# Wombat Side Pool and Dynamic Pool

Wombat Team

Wombat Exchange

**Abstract.** In this paper, we describe how Wombat caters experimental stablecoins and liquid staking tokens in our newly designed side pools and dynamic pools. Our design allows us to maintain open pool liquidity and efficiency while minimizing risks for liquidity providers.

## 1 Introduction

Our Wombat Pool v1 had been successfully audited and released to BNB mainnet to cater for our main pool stablecoins, i.e., BUSD, USDT, USDC, and DAI. The protocol robustness is based on the stability of maintaining our global coverage ratio equilibrium, i.e., $r^* = 1$, and the following assumptions:

- Wombat's stableswap invariant design does not require asset price input, i.e., oracles;
- Assumption of pegged assets priced at 1;
- Assumption of pegged assets reverting to their pegged prices, over time.

In order to cater to more experimental stablecoins and liquid staking tokens, we have made some innovations on top of our existing pool mechanism and designed the sidepool and dynamic pool to satisfy our needs. Our goal is to give the best protection to all assets in the pool without sacrificing low slippage nor open pool liquidity.

## 2 Side Pool (HighCovRatioPool.sol)

Experimental or newer stablecoins are riskier in nature and may demand a higher flexibility in maintaining their price peg at 1. Instead of continuously monitoring an asset's health and pausing the asset pool during highly-fluctuating markets, e.g., soft depeg, we note that the coverage ratio of depegging stablecoins is invariably high since traders will swap this stablecoin for other assets in the pool. To prevent other assets in the protocol from being drained, we introduce an additional *high coverage ratio fee* that will be applied on top of a normal haircut of a swap. Note that the high coverage ratio fee is retained by Wombat and will not be included as part of the total assets for accounting purpose to maintain $r^* = 1$.

Recall from the original Wombat Whitepaper [1] that if a trader wants to swap $\Delta_i > 0$ token $i$ to token $j$, then

$$\Delta_j = \frac{L_j\left(r_j - \frac{A}{r_j}\right) - \Delta_i\left(1 + \frac{A}{r_i\left(r_i + \frac{\Delta_i}{L_i}\right)}\right) + \sqrt{\left(L_j\left(r_j - \frac{A}{r_j}\right) - \Delta_i\left(1 + \frac{A}{r_i\left(r_i + \frac{\Delta_i}{L_i}\right)}\right)\right)^2 + 4AL_j^2}}{2} - L_j r_j,$$

where $L_i$, $L_j$, $r_i$, $r_j$, and $A$ are the liability of token $i$, the liability of token $j$, the coverage ratio of token $i$, the coverage ratio of token $j$, and the amplification factor, respectively. Since $\Delta_j$ depends on $L_i$, $L_j$, $r_i$, $r_j$,

$A$, and $\Delta_i$, we define $\Delta_j = \Delta(L_i, L_j, r_i, r_j, A, \Delta_i)$. Note that $\Delta_j < 0$ since it is from the perspective of the protocol. According to the original Wombat Whitepaper, the trader will receive $(1-h)|\Delta_j|$ token $j$, where $h$ is the haircut fee percentage.

In the side pool that contains experimental or newer stablecoins, the amplification factor $A$ will be larger than that of the main pool. This creates a higher slippage to swap from token $i$ to token $j$ if $r_i > 1$, which discourages further swaps from token $i$ to other tokens and motivates traders swapping from other tokens to token $i$ by providing higher arbitrage opportunities. Furthermore, let $1 < c_1 < c_2$ denote the lower and upper limits between which the high coverage ratio fee is assessed. For the sake of our discussion, we may consider $c_1 = 1.5$ and $c_2 = 1.8$. After the swap, let $r_i' = r_i + \frac{\Delta_i}{L_i}$ be the resultant coverage ratio of token $i$.

For any given $L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i$, and $\Delta_j = \Delta(L_i, L_j, r_i, r_j, A, \Delta_i)$, let $S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i)$ denote the amount of token $j$ that the trader receives when swapping token $i$ to token $j$ in the side pool and be defined as follows.

