A Note on Borrowing Constant Function Market Maker Shares

Tarun Chitra
tarun@gauntlet.network

Guillermo Angeris
angeris@stanford.edu

Alex Evans
alex@placeholder.vc

Hsien-Tang Kao
ht@gauntlet.network

April 2021

Abstract

Constant function market makers (CFMMs) such as Uniswap, Balancer, and Curve, among many others, make up some of the largest decentralized exchanges on smart contract platforms like Ethereum. As the amount of capital deposited in these protocols has grown, improving capital efficiency for liquidity providers (LPs) has become an increasingly important challenge. One way to improve efficiency is to allow LPs to borrow Ether or USD against their shares in a CFMM protocol. In this note, we investigate the security and capital efficiency of allowing such lending. We provide sufficient conditions for LP borrowing to be at least as secure and capital efficient as direct borrowing in Aave/Compound. Furthermore, we show that the exposure taken by CFMM lenders can be replicated via barrier options, allowing for risks to be hedged. Finally, we show that the payoff of borrowed CFMM LP shares replicates bounded convex payoffs. Combined, these results suggest that CFMM lending is a safe mechanism for improving capital efficiency.

1 Introduction

Constant Function Market Makers (CFMMs) have grown to tens of billions of dollars of available liquidity and billions of dollars of daily trading volume. These systems are used to facilitate the decentralized exchange of cryptoassets, allowing for capital providers searching for yield to be automatically matched with traders looking to swap. Capital providers, commonly referred to as liquidity providers (LPs), supply assets to a smart contract in order to earn yield. On every transaction with a CFMM, trading fees accrue to compensate liquidity providers for allowing their capital to be used in executing a swap. In some situations, these fees do not cover the losses that liquidity providers engender due to large price movements. This opportunity cost, colloquially known as impermanent loss, represents the fact that LPs effectively hold shares in a derivative asset with concave ("negative gamma") exposure [AC20, AEC20]. One mechanism to improve capital efficiency for LPs is to provide lending mechanisms for LPs to achieve partial liquidity on their positions. Unlike in conventional finance, such lending mechanisms are inherently composable with CFMMs thanks to the open and common interfaces in decentralized finance (DeFi). Composability is the most important improvement that DeFi provides over traditional lending and trading and LP share lending is the quintessential example of something difficult to do without a blockchain.

One of the main hurdles to increasing both usage and liquidity for CFMMs is capital efficiency. Roughly speaking, capital efficiency refers to the minimum amount of assets needed to be added to a pool to ensure that trades of a given size never incur more than a certain amount of transaction cost. An ideal, capital efficient protocol would allow the CFMM to profitably execute a swap (e.g. buy the asset to be sold and return the traders' desired asset) while minimizing the amount of capital placed in the pool. Capital efficiency is controlled (to first-order) by the curvature of the CFMM trading function [AEC20, §2]. In practice, adjustments to curvature have led to dramatically reduced fees — whereas Uniswap charges 0.3% per swap Curve is able to charge 0.04% per swap due to lower curvature and support only for mean-reverting assets. The latest versions of Balancer [Mar21b] and Uniswap [AZS$^+$21] implicitly allow LPs to adjust the curvature of their individual position, thus improving an individual LP's capital efficiency.

Another mechanism for improving capital efficiency is to lend out either the assets contained in the pool or the LP shares themselves. Sushiswap's Kashi [Ayo21] and Balancer and Aave's asset manager [Mar21a] earn yield on assets in LP shares when they are not needed. This is similar, in spirit, to how exchange-tradeable funds (ETFs) often lend out a portion of their assets to short sellers in order to earn additional yield [Boy20, BW16]. On the other hand, lenders such as Aave [FCCM21], Alpha Homora [Pit], and MakerDAO [JMW$^+$20] allow for LP share holders to directly borrow assets such as stablecoins (Dai, USDC, USDT) and Ethereum. In these loans, LP shares are used as collateral in an over-collateralized loan that is liquidated if the value of the LP share is ever less than the value of the asset borrowed. Most users of these loans usually aim to earn positive yield on their borrowed assets, improving the borrower's expected returns. Both of these solutions improve capital efficiency because they allow for capital unused in processing swaps to earn addition yield (in addition to CFMM fees).

How should one assess whether a lending platform is providing improved capital efficiency? Recall that an LP share represents fractional ownership in a portfolio of several assets. Each trade against the portfolio rebalances the portfolio and changes its value. This rebalancing can be viewed as a control mechanism for keeping a portfolio at approximately constant mixture via a game between traders, arbitrageurs, and liquidity providers (e.g. LP share holders) [EAC21]. In the process, LPs can realize losses indirectly due to concavity of their payoff function. For instance, if an LP believes that trading will be mean-reverting (which leads to high LP profits and lower arbitrageur profits [AEC20]), they can borrow against their LP shares and then mint new LP shares to earn a higher share of fees.

