# COMS 6998-006 (Foundations of Blockchains): Homework #8

Due by 11:59 PM on Thursday, December 9, 2021

**Instructions:**

(1) Solutions are to be completed and submitted in pairs.

(2) We are using Gradescope for homework submissions. See the course home page for instructions, the late day policy, and the School of Engineering honor code.

(3) Please type your solutions if possible and we encourage you to use the LaTeX template provided on the Courseworks page.

(4) Write convincingly but not excessively. (We reserve the right to deduct points for egregiously bad or excessive writing.)

(5) Except where otherwise noted, you may refer to your lecture notes and the specific supplementary readings listed on the course Web page *only*.

(6) You are not permitted to look up solutions to these problems on the Web. You should cite any outside sources that you used. All words should be your own. Submissions that violate these guidelines will (at best) be given zero credit, and may be treated as honor code violations.

(7) You can discuss the problems verbally at a high level with other pairs. And of course, you are encouraged to contact the course staff (via the discussion forum or office hours) for additional help.

(8) If you discuss solution approaches with anyone outside of your pair, you must list their names on the front page of your write-up.

(9) Some of these problems are difficult, so your group may not solve them all to completion. In this case, you can write up what you've got (subject to (4), above): partial proofs, lemmas, high-level ideas, counterexamples, and so on.

## Problem 1

(20 points) Recall that the spot price in a Uniswap pool is

$$\pi(x, y) = \frac{y}{x},$$

where $x$ and $y$ denote the number of A-tokens and B-tokens in the pool, respectively.

(a) (4 points) Suppose the going price on the open market (e.g., Coinbase) for token A (e.g., ETH), in terms of token B (e.g., USDC), is $p$. Argue why you would expect any Uniswap pool with these two tokens to contain token quantities $x$ and $y$ that satisfy $\frac{y}{x} = p$ (or something very close to this).

(b) (3 points) Prove that, under the proposed equilibrium assumption from part (a), the two parts of a Uniswap pool (the A-tokens and the B-tokens) have equal value. Conclude that, at equilibrium, the combined value (denominated in B-tokens) of a Uniswap pool with token quantities $x$ and $y$ and with a market price of $p$ (of A-tokens in terms of B-tokens) can be written as $2px$ or as $2y$.

(c) (3 points) Suppose the price (of A-tokens in terms of B-tokens) jumps by a factor of $(1+\delta)^2$. (E.g., if the price doubles, $\delta = \sqrt{2} - 1 \approx 0.414$.) What will be the token quantities $(x', y')$ at the new equilibrium?

(d) (2 points) What is the combined value (denominated in B-tokens) of the new quantities of tokens $(x', y')$ given the new price?

(e) (2 points) What would have been the value of the original quantities of tokens $(x, y)$ at the new price?

(f) (3 points) The *divergence loss* is the difference between the quantity in (e) and that in (d). Give a simple formula for the divergence loss, as a function of $\delta$ and the original token quantities.

(g) (3 points) What happens to the ratio between the quantities in (d) and (e) as we take $\delta \to \infty$?

## Problem 2

(15 points) A *constant-function market maker (CFMM)* is defined by a trading invariant function $f(x, y)$ (where $x$ and $y$ denote the number of A-tokens and B-tokens in the pool, respectively), with a trade $(x, y) \mapsto (x', y')$ permitted if and only if it leaves the function $f$ invariant: $f(x', y') = f(x, y)$. Note that Uniswap is the CFMM defined by the function $f(x, y) = xy$.

(a) (6 points) Assume that $f$ is continuously differentiable. Prove that, in general, the implied spot price (of an infinitesimal purchase of $A$-tokens, denominated in $B$-tokens) is

$$\pi(x, y) = \frac{\frac{\partial f}{\partial x}\big|_{(x,y)}}{\frac{\partial f}{\partial y}\big|_{(x,y)}}.$$

[Hint: Feel free to use the Implicit Function Theorem without proof. Alternatively, you can provide a non-rigorous intuitive argument, as long as it is quite convincing.]

(b) (5 points) Prove that for every continuously differentiable and strictly increasing function $g$ (e.g., $g(z) = \sqrt{z}$), the CFMM with trading invariant function $f(x, y) := g(xy)$ has the same implied spot price as in a Uniswap pool (for every $x$ and $y$).

[Hint: Chain Rule.]

(c) (4 points) Balancer is a generalization of Uniswap, and is a CFMM that uses the trading invariant function $f(x, y) = x^w y^{1-w}$ for some parameter $w$. (The value of $w$ is specified at pool creation time and then fixed forevermore.) What is the corresponding spot price, as a function of $w$?

## Problem 3

(10 points)

(a) (4 points) Prove that in a Uniswap pool that is at equilibrium in the sense of Problem 1, the value (in USD, say) of the A-tokens in the pool equals the value (again, in USD) of the B-tokens in the pool.

(b) (6 points) State and prove a version of (a) that holds for the Balancer pools described in part (c) of Problem 2.

## Problem 4

(20 points) Uniswap pools have trading fees (which to this point we have been assuming are zero). Let $\mu$ denote a fee rate (e.g., .3%). Now, to buy $\Delta$ A-tokens from the pool, the required deposit $\Delta'$ of B-tokens must satisfy

$$(x - \Delta)(y + (1 - \mu)\Delta') = xy;$$

that is, the product of token quantities should remain constant after setting aside a $\mu$ fraction of the deposited coins to cover fees. The full $\Delta'$ amount of B-tokens is deposited in the pool (both the $1-\mu$ fraction to cover the cost of the A-tokens, and the additional $\mu$ fraction for fees to the pool and its liquidity providers).

(a) (5 points) Argue that every trade strictly increases the product of the pool's token quantities. (That is, the "$k$" parameter increases each time there's a trade.)

(b) (5 points) Inclusive of fees, what is now the spot price (as a function of $x$, $y$, and $\mu$)?

(c) (5 points) Suppose:

- the current market price of token A (in terms of token B) is $p$;
- a Uniswap pool is initialized with token quantities $x$ (of A-tokens) and $y$ (of B-tokens) that satisfy $p = \frac{y}{x}$ (i.e., the pool is initialized at equilibrium, in the sense of Problem 1);
- the market price then jumps to $(1+\delta)^2 p$;
- some trader makes a single trade that brings the token quantities to the corresponding new equilibrium $(x', y')$ (as calculated in Problem 1(d)).

What is the smallest value of $\mu$ that, for every $\delta > 0$, guarantees that the creator of the pool is no worse off than if it had simply held onto its assets?

[Note Problem 1(f) is relevant here.]

(d) (5 points) Repeat part (c) under the additional assumption that the market price will never leave the interval $[p, 4p]$ (i.e., assuming that $\delta \in [0, 1]$).