Balancer Safe LP-Price Derivation

andany

24/08/15

V is the invariant of the Balancer Pool (as defined by Balancer). r_i's are the token reserve amounts and r_i''s are the fair token reserve anounts. W_i's are the respective (normalized) token weights. s_i's are the spot prices (formula taken from balancer docs). π is the fair total pool value of the Balancer Pool.

$$\begin{aligned}
V &= {r_0}^{W_0} \cdot {r_1}^{W_1} \\
s_0 &= \frac{r_1/W_1}{r_0/W_0} \\
\implies \quad {s_0}^{W_0} &= \frac{{r_1}^{W_0}/{W_1}^{W_0}}{{r_0}^{W_0}/{W_0}^{W_0}} \\
&= \frac{{r_1}^{W_0} \cdot {r_1}^{W_1}/{W_1}^{W_0}}{{r_0}^{W_0} \cdot {r_1}^{W_1}/{W_0}^{W_0}} \\
&= \frac{{r_1}^{W_0+W_1}/{W_1}^{W_0}}{V/{W_0}^{W_0}} \\
&= \frac{r_1 \cdot {W_0}^{W_0}}{V \cdot {W_1}^{W_0}} \\
\implies r_1' &= \frac{{s_0}^{W_0} \cdot V \cdot {W_1}^{W_0}}{{W_0}^{W_0}} \\
&= \frac{{s_0}^{W_0} \cdot V \cdot {W_1}^{W_0} \cdot {W_1}^{W_1}}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \\
&= \frac{{s_0}^{W_0} \cdot V \cdot {W_1}^{W_0+W_1}}{{W_0}^{W_0} \cdot {W_1}^{W_1}}
\end{aligned}$$

$$\begin{aligned}
\implies r_1' &= \frac{{s_0}^{W_0} \cdot V \cdot W_1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \\
\text{analogously: } r_0' &= \frac{{s_1}^{W_1} \cdot V \cdot W_0}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \\
p_0 &= s_0 \cdot p_1 \\
\implies s_0 &= \frac{p_0}{p_1} \\
\text{analogously: } s_1 &= \frac{p_1}{p_0} \\
\pi(W_0, W_1) &= p_0 \cdot r_0' + p_1 \cdot r_1' \\
&= p_0 \cdot \frac{{s_1}^{W_1} \cdot V \cdot W_0}{{W_0}^{W_0} \cdot {W_1}^{W_1}} + p_1 \cdot \frac{{s_0}^{W_0} \cdot V \cdot W_1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \\
&= p_0 \cdot \frac{{p_1}^{W_1} \cdot V \cdot W_0}{{p_0}^{W_1} \cdot {W_0}^{W_0} \cdot {W_1}^{W_1}} + p_1 \cdot \frac{{p_0}^{W_0} \cdot V \cdot W_1}{{p_1}^{W_0} \cdot {W_0}^{W_0} \cdot {W_1}^{W_1}} \\
&= \frac{{p_0}^{W_0} \cdot {p_1}^{W_1} \cdot V \cdot W_0 + {p_1}^{W_1} \cdot {p_0}^{W_0} \cdot V \cdot W_1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \\
&= \frac{W_0 + W_1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \cdot V \cdot {p_0}^{W_0} \cdot {p_1}^{W_1} \\
\implies \pi(W_0, W_1) &= \frac{1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \cdot V \cdot {p_0}^{W_0} \cdot {p_1}^{W_1}
\end{aligned}$$

The fair price of the LP-token is obtained through dividing the fair pool value (π) by the LP-token supply (Γ): $\pi(W_0, W_1) \cdot \Gamma^{-1}$