Before interacting with an LP share lending platform, the user first creates LP shares by depositing the requisite assets to a CFMM contract. The user then places their LP shares in the lending protocol and can borrow units of the numéraire asset, upt to some collateralization threshold. Suppose that $c_t \in \mathbf{R}^n$ is the price vector of each asset in terms of the numéraire (first asset) at time $t > 0$. If the value of the collateral ever falls below the minimum collateralization threshold, the lender is liquidated, incurring a penalty. Unlike a loan of a single asset for another, the choice of numéraire and more generally, the portfolio value function, can lead to drastically different liquidation conditions. This means that risk parameters such as collateralization requirements need to be adjusted not only with regards to the volatility of the assets in the portfolio, but with regards to the volatility of the entire portfolio. Computing the net volatility of the portfolio relative to the components can lead to results that appeal to Simpson's Paradox. For instance, suppose that the volatility of asset A is 25% annualized and that of asset B is 50% annualized. Borrowing asset B against asset A collateral will require less collateral (measured in numéraire terms) than borrowing asset A against assert B (in numéraire terms). We should expect, in an averaged sense, that the collateral requirements for the more risky borrowing scenario to be two times the other scenario. However, it is possible that borrowing asset A or asset B against an LP share consisting of assets A and B will require more collateral than a borrow against asset B or asset A (respectively). This is because if assets A and B are highly correlated, then the probability of a liquidation against an LP share is higher than the sum of the probabilities of liquidation with A or B as collateral.

In this note, we provide the first (to the authors' best knowledge) formalism of LP share lending. We first compare collateral requirements between borrowing assets A against asset B compared to borrowing asset A against an LP share consisting of assets A and B. In the process, we generalize the notion of a collateral factor and portfolio value such that traditional cryptoasset borrowing can be viewed as LP share borrowing with a particular portfolio value function. We demonstrate that the security of LP share lending reduces to that of traditional on-chain lending [FCCM21, KCCM20, LH19] provided that the loan-to-value ratio (also known as the collateral factor) dynamically updates with LP share value. In Appendix A, we expand this result to borrowing arbitrary LP shares against other LP shares. These results show that LP share lending can, with proper design, be as safe as traditional asset lending. Moreover, the results provide a quantitative understanding of the capital efficiency differences between LP share and direct lending. Counterintuitively, we find that there exist certain scenarios when LP share lending is *more* capital efficient than direct lending.

In order to quantify the precise risk involved in lending, we investigate the outstanding position of the lending protocol itself. Using the machinery of generalized collateral factors, we show that one can replicate the exposure that the protocol holds via a covered options portfolio that includes collateral, quanto options, and binary ('one-touch') options. Using this replication, we provide a mechanism for a lending protocol to hedge its risk given a set of collateral factors. Our replication utilizes Black-Scholes assumptions and put-call symmetry [CEG99, CL09] to construct exact solutions for lender risk. This replicating portfolio effectively demonstrates that an LP share lender can hedge their portfolio risk by purchasing portfolio insurance [Car87]. We note that while our results hold in the no-arbitrage, feeless scenario, emergent phenomena discovered via simulation and during crises, such as cascading liquidations [KCCM20, FCCM21, KCCM21], are not insured via these hedges. However, these results provide a basis for constructing hedges and insurance for on-chain lenders to ensure that CFMM lending is always at least as safe as traditional lending.

Finally, we show that a particular set of locally convex payoff functions can be replicated by borrowing against LP positions (which are necessarily concave), extending the results of [AEC21] to convex payoffs. This demonstrates that borrowers of LP shares are incentivized to create positions in order to construct bounded convex exposures (e.g. barrier options) in a decentralized manner. Combined, these results demonstrate that a) lenders can provide improved capital efficiency b) lenders can hedge their risks with portfolio insurance and c) borrowers can cheaply construct leveraged positions. Given the reduced computational complexity of CFMMs, this suggests that the space of decentralized, on-chain finance is at least as large as those of traditional financial products.

2 Formalism

2.1 Lending Protocols

Decentralized lending protocols such as Aave [FCCM21] and Compound [KCCM20] allow users to trustlessly execute overcollateralized loans between cryptoassets. A user of a lending protocol deposits collateral of coin i into a smart contract that pools assets by type. For instance, a user might deposit 100 ETH or \$100,000 into this contract. A borrower is a user that borrows another cryptoasset against their deposited collateral. For instance, a borrower might deposit 100 ETH and borrow \$10,000 against their ETH collateral. The loans are overcollateralized in that the value of the borrowed asset must always be less than the value of the deposited collateral (where value is measured in relative terms).

Formally, let $p_{i,j}(t)$ be the price of asset i in terms of asset j. If a user deposits X units of asset j into the protocol, they can borrow at most $c_f \cdot p_{i,j}(t) \cdot X$ units of asset i. The constant $c_f \in (0, 1)$ is known as the *collateral factor* and represents the maximum borrowable quantity relative to the price. A small collateral factor is conservative and less-risky for the lender, but is capital inefficient for the borrower. On the other hand, a collateral factor near 1 is risky for the lender but capital efficient for the borrower.

Suppose that at time $t > 0$, a borrower deposits X units of asset j and borrows $Y < c_f \cdot p_{i,j}(t) \cdot X$ units of asset i. If at any time $t' > t$, the borrower has not repaid the loan then the loan is in one of two states. The loan is *liquidatable* when $c_f \cdot p_{i,j}(t') \cdot X < Y$. A liquidatable loan can be partially liquidated from the protocol, leaving the borrower with collateral $X' < X$ that is still redeemable. A loan is *insolvent* or *defaulted* when $p_{i,j}(t') \cdot X < Y$. When in this state, the entire loan can be liquidated and the borrower cannot redeem any collateral (e.g. $X' = 0$ doesn't change). Both liquidatable and insolvent loans are effectively auctioned (akin to a foreclosure auction) to a user who buys it from the smart contract at a discount (known as the *liquidation incentive*). Liquidatable loans will have a portion of the loan auctioned (e.g. the amount ΔX needed to return the loan to a state $c_f p_{i,j}(t')(X - \Delta X) > Y$), whereas insolvent loans are completely liquidated. The goal of lending protocols is to choose c_f (as well as other parameters, such as the liquidation incentive and the interest rate curve) such that the expected number of liquidations is minimized while remaining attractive for borrowers.