- If $r_i' \leq c_1$, then $S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i) = (1-h)|\Delta_j|$, i.e., there is no additional fee imposed on this swap.
- If $c_1 \leq r_i$, then
$$S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i) = (1-h)|\Delta_j| \cdot \max\left(\frac{c_2 - \frac{r_i + r_i'}{2}}{c_2 - c_1}, 0\right).$$
The high coverage ratio fee grows linearly with the average of $r_i$ and $r_i'$; when this average is $c_2$ or higher, the high coverage ratio fee is 100% of the swap amount, meaning that the trader will receive 0 token $j$. This practice ensures that no trader will have the incentive to continue swapping from token $i$ to token $j$ when the coverage ratio of token $i$ is too high.
- If $r_i < c_1 < r_i'$, then let $\widetilde{\Delta_i} = L_i(c_1 - r_i)$ be the portion of the swap that pushes the coverage ratio from $r_i$ to $c_1$, and $\widetilde{\widetilde{\Delta_i}} = \Delta_i - \widetilde{\Delta_i}$ be the portion of the swap that pushes the coverage ratio from $c_1$ to $r_i'$. Correspondingly, let
$$\begin{aligned}\widetilde{\Delta_j} &= \Delta(L_i, L_j, r_i, r_j, A, \widetilde{\Delta_i}) \\ &= \frac{L_j\left(r_j - \frac{A}{r_j}\right) - \widetilde{\Delta_i}\left(1 + \frac{A}{r_i c_1}\right) + \sqrt{\left(L_j\left(r_j - \frac{A}{r_j}\right) - \widetilde{\Delta_i}\left(1 + \frac{A}{r_i c_1}\right)\right)^2 + 4AL_j^2}}{2} - L_j r_j,\end{aligned}$$
$\widetilde{\widetilde{\Delta_j}} = \Delta_j - \widetilde{\Delta_j}$, and $\widetilde{r_j} = r_j + \frac{\widetilde{\Delta_j}}{L_j}$. Then
$$\begin{aligned}&S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i) \\ &= S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \widetilde{\Delta_i}\right) + S\left(L_i, L_j, c_1, \widetilde{r_j}, A, h, c_1, c_2, \widetilde{\widetilde{\Delta_i}}\right) \\ &= (1-h)\left|\widetilde{\Delta_j}\right| + (1-h)\left|\widetilde{\widetilde{\Delta_j}}\right| \cdot \max\left(\frac{c_2 - \frac{c_1 + r_i'}{2}}{c_2 - c_1}, 0\right).\end{aligned}$$
This formula allows us to assess the high coverage ratio fee only on the portion of the swap that pushes the coverage ratio from $c_1$ to $r_i'$.

The following theorem shows that the high coverage ratio fee is not path independent.

**Theorem 1.** *Let* $0 < \overline{\Delta_i} < \Delta_i$, $\overline{\overline{\Delta_i}} = \Delta_i - \overline{\Delta_i}$, $\overline{\Delta_j} = \Delta(L_i, L_j, r_i, r_j, A, \overline{\Delta_i})$, *and* $\overline{\overline{\Delta_j}} = \Delta_j - \overline{\Delta_j}$. *Let* $\overline{r_i} = r_i + \frac{\overline{\Delta_i}}{L_i}$ *and* $\overline{r_j} = r_j + \frac{\overline{\Delta_j}}{L_j}$. *If* $\frac{\max(r_i, c_1) + r_i'}{2} \leq c_2$, *then*
$$S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\Delta_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\Delta_i}}\right) \geq S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i).$$