We can see that the formula for π reduces to the known fair total pool value for $W_0 = W_1 = 1/2$:

$$\begin{aligned}
\pi(1/2, 1/2) &= \frac{1}{1/2^{1/2} \cdot 1/2^{1/2}} \cdot V \cdot {p_0}^{1/2} \cdot {p_1}^{1/2} \\
&= \frac{1}{1/2^{1/2+1/2}} \cdot V \cdot \sqrt{p_0 \cdot p_1} \\
&= \frac{1}{1/2} \cdot V \cdot \sqrt{p_0 \cdot p_1} \\
&= 2 \cdot V \cdot \sqrt{p_0 \cdot p_1}
\end{aligned}$$

Consider the 20WBTC-80BADGER Pool as an example for non-equal weights.

$$\begin{aligned}
\text{Pool Value } (PV)\text{:}\ & 7,053,126 \\
\text{BADGER Value } (r_0 \cdot p_0)\text{:}\ & 5,630,522 \\
\text{WBTC Value } (r_1 \cdot p_1)\text{:}\ & 1,422,603
\end{aligned}$$

$$\begin{aligned}
\pi(4/5, 1/5) - PV &= \frac{1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \cdot V \cdot {p_0}^{W_0} \cdot {p_1}^{W_1} - PV \\
&= \frac{1}{{W_0}^{W_0} \cdot {W_1}^{W_1}} \cdot (r_0 \cdot p_0)^{W_0} \cdot (r_1 \cdot p_1)^{W_1} - PV \\
&= \frac{1}{(4/5)^{4/5} \cdot (1/5)^{1/5}} \cdot (r_0 \cdot p_0)^{4/5} \cdot (r_1 \cdot p_1)^{1/5} - PV \\
&= \frac{1}{(4^4/5^5)^{1/5}} \cdot (r_0 \cdot p_0)^{4/5} \cdot (r_1 \cdot p_1)^{1/5} - PV \\
&= \frac{5}{4^{4/5}} \cdot (r_0 \cdot p_0)^{4/5} \cdot (r_1 \cdot p_1)^{1/5} - PV \\
&= \frac{5}{4^{4/5}} \cdot (5,630,522)^{4/5} \cdot (1,422,603)^{1/5} - 7,053,126 \\
&\approx -64 \\
&= \sigma
\end{aligned}$$

σ is well within the margin of error for this calculation, as it's due to the effects of imprecise and lagged data. This is made especially clear when the result is divided by the LP token supply to arrive at the fair LP token price.

Since LP tokens are tokens themselves, we can recursively find the fair pool value of the n-token LP by finding the fair pool value of the two token LP: [$(n-1)$-TOKEN LP]/[NEW TOKEN].

Let π_i be the $(i+1)$-token LP.
Let W_t be the actual weight for token t in the n-token pool.
Let ω_t be the relative weight for token t in the $(i \leq n)$-token pool.
Let $\Omega_i = \sum_{t=0}^{i-1} \omega_t = 1 - \omega_i$ for all $i \leq n$.
Let $\omega^{\star}_{t,i} = \frac{\omega_t}{\Omega_i}$ be the relative weight of token t in the i-token pool.
Let $V = \prod_{t=0}^{n-1} {r_t}^{W_t}$ be the n-token LP pool invariant.
Let $V_i = \prod_{t=0}^{i-1} {r_t}^{\omega_t}$ be the $i \leq n$-token LP pool invariant.
Let $V_{i,i+1} = \prod_{t=0}^{i-1} {r_t}^{\omega_t}$ be the partial invariant for the $(i+1)$-token LP pool.
Notice that the LP token supply for the $(i \leq n)$-token pool is Γ^{Ω_i} where Γ is the LP-token supply for the n-token pool.
Notice also that the reserve amount for the $(i \leq n)$-token pool is Γ^{Ω_i}.
Hence the recursive formula for π_i is:

$$\begin{aligned}
\pi_i &= \frac{1}{{\Omega_i}^{\Omega_i} \cdot {\omega_i}^{\omega_i}} \cdot \Gamma^{\Omega_i} \cdot {r_i}^{\omega_i} \cdot \frac{\pi_{i-1}^{\Omega_i}}{\Gamma^{\Omega_i}} \cdot {p_i}^{\omega_i} \\
&= \frac{1}{{\Omega_i}^{\Omega_i} \cdot {\omega_i}^{\omega_i}} \cdot {r_i}^{\omega_i} \cdot \pi_{i-1}^{\Omega_i} \cdot {p_i}^{\omega_i}
\end{aligned}$$