Currently, lending protocols such as Aave and Compound allow for any ERC-20 asset to be borrowed or lent (upon approval from a governance vote). This includes LP tokens, which can be represented using token standards such as ERC-20.[1]

2.2 CFMMs

We will briefly review the basic definitions needed for constructing a CFMM (for more details, we encourage the reader to refer to [AC20, EAC21, AEC21]. Suppose that we have a CFMM described by a convex trading function $\varphi : \mathbf{R}^n_+ \to \mathbf{R}$, as described in [AC20, §1]. At each time $t \in \mathbf{N}$, the reserves $R(t) \in \mathbf{R}^n_+$ determine a set of marginal prices, $p^{\varphi}_{i,j}(t)$, defined as:

$$p^{\varphi}_{i,j}(t) = \frac{\partial_i \varphi(R(t))}{\partial_j \varphi(R(t))}$$

which is the price of coin i in terms of coin j. Without the loss of generality, we will assume that the first index is the numéraire and use the notation $p^{\varphi}_i(t) = p^{\varphi}_{i,1}(t)$ and $p^{\varphi}(t) = (p^{\varphi}_1(t), \ldots, p^{\varphi}_n(t))$. The numéraire portfolio value of a CFMM, $P^{\varphi}_V(t)$, is the total value of the assets measured relative to a numéraire and is defined as

$$V_{\varphi}(p^{\varphi}(t)) = \sum_{i=1}^{n} R_i(t) p^{\varphi}_i(t) = R(t) \cdot p^{\varphi}(t)$$

3 Capital Efficiency

Consider a Compound market where asset A can be borrowed against asset B with collateral factor (or loan-to-value) c_f. Similarly, consider a second Compound market where asset A can be borrowed against a Balancer pool consisting of assets A and B with collateral factor c_f^{LP}. For this pool, the trading function can be represented as,

$$\varphi(R_a, R_b) = R_a^{w_a} R_b^{w_b}$$

where the weights $w_a, w_b \in (0, 1)$ satisfy $w_a + w_b = 1$. By definition, collateral factors are defined as the ratio of the maximum quantity q_A that can be borrowed given quantity q_B

[1] We note that Uniswap V3 [AZS$^+$21] turns LP tokens into non-fungible tokens rather than ERC-20 assets. However, these NFTs can be fractionalized/securitized into ERC-20s to recover the ability to be borrowed and lent.

as collateral at price $p_{A,B}(t)$. We extend this definition to portfolios (such as CFMMs) by defining the collateral factor as the ratio of the maximum borrowable quantity q_A to the A-denominated portfolio value of the collateral. Using this definition we can write c_f, c_f^{LP} in terms of the borrowable quantities

$$\begin{aligned} c_f &= \frac{q_A}{q_B p_{A,B}(t)} \\ c_f^{\varphi} &= \frac{q_A}{w_A q_A + w_B q_B p_{A,B}(t)} \end{aligned}$$

We can write c_f^{φ} in terms of c_f as

$$\begin{aligned} c_f^{\varphi} &= \frac{q_a}{q_B p_{A,B}(t)} \left(\frac{1}{\frac{w_A q_A}{q_B p_{A,B}(t)} + w_B} \right) \\ &= c_f \left(\frac{q_B p_{A,B}(t)}{w_A q_A + w_B q_B p_{A,B}(t)} \right) \end{aligned} \tag{1}$$

We can have more aggressive borrowing from the LP share for fixed c_f if $c_f^{\varphi} > c_f$ which occurs only if

$$\begin{aligned} & q_B p_{A,B}(t) > w_A q_A + w_B q_B p_{A,B}(t) \\ \iff & (1 - w_B) q_B p_{A,B}(t) > w_A q_A \\ \iff & w_A q_B p_{A,B}(t) > w_A q_A \\ \iff & q_B p_{A,B}(t) > q_A \end{aligned}$$

Therefore, borrowing against an LP share (sans fees/growth) is more efficient than a direct borrow if

$$\boxed{q_B p_{A,B}(t) > q_A} \tag{2}$$

This result demonstrates that it is possible for borrowing against an LP share to be more capital efficient than borrowing directly against collateral. Moreover, note that equation (1) also intimates that a dynamic collateral factor — c_f^{φ} changes as a function of price — can *exactly* replicate the capital requirements of a direct collateral borrowing at collateral factor c_f. This also suggests that LP share lending is better than direct collateral lending (sans impermanent loss) — with the proper selection of collateral factors, a lender can earn fees from the CFMM itself (e.g. from trading activity) and from lending out the CFMM to borrowers who want to concentrate their earnings. We have seen a number of attempts of mixing CFMMs with lending to improve capital efficiency for trading and this result provides some theoretical underpinning to the growth of these platforms [Ayo21].

Note that this analysis does not account for accrued fees and it is possible for this condition to be weakened. If $f_A, f_B \in \mathbf{R}$ are the net accrued fees, then we can replace q_A, q_B with $q_A + f_A, q_B + f_B$ in eq. (2). Note that these accruals can be negative (to account for so-called impermanent loss). Finally, note that we generalize the two component borrowing with LP shares as collateral to the general n-dimensional scenario of borrowing LP shares against other LP shares in Appendix A. Since we can embed traditional borrowing within the context of LP share borrowing (e.g. by making the portfolio weights a delta function), this is the most generic type of lending/borrowing activity in DeFi.

