invariant

$$x_i x_j = k_{i,j}. \tag{2}$$

However, one issue of Uniswap is that the pricing slippage can be considerable high even we know that both tokens are backed by the same asset. Several ways are proposed to improve the slippage issue including StableSwap (accessible via curve.fi) and mStable.

In StableSwap, the invariant becomes

$$An^n \sum_i^n x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod_i^n x_i}, \tag{3}$$

where A is a called "amplification coefficient" constant and D is a variable to maintain the equality of the equation.

In mStable, the invariant becomes the following equations with additional constrains:

$$\sum_i^n x_i = m, \tag{4}$$

$$\frac{x_i}{m} \leq W_i, \tag{5}$$

where W_i is the weight of the token i so that the percentage of the token in the basket should never exceed the weight.

If a swap satisfies the weight constraints, then a user can swap any token with 1:1 ratio in mStable, which StableSwap cannot guarantee. However, if any constraint is broken, such swap is prohibited in mStable, while StableSwap can still swap at the price of higher pricing slippage. In fact, at the time of writing the article, USDC token in mStable almost reaches the weight constraints (54.83% out of 55%), which means that a user can hardly swap USDC for other tokens in a large quantity even the user would like to pay the pricing slippage.

2 Proposed Smooth Swap Protocol

The smooth swap protocol (SSP) aims to harvest the benefits of StableSwap and mStable - it could guarantee 1:1 ratio swap as long as the swap satisfies the weight constraints. Further, even the weight constraints are broken, the protocol still allows the users to swap the tokens at higher price.

To achieve that, SSP introduces additional weight-related constants, variables, and functions.

- Hard-limit weight constant W_i. If a swap results in a broken hard-limit weight, such swap will fail immediately. Note that the hard-limit weight can be 0 if a token is disabled or 100%.
- Soft-limit weight constant V_i and soft-limit weight variable w_i. The soft-limit weight variable w_i is initialized as V_i. If a swap breaks a soft-limit weight constraint, i.e.,
$$\frac{x_i}{m} > w_i, \tag{6}$$
a penalty of the swap will be imposed. After every swap, the soft-limit weight variable will be adjusted to
$$w_i = \min\left(\frac{x_i}{m}, V_i\right). \tag{7}$$
- Penalty function $p(x_1, ..., x_n, dx_1, ..., dx_n, w_1, ..., w_n, V_1, ..., V_n, W_1, ..., W_n)$. The penalty function determines how much penalty if a soft-limit weight variable is broken.

3 Smooth Swap Protocol Token

Smooth swap protocol (SSP) token is a governance token that allows holders to vote the following actions:

- Add a new token to the basket;
- Determine the values of soft-limit weight and hard-limit weight constants;
- Determine the penalty function if a soft-limit weight constraint is broken;
- Determine the swap fee.

4 Smooth Swap Token

Smooth swap (SS) token represents the ownership of the pegged tokens. The liquidity pool supports the following operations with the SS token:

- Mint: A user can mint an SS token by depositing any token in the basket. The user will get 1:1 SS token as long as the mint does not break the weights or less SS token if a weight is broken but hard-limit weight is not reached.
- Redeem: By returning an SS token to the pool, the user can obtain 1:1 of any token in the basket in the pool as long as the current weights are not broken. If a weight is broken in redeem, less token will be return to the user.
- Swap: Simply combining Mint and Redeem operations by depositing a token and retrieving different tokens.

Since Mint returns 1:1 or less SS token and Redeem returns 1:1 or less backed tokens in the baskets, we could ensure that

$$TotalSupplyOfSSToken \geq m. \tag{8}$$

5 Comparisons with StableSwap and mStable

Smooth swap protocol subsumes StableSwap and mStable as special cases. If $W_i = 100\%$, $w_i = V_i = 0$ (Note that w_i is also constant here), and the penalty function reflects the invariant in Eq. (3), then the protocol becomes StableSwap. If the hard-limit weight constants equal to the soft-limit weight constants, i.e., $W_i = V_i$, then the protocol reduces to mStable.