Following is the derivation of π_2.

$$\begin{aligned}
\text{Given: } \pi_1 &= \frac{1}{{\omega_0}^{\omega_0} \cdot {\omega_1}^{\omega_1}} \cdot V_2 \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \\
\text{And given: } \pi_i &= \frac{1}{{\Omega_i}^{\Omega_i} \cdot {\omega_i}^{\omega_i}} \cdot {r_i}^{\omega_i} \cdot \pi_{i-1}^{\Omega_i} \cdot {p_i}^{\omega_i} \\
\text{Then: } \pi_2 &= \frac{1}{{\Omega_2}^{\Omega_2} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \cdot \pi_1^{\Omega_2} \cdot {p_2}^{\omega_2} \\
&= \frac{1}{{\Omega_2}^{\Omega_2} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \\
&\cdot \left(\frac{1}{(\omega_0/\Omega_2)^{(\omega_0/\Omega_2)} \cdot (\omega_1/\Omega_2)^{(\omega_1/\Omega_2)}} \cdot V_2 \cdot {p_0}^{(\omega_0/\Omega_2)} \cdot {p_1}^{(\omega_1/\Omega_2)} \right)^{\Omega_2} \cdot {p_2}^{\omega_2}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{{\Omega_2}^{\Omega_2} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \cdot \left(\frac{1}{(\omega_0/\Omega_2)^{\omega_0} \cdot (\omega_1/\Omega_2)^{\omega_1}} \cdot V_{2,3} \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \right) \cdot {p_2}^{\omega_2} \\
&= \frac{1}{(1-\omega_2)^{(1-\omega_2)} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \\
&\cdot \left(\frac{1}{(\omega_0/(1-\omega_2))^{\omega_0} \cdot (\omega_1/(1-\omega_2))^{\omega_1}} \cdot V_{2,3} \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \right) \cdot {p_2}^{\omega_2} \\
&= \frac{1}{(1-\omega_2)^{(1-\omega_2)} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \cdot \frac{(1-\omega_2)^{\omega_0} \cdot (1-\omega_2)^{\omega_1}}{{\omega_0}^{\omega_0} \cdot {\omega_1}^{\omega_1}} \cdot V_{2,3} \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \cdot {p_2}^{\omega_2} \\
&= \frac{1}{(1-\omega_2)^{(1-\omega_2)} \cdot {\omega_2}^{\omega_2}} \cdot {r_2}^{\omega_2} \cdot \frac{(1-\omega_2)^{\omega_0+\omega_1}}{{\omega_0}^{\omega_0} \cdot {\omega_1}^{\omega_1}} \cdot V_{2,3} \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \cdot {p_2}^{\omega_2} \\
&= \frac{1}{(1-\omega_2)^{(1-\omega_2)} \cdot {\omega_2}^{\omega_2}} \cdot \frac{(1-\omega_2)^{(1-\omega_2)}}{{\omega_0}^{\omega_0} \cdot {\omega_1}^{\omega_1}} \cdot V_3 \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \cdot {p_2}^{\omega_2} \\
&= \frac{1}{{\omega_0}^{\omega_0} \cdot {\omega_1}^{\omega_1} \cdot {\omega_2}^{\omega_2}} \cdot V_3 \cdot {p_0}^{\omega_0} \cdot {p_1}^{\omega_1} \cdot {p_2}^{\omega_2}
\end{aligned}
$$

The following is a summary of the results thus far.

$$
\begin{aligned}
\pi_1 &= \frac{1}{\prod_{t=0}^{1} {\omega_t}^{\omega_t}} \cdot V_2 \cdot \prod_{t=0}^{1} {p_t}^{\omega_t} \\
\pi_2 &= \frac{1}{\prod_{t=0}^{2} {\omega_t}^{\omega_t}} \cdot V_3 \cdot \prod_{t=0}^{2} {p_t}^{\omega_t}
\end{aligned}
$$

Here, we can see an inductive pattern emerge. The base case for the inductive proof has already been shown.