4 Replicating Portfolio of a CFMM lender

A natural question to ask is if it is possible to describe the position held by a CFMM lender in terms of other financial instruments. For instance, a CFMM lender such as the Maker or Alpha Homora protocols is holding collateral (e.g. an LP share) and effectively gives a borrower a call option to repurchase their collateral. Concretely, one might ask if one can describe the net position held by Compound by prices and option prices on particular crypto assets. Abstractly, this intimates that the exposure of a CFMM lender is similar to that of a covered call. The goal of this section is to make this intuition more precise and to provide formulas for the risk held by the protocol as a lender. The main assumptions made will be standard quantitative finance assumptions regarding no-arbitrage. Recent work has shown that covered calls can be emulated by CFMMs and we illustrate that the exposure that a CFMM lender holds can be replicated by another CFMM [AEC21]. This recursive nature of replicating a lender using CFMMs suggests that CFMMs are the fundamental building block of both trading and lending in compute constrained, decentralized settings.

The analogy made to covered calls, which while intuitively apt, is not quite precise. In a lending protocol without liquidations (e.g. Synthetix prior to SIP-15), the position held a lending protocol is closest to that of a covered quanto call position [H$^+$09, Ch. 29] [Wys10]. However, without liquidations, the no-arbitrage, complete market behavior of exercising an option when it has positive value doesn't exist. To motivate later constructions, we will first describe an example of why a covered call is not the correct model for CFMM lending.

4.1 Quanto Options and Covered Calls

Suppose that a borrower opens up a position where they place q_c units of collateral in a lending smart contract and borrow q_b units of borrowed asset. Let $p(t)$ be the price of the collateral asset in units of borrowed asset and $p(t_0)$ be the price at the time t_0 that the borrow position was opened. Assume that the borrower maximizes their borrow so that $\frac{q_c}{p(t_0)q_b} = c_f$ for a collateral factor $c_f \in (0, 1)$. The liquidation price, $p_{\text{liq}} = c_f p(t_0)$, is the price at which the lender loses money. The protocol's portfolio consists of q_c units of collateral and an obligation to let the buyer buy back q_c units of collateral for q_b units of borrowed asset (plus interest). If $p(t) < c_f p(t_0)$ and the protocol was replicated by a covered call (short put plus premium), then the borrower can buy back q_c units of collateral for $p(t)q_b < c_f p(t_0)q_b < q_c$ units of collateral and books a profit of $q_c - p(t)q_b$ units of collateral asset. Clearly, the lender wants to avoid such a scenario as they have to pass losses through the liquidity providers. Note that in finance terminology, that an option with an adjustable delivery quantity is called a *quanto option* — an option struck in one asset, paid back in another [H$^+$09, Ch. 29].

In practice, protocols limit the amount that can be bought back when $p(t) < c_f p(t_0)$ by using liquidations. A protocol executes a liquidation by effectively selling a slightly out of the money option to any market participant (a set which includes the borrower). There are two broad ways that protocols execute liquidations. Protocols like Compound and Aave will choose $a \in (0, \frac{1}{2})$ and allow a market participant to buy the collateral for $(1-a)c_f p(t_0)$ provided that $p(t) < c_f p(t_0)$. The discount percentage a is known as a liquidation incentive. On the other hand, protocols like MakerDAO auction off the collateral at a price $a_t c_f p(t_0)$ where $a_t \in (0,1)$ is non-increasing in $t > 0$. A market participant who executes this option at a price lower than spot price $p(t)$ is known as a *liquidator*. Given that the implicit option is only valid when $p(t) < c_f p(t_0)$, the protocol is effectively selling a barrier option [H$^+$09] to the market at a strike price that is discounted (e.g. $(1-a)c_f p(t_0)$). Combined, these two observations indicate that lending protocols — both CFMM lenders and direct lenders of underlying assets — are effectively selling options to market participants. However, the nature of these options is different depending on which participant executes the option and the barrier price (e.g. the liquidation price $c_f p(t_0)$).

4.2 Parameters in Aave and Compound

In the preceeding sections, we were somewhat lax with our treatment of collateral factors and liquidation thresholds. This section will focus on mapping the precise parameters used in Aave and Compound to a reduced collateral factor ℓ, that we will use in the quantitative results of the sequel. The two largest pure lending protocols in DeFi are Aave [FCCM21] and Compound [KCCM20]. These protocols have both had over \$5 billion of assets held within them and have issued hundreds of billions of dollars of loans over their lifetimes. While the two protocols are extremely similar, they have differences in terminology for parameters utilized. In this section, we will describe how their parameters map to the ones used in the sequel.

As in §3, the collateral factor is defined as the maximum amount that can be borrowed given a particular collateral deposit. Compound invented this terminology [LH19], whereas Aave refers to the same quantity as loan-to-value or LTV. For consistency, we will refer to LTV symbolically as c_f throughout this paper. Another important parameter is the liquidation threshold, $\ell_t \in (0,1)$, which is the point at which a loan is defined to be liquidatable. Note that by definition $c_f \leq \ell_t$. To see this, note that c_f defines the maximum borrow given an initial collateral position and price of the collateral asset in units of borrowed asset, $p(t_0)$. If $\ell_t < c_f$, then a maximum sized loan (e.g. q_b such that $\frac{q_b}{p(t_0)q_c} = c_f$) would be instantly liquidatable on creation.