*Proof.* Due to path independence of the algorithm and an increase of slippage when the coverage ratio deviate further from 1, as proved in the original Wombat Whitepaper, we have $\overline{\overline{\mathit{\Delta}_j}} = \mathit{\Delta}\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, \overline{\overline{\mathit{\Delta}_i}}\right)$ and $\frac{\overline{\mathit{\Delta}_i}}{\overline{\overline{\mathit{\Delta}_i}}} < \frac{\left|\overline{\mathit{\Delta}_j}\right|}{\left|\overline{\overline{\mathit{\Delta}_j}}\right|}$. If $r_i' \leq c_1$, then

$$
\begin{aligned}
&S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\mathit{\Delta}_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\mathit{\Delta}_i}}\right) \\
&= (1-h)\left|\overline{\mathit{\Delta}_j}\right| + (1-h)\left|\overline{\overline{\mathit{\Delta}_j}}\right| \\
&= (1-h)|\mathit{\Delta}_j| \\
&= S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \mathit{\Delta}_i).
\end{aligned}
$$

If $c_1 \leq r_i$, then

$$
\begin{aligned}
&S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\mathit{\Delta}_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\mathit{\Delta}_i}}\right) - S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \mathit{\Delta}_i) \\
&= (1-h)\left|\overline{\mathit{\Delta}_j}\right| \cdot \frac{c_2 - \frac{r_i + \overline{r_i}}{2}}{c_2 - c_1} + (1-h)\left|\overline{\overline{\mathit{\Delta}_j}}\right| \cdot \frac{c_2 - \frac{\overline{r_i} + r_i'}{2}}{c_2 - c_1} - (1-h)|\mathit{\Delta}_j| \cdot \frac{c_2 - \frac{r_i + r_i'}{2}}{c_2 - c_1} \\
&= (1-h)\left|\overline{\mathit{\Delta}_j}\right| \cdot \left(\frac{c_2 - \frac{r_i + \overline{r_i}}{2}}{c_2 - c_1} - \frac{c_2 - \frac{r_i + r_i'}{2}}{c_2 - c_1}\right) + (1-h)\left|\overline{\overline{\mathit{\Delta}_j}}\right| \cdot \left(\frac{c_2 - \frac{\overline{r_i} + r_i'}{2}}{c_2 - c_1} - \frac{c_2 - \frac{r_i + r_i'}{2}}{c_2 - c_1}\right) \\
&= \frac{1-h}{2(c_2 - c_1)}\left(\left|\overline{\mathit{\Delta}_j}\right| \cdot (r_i' - \overline{r_i}) + \left|\overline{\overline{\mathit{\Delta}_j}}\right| \cdot (r_i - \overline{r_i})\right) \\
&= \frac{1-h}{2(c_2 - c_1)}\left(\left|\overline{\mathit{\Delta}_j}\right| \cdot \left(r_i + \frac{\mathit{\Delta}_i}{L_i} - \left(r_i + \frac{\overline{\mathit{\Delta}_i}}{L_i}\right)\right) + \left|\overline{\overline{\mathit{\Delta}_j}}\right| \cdot \left(r_i - \left(r_i + \frac{\overline{\mathit{\Delta}_i}}{L_i}\right)\right)\right) \\
&= \frac{1-h}{2(c_2 - c_1)L_i}\left(\left|\overline{\mathit{\Delta}_j}\right| \cdot \overline{\overline{\mathit{\Delta}_i}} + \left|\overline{\overline{\mathit{\Delta}_j}}\right| \cdot \left(-\overline{\mathit{\Delta}_i}\right)\right) > 0
\end{aligned}
\tag{1}
$$

since $\frac{\overline{\mathit{\Delta}_i}}{\overline{\overline{\mathit{\Delta}_i}}} < \frac{\left|\overline{\mathit{\Delta}_j}\right|}{\left|\overline{\overline{\mathit{\Delta}_j}}\right|}$. Lastly, it remains to consider $r_i < c_1 < r_i'$. If $\overline{\mathit{\Delta}_i} \leq c_i$, then