Proof by induction for the general case:

$$\text{Claim: } \pi_i = \frac{1}{\prod_{t=0}^{i} {\omega_t}^{\omega} t} \cdot V_{i+1} \cdot \prod_{t=0}^{i} {p_t}^{\omega_t}$$

$$\text{Suppose: } \pi_k = \frac{1}{\prod_{t=0}^{k} {\omega_t}^{\omega} t} \cdot V_{k+1} \cdot \prod_{t=0}^{k} {p_t}^{\omega_t} \text{ for } i = k$$

$$\begin{aligned}
\text{Then: } \pi_{k+1} &= \frac{1}{{\Omega_{k+1}}^{\Omega_{k+1}} \cdot {\omega_{k+1}}^{\omega_{k+1}}} \cdot {r_{k+1}}^{\omega_{k+1}} \cdot \pi_k^{\Omega_{k+1}} \cdot {p_{k+1}}^{\omega_{k+1}} \\
&= \frac{1}{{\Omega_{k+1}}^{\Omega_{k+1}} \cdot {\omega_{k+1}}^{\omega_{k+1}}} \cdot {r_{k+1}}^{\omega_{k+1}} \\
&\cdot \left(\frac{1}{\prod_{t=0}^{k} \left(\omega_t/\Omega_{k+1}\right)^{(\omega_t/\Omega_{k+1})}} \cdot V_{k+1} \cdot \prod_{t=0}^{k} {p_t}^{(\omega_t/\Omega_{k+1})} \right)^{\Omega_{k+1}} \cdot {p_{k+1}}^{\omega_{k+1}} \\
&= \frac{1}{{\Omega_{k+1}}^{\Omega_{k+1}} \cdot {\omega_{k+1}}^{\omega_{k+1}}} \cdot {r_{k+1}}^{\omega_{k+1}} \cdot \frac{1}{\prod_{t=0}^{k} \left(\omega_t/\Omega_{k+1}\right)^{\omega_t}} \cdot V_{k+1,k+2} \cdot \prod_{t=0}^{k} {p_t}^{\omega_t} \cdot {p_{k+1}}^{\omega_{k+1}} \\
&= \frac{1}{{\Omega_{k+1}}^{\Omega_{k+1}} \cdot {\omega_{k+1}}^{\omega_{k+1}}} \cdot \frac{{\Omega_{k+1}}^{\sum_{t=0}^{k} \omega_t}}{\prod_{t=0}^{k} {\omega_t}^{\omega_t}} \cdot V_{k+2} \cdot \prod_{t=0}^{k+1} {p_t}^{\omega_t} \\
&= \frac{1}{{\Omega_{k+1}}^{\Omega_{k+1}}} \cdot \frac{{\Omega_{k+1}}^{\Omega_{k+1}}}{\prod_{t=0}^{k+1} {\omega_t}^{\omega_t}} \cdot V_{k+2} \cdot \prod_{t=0}^{k+1} {p_t}^{\omega_t} \\
&= \frac{1}{\prod_{t=0}^{k+1} {\omega_t}^{\omega_t}} \cdot V_{k+2} \cdot \prod_{t=0}^{k+1} {p_t}^{\omega_t}
\end{aligned}$$