Compound and Aave differ in how they define these two parameters. In Compound, one always has $\ell_t = c_f$, such that a maximum sized borrow position is instantly liquidatable if $p(t_0 + \epsilon) < p(t_0)$ for some $\epsilon > 0$. In Aave, these are kept as separate parameters, only subject to the condition $c_f \leq \ell_t$. If a borrower maximizes their position (q_b, q_c) such that $c_f = \frac{q_b}{q_c p(t_0)}$, then the price of liquidation in Aave is define as

$$p_{\text{liq}}^{\text{aave}} = \frac{c_f}{l_t} p(t_0)$$

If $p(t) < \frac{c_f}{l_t}p(t_0)$, then the liquidator can buy back q_c units of collateral with

$$q_c p(t) < q_c \frac{c_f}{l_t} p(t_0) = \frac{q_b}{l_t}$$

units of borrowed asset. For the rest of this section, we will let $\ell = \frac{c_f}{l_t}$ be the reduced collateral factor, which plays a role in the model constructed in the next section.

4.3 Model Description

In the rest of this section, we will make some additional assumptions to ease the usage of no-arbitrage pricing. Without the loss of the generalize, we will describe the model in terms of borrowing an asset B using collateral of asset A without specializing the the scenario where assets A and B are CFMMs. The analysis of §3 justifies this as we can replicate parameters such as the collateral factor, for a CFMM by dynamic adjustment of the parameters described in this section. Firstly, we assume that the prices of the collateral asset $S_{\text{collateral}}(t)$ and borrowed asset $S_{\text{borrow}}(t)$ obey geometric brownian motions relative to a fixed, common numéraire:

$$dS_{\text{collateral}}(t) = (r_c - r)S_{\text{collateral}}(t)dt + \sigma_c S_{\text{collateral}}(t)dW_t^c \tag{3}$$
$$dS_{\text{borrow}}(t) = (r_b - r)S_{\text{borrow}}(t)dt + \sigma_b S_{\text{borrow}}(t)dW_t^b \tag{4}$$
$$dW_t^b dW_t^c = -\rho dt \tag{5}$$

where r_b, r_c and r are the risk-free rates on the borrowed asset, collateral asset, and numéraire, respectively, and ρ is a correlation term. Note that ρ is negative due to no-arbitrage pricing: the triangle of selling numéraire for borrowed asset, selling borrowed asset for collateral asset, and then finally selling collateral asset for numéraire needs to have zero profit (which only occurs when the correlation is negative).

In this notation, we can write $p(t) = \frac{S_{\text{collateral}}(t)}{S_{\text{borrow}}(t)}$ and an application of Ito's lemma and the chain rule gives (c.f. [Wys10, Eq. 6])

$$dp(t) = (r_b - r_c - \sigma_b^2 - \rho\sigma_b\sigma_c)p(t)dt + \left(\sqrt{\sigma_b^2 + \rho\sigma_b\sigma_c}\right)p(t)dW^p(t)$$

where $dW^p(t)$ is a Brownian motion independent of W^c, W^b. For simplicity, we will denote the associated drift and volatility of this process as follows:

$$\mu_p = r_b - r_c - \sigma_b^2 - \rho\sigma_b\sigma_c \tag{6}$$
$$\sigma_p^2 = \sigma_b^2 + \rho\sigma_b\sigma_c \tag{7}$$

4.4 Borrower: Digital Call Option

We first claim that a lending protocol sells a quanto digital call option to the borrower. A quanto digital call option [Wys10, §1.4] is an option with payoff $DO(K, S, Q)$ defined as,

$$DO(K, S, Q) = Q\mathbf{1}_{S \geq K}$$

where S is the price of the borrowed asset in terms of the collateral asset, K is a strike price, and Q is the quanto factor. The quanto factor represents the notional in the settlement asset (e.g. collateral asset) that is paid when the option is executed provided that $S \geq K$. In the case of a lending protocol, we claim that the borrower holds a digital option with payoff $DO(\ell p(t_0), p(t), q_c)$, where q_c is the collateral placed in the protocol. Note that this option naturally expresses the idea that the borrower can only retrieve their collateral provided that $p(t) \geq \ell p(t)$. Standard option pricing theory shows that the no-arbitrage value of a quanto digital option is [Wys10, §1.4]:

$$\mathsf{DO}(\tilde{c}_f, p(t_0), q_c) = \mathop{\mathbf{E}}_{\mathsf{GBM}(\mu,\sigma)}[DO(\ell p(t_0), p(t), q_c)] = q_c e^{-r_c T} N(d_-) \tag{8}$$

where:

- $\mathsf{GBM}(\mu, \sigma)$ is a geometric brownian motion with mean μ and standard deviation σ
- $N : \mathbb{R} \to [0, 1]$ is the normal cumulative distribution function, $N(x) = \int_{-\infty}^{x} e^{-\frac{x^2}{2}} dx$
- $d_\pm = \frac{-\ln \ell + (\mu_p \pm \frac{1}{2}\tilde{\sigma_p}^2)}{\sigma_p \sqrt{t - t_0}}$

If we take the derivative of (8) with respect to c_f, we find

$$\partial_\ell \mathsf{DO}(\ell, p(t_0), q_c) = -\Omega\left(\ell^{\frac{1}{\sigma_p\sqrt{t-t_0}} - 1}\right)$$