$$
\begin{aligned}
&S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\mathit{\Delta}_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\mathit{\Delta}_i}}\right) \\
&= S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\mathit{\Delta}_i}\right) \\
&\qquad + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \widetilde{\mathit{\Delta}_i} - \overline{\mathit{\Delta}_i}\right) + S\left(L_i, L_j, c_1, \widetilde{r_j}, A, h, c_1, c_2, \widetilde{\widetilde{\mathit{\Delta}_i}}\right) \\
&= (1-h)\left|\overline{\mathit{\Delta}_j}\right| + (1-h)\left|\widetilde{\mathit{\Delta}_j} - \overline{\mathit{\Delta}_j}\right| + (1-h)\left|\widetilde{\widetilde{\mathit{\Delta}_j}}\right| \cdot \frac{c_2 - \frac{c_1 + r_i'}{2}}{c_2 - c_1} \\
&= (1-h)\left|\widetilde{\mathit{\Delta}_j}\right| + (1-h)\left|\widetilde{\widetilde{\mathit{\Delta}_j}}\right| \cdot \frac{c_2 - \frac{c_1 + r_i'}{2}}{c_2 - c_1} \\
&= S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \mathit{\Delta}_i).
\end{aligned}
$$

If $c_i < \overline{\Delta_i}$, then

$$
\begin{aligned}
&S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \overline{\Delta_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\Delta_i}}\right) - S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i) \\
&= S\left(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \widetilde{\Delta_i}\right) + S\left(L_i, L_j, c_1, \widetilde{r_j}, A, h, c_1, c_2, \overline{\Delta_i} - \widetilde{\Delta_i}\right) \\
&\qquad + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\Delta_i}}\right) - S(L_i, L_j, r_i, r_j, A, h, c_1, c_2, \Delta_i) \\
&= (1-h)\left|\widetilde{\Delta_j}\right| + (1-h)\left|\overline{\Delta_j} - \widetilde{\Delta_j}\right| \cdot \frac{c_2 - \frac{c_1 + \overline{r_i}}{2}}{c_2 - c_1} + (1-h)\left|\overline{\overline{\Delta_j}}\right| \cdot \frac{c_2 - \frac{\overline{r_i} + r_i'}{2}}{c_2 - c_1} \\
&\qquad - \left((1-h)\left|\widetilde{\Delta_j}\right| + (1-h)\left|\widetilde{\widetilde{\Delta_j}}\right| \cdot \frac{c_2 - \frac{c_1 + r_i'}{2}}{c_2 - c_1}\right) \\
&= S\left(L_i, L_j, c_1, \widetilde{r_j}, A, h, c_1, c_2, \overline{\Delta_i} - \widetilde{\Delta_i}\right) + S\left(L_i, L_j, \overline{r_i}, \overline{r_j}, A, h, c_1, c_2, \overline{\overline{\Delta_i}}\right) - S\left(L_i, L_j, c_1, \widetilde{r_j}, A, h, c_1, c_2, \widetilde{\widetilde{\Delta_i}}\right) \\
&> 0 \qquad \text{(by equation (1))}.
\end{aligned}
$$

□

From Theorem 1, we see that when the coverage ratio is higher than $c_1$, it is beneficial for traders to split a swap into successive smaller swaps. This shows that the high coverage ratio fee does not satisfy path independence. However, the gain received by the traders when splitting a swap is insignificant, since the difference between $\frac{\overline{\overline{\Delta_i}}}{\overline{\Delta_i}}$ and $\frac{\left|\overline{\Delta_j}\right|}{\left|\overline{\overline{\Delta_j}}\right|}$ is very small. Besides, the amplification factor $A$ of the side pool is higher than that of the main pool, motivating traders to make use of the enhanced arbitrage opportunities and maintain the coverage ratios closer to 1. Hence, we expect that the coverage ratio to be lower than $c_1$ except under some extreme conditions, e.g., depeg or soft depeg. In other words, the high coverage ratio fee will only kick in to protect the liquidity in the protocol against highly-fluctuating markets, and under the normal market condition, the algorithm still observes path independence.