Since $\frac{1}{\prod_{t=0}^{k} {\omega_t}^{\omega_t}} \cdot V_{k+1} \cdot \prod_{t=0}^{k} {p_t}^{\omega_t} \implies \frac{1}{\prod_{t=0}^{k+1} {\omega_t}^{\omega_t}} \cdot V_{k+2} \cdot \prod_{t=0}^{k+1} {p_t}^{\omega_t}$ for all k, and since the claim is true for π_1, it follows that $\pi_i = \frac{1}{\prod_{t=0}^{i} {\omega_t}^{\omega_t}} \cdot V_{i+1} \cdot \prod_{t=0}^{i} {p_t}^{\omega_t}$ for all i. Therefore, the fair LP-price for the n-token pool is:

$$\pi_{n-1} \cdot \Gamma^{-1} = \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot V \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$

♪

We can prove that this is indeed correct formula as follows:

1. Suppose (WLOG) someone trades token i for token o.

   From Balancer's Developer Docs, we have: $A_o = r_o \cdot \left(1 - \left(\frac{r_i}{r_i + A_i}\right)^{W_i/W_o}\right)$,
   where A_o and A_i is the amount of token o received and amounts of token i sent, respectively. $\pi^\star_{n-1}$ signifies the changed pool value as a result of the trade.

   Then $\pi^\star_{n-1} \cdot \Gamma^{-1} = \dfrac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot (r_o - A_o)^{W_o} \cdot (r_i + A_i)^{W_i} \cdot \prod_{t \neq i,o}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$

$$= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot \left(r_o - r_o \cdot \left(1 - \left(\frac{r_i}{r_i + A_i}\right)^{W_i/W_o}\right)\right)^{W_o} \cdot (r_i + A_i)^{W_i}$$
$$\cdot \prod_{t \neq i,o}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$
$$= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot {r_o}^{W_o} \cdot \left(1 - \left(1 - \left(\frac{r_i}{r_i + A_i}\right)^{W_i/W_o}\right)\right)^{W_o} \cdot (r_i + A_i)^{W_i}$$
$$\cdot \prod_{t \neq i,o}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$
$$= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot {r_o}^{W_o} \cdot \left(\frac{r_i}{r_i + A_i}\right)^{W_i} \cdot (r_i + A_i)^{W_i} \cdot \prod_{t \neq i,o}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$
$$= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot {r_o}^{W_o} \cdot {r_i}^{W_i} \cdot \prod_{t \neq i,o}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$
$$= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot \prod_{t=0}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1}$$
$$= \pi_{n-1} \cdot \Gamma^{-1}$$

   Since A_o and A_i are arbitrary, our formula for for $\pi_{n-1} \cdot \Gamma^{-1}$ is protected for all values of A_o and A_i, including flashloans and MEV attacks. ♪

2. Suppose some mints or burns LP tokens, changing the supply of the LP tokens by a factor of x. $\pi^\star_{n-1}$ signifies the changed pool value as a result of LP mint/burn.

$$
\begin{aligned}
\text{Then } \pi^\star_{n-1} \cdot \Gamma^{-1} &= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot \prod_{t=0}^{n-1} (x \cdot r_t)^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot (x \cdot \Gamma)^{-1} \\
&= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot \prod_{t=0}^{n-1} x^{W_t} \cdot \prod_{t=0}^{n-1} {r_t}^{W_t} \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot x^{-1} \cdot \Gamma^{-1} \\
&= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot x^{\sum_{t=0}^{n-1} W_t} \cdot V \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot x^{-1} \cdot \Gamma^{-1} \\
&= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot x \cdot V \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot x^{-1} \cdot \Gamma^{-1} \\
&= \frac{1}{\prod_{t=0}^{n-1} {W_t}^{W_t}} \cdot V \cdot \prod_{t=0}^{n-1} {p_t}^{W_t} \cdot \Gamma^{-1} \\
&= \pi_{n-1} \cdot \Gamma^{-1}
\end{aligned}
$$

Since x is arbitrary, our formula is protected from all attempts at manipulating the LP token supply. ♪