Firstly, this shows that the price of the option decreases as the collateral factor increases. This captures the intuitive that the option is less valuable the more likely you are to be liquidated. Secondly, let $\tau = \frac{1}{\sigma_p^2}$. While $t < t_0 + \tau$, the impact of a high collateral factor on option value is large, whereas when $t > t_0 + \tau$ the impact of a low collateral factor is larger. Recall that $c_f \in (0, 1)$ represents the maximal percentage of borrowable assets. When c_f is near 1, a loan is much more likely to be liquidated, regardless of volatility. However, when the ℓ is near 0, a loan is only likely to be liquidated under extremely large price moves. The likelihood of these occurring when $t < t_0 + \tau$ is very low and hence there is little impact on the option value. However, after $t > t_0 + \tau$, the probability of this happening is non-trivial and we see a large impact on option price. Combined, these observations illustrate that the option value can handle relatively high collateral factors (higher capital efficiency) for long periods of time only if the asset volatility is low. Unlike prior numerical assessments of this risk [KCCM20], we were able to arrive at this result strictly via no-arbitrage pricing arguments. This result also suggests that repeated updates to collateral factors according to volatility [FCCM21] is theoretically justified.

4.5 Liquidator: Barrier Option

On the other hand, the liquidator is issued a barrier option that is only executable when $p(t) < \ell p(t_0)$. This is known as a down-and-in call and can be statically replicated via standard options [CEG99]. Let $C(K)$ be the price of a standard call option struck at K and let $P(K)$ be the price of a standard put option. Then we can write the payoff of a down-and-in European call with barrier at $H > K$, $DOIC(K, H)$, as

$$DOIC(K, S, H) = (S - K)_+ \mathbf{1}_{S \leq H}$$

Put-call symmetry replication results from [CEG99, §II.A] show that

$$\mathbf{E}[DOIC(K, S, H)] = \frac{K}{H} \mathbf{E}\left[P\left(\frac{H^2}{K}\right)\right]$$

For Aave and Compound, we can view the liquidator as holding a down-and-in call struck at a discount to the liquidation price $K = (1 - a)\ell p(t_0)$ and with barrier $\ell p(t_0)$. Therefore, the expected value of this option under no-arbitrage pricing to the liquidator is:

$$\mathbf{E}[DOIC((1 - a)\ell p(t_0), p(t), \ell p(t_0))] = (1 - a)\, \mathbf{E}\left[P\left(\frac{\ell p(t_0)}{1 - a}, p(t)\right)\right] \tag{9}$$

where $P(K, S)$ is a put struck at K with current price S. If we add a quanto factor and use the traditional Black-Scholes pricing formula [H$^+$09], this gives a liquidator option value of

$$\begin{aligned} \mathsf{DOIC}(a, c_f, p(t_0), t, q_c) &= q_c \mathop{\mathbf{E}}_{\mathsf{GBM}(\mu,\sigma)}[DOIC((1 - a)c_f p(t_0), p(t), c_f p(t_0))] & (10) \\ &= (1 - a)q_c e^{-r\tau}(N(-d_-)\frac{c_f p(t_0)}{1 - a} - N(-d_+)e^{r\tau} p(t)) & (11) \end{aligned}$$

where

$$d_\pm = \frac{1}{\sigma\sqrt{\tau}}\left(\ln\frac{1 - a}{\ell} + r \pm \frac{1}{2}\sigma^2\right)$$

and $\tau = t - t_0$. We note that more complicated exposures taken by liquidators such as the pooled exposure of Liquity [KCCM21] or the auction of MakerDAO [KL21] can also be replicated, although the Black-Scholes put-call symmetry formula doesn't apply. In [CL09, §5], one uses put-call symmetry to approximate asymmetric barrier options, which can be used for ascending or descending auctions (e.g. a_t is monotone).

4.6 Combined Exposure

Combining equations (8) with (9) intimates that under no-arbitrage, no liquidator competition, and geometric brownian motion (effectively the same assumptions as Black-Scholes), the portfolio held by the lender can be replicated by:

- q_c units of collateral
- Short $DO(\ell p(t_0), p(t), q_c)$
- Short $DOIC((1 - a)\ell p(t_0), p(t), c_f p(t_0))$

Using standard no-arbitrage arguments, it can be shown that $C(K, p(t)) \geq DOIC((1 - a)\ell p(t_0), p(t), \ell p(t_0)) + DO(\ell p(t_0), p(t), q_c)$. Intuitively, this follows from the idea that an unconditional call option $C(K, p(t))$ is more valuable than the sum of the two conditional options unless $a = 1$ and the option is European. This demonstrates that a CFMM lender is more overcollateralized than a covered call and as per [AEC21, §4], this exposure can be replicated via a CFMM.

5 Convex Payoff Approximation

Recently, it was shown that there is a bijective correspondance between certain concave payoff functions and CFMM trading functions. In [AEC21, §1.1], it is shown the 1-homogeneous, increasing, non-negative, concave payoff functions $V : \mathbf{R}^n \to \mathbf{R}$ can be replicated by holding LP shares. Given that a number of payoff functions that exist in finance are convex, such as the payoff of a call option, a natural question is whether CFMMs can be used to replicate convex positions. One natural way to do this is to short a CFMM share, which is enabled by lending. If a CFMM share has concave payoff function $V(c)$, then shorting the CFMM share should yield payoff $-V(c)$, which is convex.