*Note:*

1. The high coverage ratio fee only applies to swaps. Deposits and withdrawals are not affected even when the coverage ratios are higher than $c_1$, except that there is a liquidity cap for every asset in the side pool.
2. Every side pool has BUSD as one of the available tokens, which serves as a bridging asset between the main pool and the side pool.
3. In the Wombat user interface, when traders try to swap token $i$ to token $j$, there is a "reverse quote function" that allows traders to specify $|\Delta_j|$, i.e., the amount of token $j$ that they want to receive, and the interface will provide a quote for the corresponding $\Delta_i$. This algorithm was described in Section 6 of the original Wombat Whitepaper. When the coverage ratio $r_i$ is higher than $c_1$, we shall perform a binary search to find the upper bound of the reverse quote amount. This is a functionality that we wish to support despite the low expected usage by our users, under extreme market conditions.

## 3 Liquid Staking Pool (DynamicPool.sol)

Liquid staking tokens such as "stkBNB" or "BNBx" are reward bearing tokens that holders can redeem with the liquid staking providers for their underlying locked tokens that comes with an expected yield, e.g., 1 stkBNB token can redeem for 1.06 BNB by end of year. The locking and minting of liquid staking tokens is usually instant, where the unlocking and redemption period may take 1–3 weeks depending on the provider.

These tokens are in the form of an exchange-rate based token which the exchange rate for redeeming the underlying will grow over time. Thus, external oracles, which we get from their liquid staking manager contracts respectively, are required for an accurate asset-to-asset swap.

### 3.1 Swap

Let $\mathcal{T}$ represents the set of tokens in the liquid staking pool, and for each token $k$ in $\mathcal{T}$, let $p_k$ be the oracle price of the token. Since the values of the tokens in this pool are no longer pegged to 1, the original Constant Function Market Maker (CFMM) invariant curve

$$\sum_{k\in\mathcal{T}} L_k\left(r_k-\frac{A}{r_k}\right)=D$$

needs to be modified. Naturally, we replace $L_k$ with $L_k p_k$, which represents the actual value of the liability of token $k$. Hence, the new CFMM invariant curve for the liquid staking pool is

$$\sum_{k\in\mathcal{T}} L_k p_k\left(r_k-\frac{A}{r_k}\right)=D. \tag{2}$$

To swap $\Delta_i$ token $i$ to token $j$, let $r'_j$ denote the coverage ratio of token $j$ after the swap. Then

$$\begin{aligned}
L_ip_i\left(r_i+\frac{\Delta_i}{L_i}-\frac{A}{r_i+\frac{\Delta_i}{L_i}}\right)+L_jp_j\left(r'_j-\frac{A}{r'_j}\right)&=L_ip_i\left(r_i-\frac{A}{r_i}\right)+L_jp_j\left(r_j-\frac{A}{r_j}\right)\\
L_ip_i\left(\frac{\Delta_i}{L_i}+\frac{A}{r_i}-\frac{A}{r_i+\frac{\Delta_i}{L_i}}\right)-L_jp_j\left(r_j-\frac{A}{r_j}\right)+L_jp_j\left(r'_j-\frac{A}{r'_j}\right)&=0\\
p_i\Delta_i+\frac{L_ip_iA\left(r_i+\frac{\Delta_i}{L_i}-r_i\right)}{r_i\left(r_i+\frac{\Delta_i}{L_i}\right)}-L_jp_j\left(r_j-\frac{A}{r_j}\right)+L_jp_j\left(r'_j-\frac{A}{r'_j}\right)&=0\\
\frac{p_i}{p_j}\Delta_i\left(1+\frac{A}{r_i\left(r_i+\frac{\Delta_i}{L_i}\right)}\right)-L_j\left(r_j-\frac{A}{r_j}\right)+L_j\left(r'_j-\frac{A}{r'_j}\right)&=0.
\end{aligned}$$