Let $V(c_t)$ be the portfolio value of a CFMM share (in numéraire terms) at time t and suppose that a lender allows a user to use a numéraire as collateral for borrowing a CFMM share at time $t_0 > 0$. The user flow for using this to short a CFMM share is the following:

1. User places $\frac{1}{c_f}V(c_{t_0})$ of numéraire in CFMM lending protocol, borrows 1 LP share

2. User sells LP share for numéraire, holds $V(c_{t_0})$ of numéraire

3. User is profitable if $V(c_t) < V(c_{t_0})$, but is liquidated if there is $t > t_0$ such that $V(c_t) \geq \frac{1}{c_f}V(c_{t_0})$ (e.g. portfolio value increased by $\frac{1}{c_f}$)

Therefore, if a user shorts a CFMM share their value function is:

$$\tilde{V}(c_t) = -V(c_t)\mathbf{1}_{c_f V(c_t) < V(c_{t_0})}$$

Note that this function is not convex or even quasiconvex, but it is convex when $c_f V(c_t) < V(c_{t_0})$.

6 Conclusion

To the best of our knowledge, our results represent the first formal risk analysis of a composability in DeFi. We believe these results are useful for protocol designers, liquidity providers, and for active traders who want complex exposures in DeFi. These results demonstrate that composing DeFi protocols can lead to a much broader set of financial products with varying trade-offs. Utilizing lending to generate convex payoffs opens up the CFMM design space, which had mainly been limited to 1-homogeneous, concave functions. A deeper understanding of how CFMM lending works also provides quantitative bounds on how to design protocols with respect to risk and efficiency. Analyzing how to compare collateral factors for different LP shares provides a clear description of capital efficiency trade-offs that occur when borrowing against LP shares vs. underlying assets. On the other hand, replicating a protocol's portfolio exposure allows for one to compute approximate hedges for protocols. These replication results were inspired by the spirit of [CL09], which states

> We view [put-call symmetry] results as part of a broad program that aims to use European options — whose values are determined by marginal distributions—to extract information about path-dependent risks, and to hedge those risks robustly

In a similar vein, we view the path-dependent risks held by lenders in protocols like Aave as eminently hedgeable by portfolio insurance. As there has been an increase in the usage of on-chain insurance funds by lending protocols to improve capital efficiency [FCCM21,KCCM21], these results can be utilized to provide more precision insurance constructs for protocols. On the other hand by utilizing an explicit replication, sophisticated LPs can more precisely control their exposures by utilizing lending and our results.

References

[AC20] Guillermo Angeris and Tarun Chitra. Improved Price Oracles: Constant Function Market Makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 80–91, New York NY USA, October 2020. ACM.

[AEC20] Guillermo Angeris, Alex Evans, and Tarun Chitra. When does the tail wag the dog? curvature and market making. *arXiv preprint arXiv:2012.08040*, 2020.

[AEC21] Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating market makers. *arXiv preprint arXiv:2103.14769*, 2021.

[Ayo21] Ayoki. Introducing Kashi Lending and Margin Trading on SushiSwap's Bento-Box, Mar 2021. `https://medium.com/sushiswap-org/introducing-kashi-\lending-margin-trading-on-sushiswaps-bentobox-eb91286f6910`.

[AZS$^+$21] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. 2021.

[Boy20] Emma Boyde. What is securities lending, why do etfs do it and is it risky?, Nov 2020.

[BW16] Jesse Blocher and Robert E Whaley. Two-sided markets in asset management: exchange-traded funds and securities lending. *Vanderbilt Owen Graduate School of Management Research Paper*, (2474904), 2016.

[Car87] Peter Carr. *Portfolio Insurance and Stochastic Bond Prices*, volume 88. Cornell University, Johnson Graduate School of Management, 1987.

[CEG99] Peter Carr, Katrina Ellis, and Vishal Gupta. Static hedging of exotic options. In *Quantitative Analysis In Financial Markets: Collected Papers of the New York University Mathematical Finance Seminar*, pages 152–176. World Scientific, 1999.

[CL09] Peter Carr and Roger Lee. Put-call symmetry: Extensions and applications. *Mathematical Finance: An International Journal of Mathematics, Statistics and Financial Economics*, 19(4):523–560, 2009.

[EAC21] Alex Evans, Guillermo Angeris, and Tarun Chitra. Optimal fees for geometric mean market makers. *arXiv preprint arXiv:2104.00446*, 2021.

[FCCM21] Watson Fu, Tarun Chitra, Rei Chiang, and John Morrow. Aave market risk assessment. 2021. `https://gauntlet.network/reports/aave`.

[H^{+}09] John Hull et al. *Options, futures and other derivatives/John C. Hull.* Upper Saddle River, NJ: Prentice Hall,, 2009.

[JMW^{+}20] Jiecut, Andy McCall, Wjmelements, LongForWisdom, Joshua Pritikin, MakerMan, Swakya, and Hayden Adams. [uni-v1] uniswap liquidity tokens as collateral, Apr 2020.

[KCCM20] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. An analysis of the market risk to participants in the compound protocol. In *Third International Symposium on Foundations and Applications of Blockchains*, 2020.

[KCCM21] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. Liquity market risk assessment. 2021. `https://liquity-report.gauntlet.network`.

[KL21] Hsien-Tang Kao and Nathan Lord. Makerdao auction assessment. 2021. `https://maker-report.gauntlet.network`.

[LH19] Robert Leshner and Geoffrey Hayes. Compound: The money market protocol. *White Paper*, 2019.

[Mar21a] Fernando Martinelli. Balancer partners with aave to build the first v2 asset manager, Feb 2021. `https://medium.com/balancer-protocol/balancer-partners-with-aave-to-build-the-first-v2-asset-manager-d9c173330151`.

[Mar21b] Fernando Martinelli. Balancer v2: Generalizing amms, Apr 2021. `https://medium.com/balancer-protocol/balancer-v2-generalizing-amms-16343c4563ff`.

[Pit] Nipun Pitimanaaree. What is alpha homora v2?

[Wys10] Uwe Wystup. Quanto options. *Encyclopedia of Quantitative Finance*, 2010.

A Borrowing LP shares against other LP shares

A natural question is how the results of §3 generalize to n-asset Balancer pools [AC20]. Instead of extending the previous section to borrowing more than 1 asset against and LP share as collateral, we instead consider borrowing an LP share against another LP share. It will turn out that borrowing n assets against an LP share is a special case of borrowing LP shares against one another. This is a consequence of the linearity of portfolio value.

Suppose that we have an oracle price $p(t) \in \mathbf{R}_+^{N_a}$ where $N_a \in \mathbf{N}$ is the number of assets of interest. Further, suppose we have n CFMMs with Balancer trading functions $\varphi_i : \mathbf{R}^{N_a} \to \mathbf{R}$ with weights $w_i \in \mathbf{R}_+^{N_a}$ and reserves $R_i \in \mathbf{R}_+^{N_a}$. Our goal is to consider loans that borrow φ_i LP shares using φ_j LP shares as collateral. Note that oracle price is the argument in the dual function representation of portfolio value [AC20, §4] and represents either an aggregation of the prices implied by $\{\varphi_i\}$ or the prices quoted in an infinitely liquid external market.

We first define a *generalized collateral factor* $c_{i,j}$ as the maximum number of φ_j LP shares that you can borrow using φ_i LP shares as collateral. This means that given any admissible borrows of $b_i, b_j \in \mathbf{R}^+$ units of LP shares and reserves $R_i(t), R_j(t)$ in the respective trading sets, we have:

$$c_{i,j} \geq \frac{b_j w_j^T (p(t) \odot R_j(t))}{b_i w_i^T (p(t) \odot R_i(t))}$$

where $\odot : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n$ is component-wise multiplication of two vectors,

$$(a \odot b)_i = a_i \times b_i$$

Note that we recover standard collateral factor and/or loan-to-value on Aave or Compound when $w_i = \delta_{i,k}$ for some $k \in [n]$, which is an infeasible weight for Balancer. We can thus view direct overcollateralized borrowing of assets as a limit of borrowing LP shares against LP shares, where the 'weights' of Compound borrowing look like the following

$$w_i(n) = \lim_{n \to \infty} \left(1 - \frac{1}{n}\right) \delta_{i,k} + \frac{1}{n} \delta_{i,l}$$

for $l \in [n], l \neq k$. In a sense, direct asset borrowing is an analytic continuation of CFMM borrowing, which demonstrates that CFMM borrowing is the most general form of lending activity.

Analysis akin to the §3 shows that if we have $\tilde{c}_{i,j}, \tilde{w}_i, \tilde{R}_i$ for a different LP share lending protocol, then

$$c_{i,j} \geq \tilde{c}_{i,j} \iff \frac{b_j w_j^T (p(t) \odot R_j(t))}{b_i w_i^T (p(t) \odot R_i(t))} \geq \frac{\tilde{b}_j \tilde{w}_j^T (p(t) \odot \tilde{R}_j(t))}{\tilde{b}_i \tilde{w}_i^T (p(t) \odot \tilde{R}_i(t))}$$

Note that we implicitly assume no-arbitrage (akin to [AEC20]) because we use the same oracle prices $p(t)$ on both sides of the inequality. Define $v_i(t) = b_i R_i(t) \odot w_i$ (and likewise for $\tilde{v}_i(t)$), which corresponds to the weighted portfolio value of the lien. Using this definition, we can rewrite the previous equation as,

$$c_{ij} \geq \tilde{c}_{ij} \iff \frac{v_i(t)^T p(t)}{v_j(t)^T p(t)} \geq \frac{\tilde{v}_i(t)^T p(t)}{\tilde{v}_j(t)^T p(t)} \iff \left(\left(\frac{\tilde{v}_j(t)^T p(t)}{v_j(t)^T p(t)} \right) v_i(t) - \tilde{v}_i(t) \right)^T p(t) \geq 0$$

Since prices satisfy $p(t) \geq 0$, this is equivalent to

$$\left(\frac{\tilde{v}_j(t)^T p(t)}{v_j(t)^T p(t)} \right) v_i(t) - \tilde{v}_i(t) \geq 0 \iff \left(\frac{\left(\frac{\tilde{v}_j(t)}{v_j(t)} \odot v_j(t) \right)^T p(t)}{v_j(t)^T p(t)} \right) v_i(t) - \tilde{v}_i(t) \geq 0 \tag{12}$$

where division is equivalent to element-wise division. Let $C = \inf_k \frac{\tilde{v}_j(t)_k}{v_j(t)_k}$, so that eq. (12) gives the following sufficient condition for comparing collateral factors:

$$Cv_i(t) \geq \tilde{v}_i(t) \implies c_{ij} \geq \tilde{c}_{ij} \iff Cb_i R_i(t) \odot w_i \geq \tilde{b}_i \tilde{R}_i(t) \odot w_i$$

This is the analogue of the result of §3 which provides conditions for comparing collateral factors of two different lenders. While this result is weaker than the collateral factor equivalence in the two asset scenario of §3, it shows that the worst-case relative portfolio values, C, controls borrow capital efficiency.