By multiplying $r'_j$ to both sides of the equation, we can solve for $r'_j$ with the quadratic formula. Since $\Delta_j=L_jr'_j-L_jr_j$, we have

$$\Delta_j=\frac{L_j\left(r_j-\frac{A}{r_j}\right)-\frac{p_i}{p_j}\Delta_i\left(1+\frac{A}{r_i\left(r_i+\frac{\Delta_i}{L_i}\right)}\right)+\sqrt{\left(L_j\left(r_j-\frac{A}{r_j}\right)-\frac{p_i}{p_j}\Delta_i\left(1+\frac{A}{r_i\left(r_i+\frac{\Delta_i}{L_i}\right)}\right)\right)^2+4AL_j^2}}{2}-L_jr_j.$$

### 3.2 Withdrawal or Deposit

Similar to Section 4 of the original Wombat Whitepaper, let $r^*$ denote the global equilibrium coverage ratio so that

$$\sum_{k\in\mathcal{T}} L_k p_k\left(r^*-\frac{A}{r^*}\right)=D. \tag{3}$$

By multiplying $r^*$ to both sides of the equation and applying the quadratic formula, we obtain

$$r^* = \frac{D + \sqrt{D^2 + 4A\sum_{k\in\mathcal{T}} L_k p_k}}{2\sum_{k\in\mathcal{T}} L_k p_k}.$$

Let $\Delta_i^A$ and $\Delta_i^L$ denote the changes in the asset and the liability of token $i$, respectively. In a withdrawal, $\Delta_i^L < 0$ is specified by the trader while $\Delta_i^A < 0$ is solved as a dependent variable; conversely, in a deposit, $\Delta_i^A > 0$ is specified by the trader while $\Delta_i^L > 0$ is solved as a dependent variable. The new global equilibrium coverage ratio after the withdrawal or deposit is

$$r^{*\prime} = \frac{\Delta_i^L p_i + \left(\sum_{k\in\mathcal{T}} L_k p_k\right) r^*}{\Delta_i^L p_i + \sum_{k\in\mathcal{T}} L_k p_k},$$

and the corresponding new constant $D'$ for our CFMM is

$$\left(\Delta_i^L p_i + \sum_{k\in\mathcal{T}} L_k p_k\right)\left(r^{*\prime} - \frac{A}{r^{*\prime}}\right) = D'.$$

With the new constant $D'$, we can backward deduce the coverage ratio $r_i'$ needed to maintain the equilibrium of the system:

$$(L_i p_i + \Delta_i^L p_i)\left(r_i' - \frac{A}{r_i'}\right) + \sum_{k\in\mathcal{T}\setminus\{i\}} L_k p_k \left(r_k - \frac{A}{r_k}\right) = D'$$

$$(L_i p_i + \Delta_i^L p_i)(r_i')^2 + \left(D - L_i p_i\left(r_i - \frac{A}{r_i}\right) - D'\right) r_i' - A(L_i p_i + \Delta_i^L p_i) = 0,$$

so

$$r_i' = \frac{D' - D + L_i p_i\left(r_i - \frac{A}{r_i}\right) + \sqrt{\left(D' - D + L_i p_i\left(r_i - \frac{A}{r_i}\right)\right)^2 + 4A(L_i p_i + \Delta_i^L p_i)}}{2(L_i p_i + \Delta_i^L p_i)}.$$

Finally, the corresponding change $\Delta_i^A$ in the asset of token $i$ is given by

$$\begin{aligned}\Delta_i^A &= (L_i + \Delta_i^L) r_i' - L_i r_i \\ &= \frac{D' - D + L_i p_i\left(r_i - \frac{A}{r_i}\right) + \sqrt{\left(D' - D + L_i p_i\left(r_i - \frac{A}{r_i}\right)\right)^2 + 4A(L_i p_i + \Delta_i^L p_i)^2}}{2p_i} - L_i r_i.\end{aligned}$$

If $r^* = 1$, then $r^{*\prime} = 1$, implying that $D = \sum_{k\in\mathcal{T}} L_k p_k (1 - A)$ and $D' = \left(\Delta_i^L p_i + \sum_{k\in\mathcal{T}} L_k p_k\right)(1 - A)$, thus

$$\Delta_i^A = \frac{\Delta_i^L(1-A) + L_i\left(r_i - \frac{A}{r_i}\right) + \sqrt{\left(\Delta_i^L(1-A) + L_i\left(r_i - \frac{A}{r_i}\right)\right)^2 + 4A(L_i + \Delta_i^L)^2}}{2} - L_i r_i.$$

which is identical to the formula for withdrawal given by the original Wombat Whitepaper.

### 3.3 Relationship between $r^*$ and token price

When the price of the tokens changes, $r^*$ will likely to vary and deviate from 1. The following theorem describes how $r^*$ changes when the price $p_i$ of token $i$ moves.

**Theorem 2.** *The partial derivative* $\frac{\partial r^*}{\partial p_i} \geq 0$ *if and only if* $r_i \geq r^*$.

*Proof.* First, note that the function $f(x) = x - \frac{A}{x}$ is strictly increasing over $(0, \infty)$. This can be seen by $f'(x) = 1 + \frac{A}{x^2} > 0$ for all $x > 0$. Next, if we take the partial derivative of $D$ in equation (2) with respect to $p_i$, we have $\frac{\partial D}{\partial p_i} = L_i \left( r_i - \frac{A}{r_i} \right)$. Finally, if we take the implicit partial derivative of $r^*$ in equation (3) with respect to $p_i$, we have

$$\begin{aligned} L_i \left( r^* - \frac{A}{r^*} \right) + \sum_{k \in \mathcal{T}} L_k p_k \left( 1 + \frac{A}{(r^*)^2} \right) \frac{\partial r^*}{\partial p_i} &= \frac{\partial D}{\partial p_i} \\ \sum_{k \in \mathcal{T}} L_k p_k \left( 1 + \frac{A}{(r^*)^2} \right) \frac{\partial r^*}{\partial p_i} &= L_i \left( \left( r_i - \frac{A}{r_i} \right) - \left( r^* - \frac{A}{r^*} \right) \right). \end{aligned}$$

Since $\sum_{k \in \mathcal{T}} L_k p_k \left( 1 + \frac{A}{(r^*)^2} \right) > 0$, we have $\frac{\partial r^*}{\partial p_i} \geq 0$ if and only if $r_i - \frac{A}{r_i} \geq r^* - \frac{A}{r^*}$, which occurs if and only if $r_i \geq r^*$. □

Liquid staking tokens such as BNBx or stkBNB should have higher coverage ratio than the base asset, i.e., BNB. This is because of the illiquid nature of liquid staking tokens compared to the base asset. For instance, traders will likely to swap BNBx or stkBNB to BNB on Wombat if the swap price to BNB on Wombat is comparable to the rate that one can redeem from the liquid staking providers a week later. Due to this observation, $r_i$ is likely to be greater than $r^*$. Furthermore, a slow yet continual growth of $p_i$ is expected. Slashing or penalty resulting in losses of the underlying BNB pool of the liquid staking provider is extremely rare and if happens, losses are expected to be compensated by the liquid staking provider to maintain the liquid staking token peg to the base asset BNB. Hence, by Theorem 2, when the price $p_i$ increases, $r^*$ should grow instead of dropping below 1. This is important for the overall safety of our liquid staking pool.

When $r^*$ grows higher than 1, it is easy for us to repeg it to 1 by reducing assets in the pool. In the rare occasion when $r^*$ goes below 1, we will fill the gap and push it back to 1 with the haircut fees that we accumulate over time. Since it is not expected to occur often, we should have sufficient fund to cover the difference.

*Note:* Rebasing tokens are not supported for the liquid staking pool. This also applies to all other pools on Wombat.

## References


1. Wombat Team. (2022). *Wombat — An Efficient Stableswap Algorithm.*