The Elliptic Concentrated Liquidity Pool (E-CLP)

Ariah Klages-Mundt Steffen Schuldenzucker

November 28, 2022

Abstract

We lay out a theory of the general design of automated market makers (AMMs) that follow a circle or, more generally, an ellipse curve. Various parameters of the ellipse (eccentricity, rotation, concentrated liquidity price range) can be freely configured, allowing the approach to represent a variety of trading curves. We discuss how these parameters can be chosen in an intuitive way, and we describe how the mechanism can be calibrated to given price bounds, similar to a virtual reserve construction. We describe how to implement standard operations (such as swaps and liquidity updates) in an efficient way.

In this paper, we present the *elliptic concentrated liquidity pool (E-CLP)*, an automated market maker (AMM) where trading happens along an ellipse curve. The E-CLP's advantage over other AMM curves is that it can be configured in a flexible way to shape the distribution of liquidity across the range of prices. Specifically, the following parameters can be chosen freely:

1. Price bounds $[\alpha, \beta]$. The E-CLP implements *concentrated liquidity* where the AMM only provides liquidity within the specified price range. This is important for capital efficiency; an AMM that doesn't implement concentrated liquidity has to hold back capital to provide liquidity at hypothetical prices that may never manifest.
2. Rotation angle $\phi \in [0°, 90°]$, which equivalently determines the *peg price* $\tan(\phi)$. The peg price is the price at which the curvature of the ellipse is lowest and thus price impact is smallest. The peg price would usually be chosen at a "natural" price between the two assets (if this exists), around which most of the trading is expected to take place. For example, for two stablecoins, one would typically choose $\phi = 45°$ so that $\tan(\phi) = 1$. Typically, one would choose the parameters such that $\tan(\phi) \in [\alpha, \beta]$, but this paper does not require this. Note that the peg price does *not* have to be centered within the price range.
3. Stretch factor $\lambda \geq 1$. This parameter controls the distribution of liquidity within the price range $[\alpha, \beta]$: for large λ, most of the liquidity is concentrated around the peg price, with liquidity much reduced towards the ends of the price range (or declining in one direction if $\tan(\phi) \notin [\alpha, \beta]$). Smaller λ distribute liquidity more uniformly.

$\lambda = 1$ implies a trading curve in the shape of a circle section. Geometrically, λ maps 1:1 to the eccentricity of the ellipse.

In an E-CLP, we want our reserve points to move along an ellipse or (in the simpler case) a circle; to be precise, we want to use a section of the *lower, flatter* part of the ellipse, where it is convex as a function of the asset balance x. As a stepping stone, we first discuss a hypothetical *constant-circle market maker (CCMM)* where trading happens along a circle section and only the price range can be configured. We then use our results for the analysis of the more general E-CLP, exploiting the fact that an ellipse is a stretched and rotated circle.

Wang (2020, 2021) previously described an AMM with an elliptic trading curve. However, this version of the AMM is severely limited in its configurability. Specifically, Wang (2020) only discusses an ellipse rotated by 45° and Wang (2021) only discusses ellipses rotated by 0° or 90° (corresponding to peg prices of 0 and ∞, respectively); different stretch factors only accommodate for different relative prices of the assets. No principled discussion is provided in these works and the approach does not appear flexible enough to be adjustable to provide any additional configurability. In contrast, our E-CLP can be configured in a flexible way to model a variety of liquidity profiles.

1 Constant-Circle Market Maker

We begin with the simpler constant-circle market maker (CCMM). A circle can be defined using a midpoint and a radius. However, if the midpoint is fixed, this does not adjust well when adding or removing liquidity. Instead, we construct the circle midpoint based on the current liquidity invariant and given price bounds. This is very similar in spirit to a virtual reserve construction, and many of our proofs work in a similar way; however, we're shifting the circle *upwards* in both dimensions, so that part of the circle that previously lied in the third quadrant is now in the first quadrant; in contrast, virtual reserves shift a curve *downwards* in both directions.

Formally, we are considering the curve

$$(a - x)^2 + (b - y)^2 = r^2 \tag{1}$$

across values $0 \leq x \leq a$ and $0 \leq y \leq b$. Here, r is the (radius of the circle and the) liquidity invariant and (a, b) (is the midpoint of the circle and) takes the role of offsets.

Lemma 1. *The price in a CCMM is*[1]

$$p_x = \frac{x'}{y'},$$

[1]Here $p_x = -\frac{\mathrm{d}y}{\mathrm{d}x}$, where the derivative is taken along the curve specified by (1). We sometimes use an exponent, like p_x^c , to indicate the AMM in question. For details see Klages-Mundt and Schuldenzucker (2021).

where $x' := a - x$ *and* $y' := b - y$.

Proof. Let $c(x, y) = x^2+y^2$. We have $\nabla c(x, y) = (2x, 2y)$ and thus, by the general theory (Klages-Mundt and Schuldenzucker, 2021),[2] $p_x^c(x, y) = \frac{x}{y}$ and this implies $p_x(x, y) = \frac{a-x}{b-y}$ since a and b are constant along the curve (1). □

To calibrate the offsets a and b, given price bounds $0 \leq \alpha < \beta \leq \infty$, we want to choose a and b such that they only depend on r and $p_x(x, y) \in [\alpha, \beta]$ and these bounds are tight.

Lemma 2. *The above conditions are satisfied iff*

$$a = r/\sqrt{1 + 1/\beta^2}$$
$$b = r/\sqrt{1 + \alpha^2}.$$

Furthermore,

$$x = 0 \Leftrightarrow y = y^+ := r \cdot \left(\frac{1}{\sqrt{1 + \alpha^2}} - \frac{1}{\sqrt{1 + \beta^2}} \right)$$
$$y = 0 \Leftrightarrow x = x^+ := r \cdot \left(\frac{1}{\sqrt{1 + 1/\beta^2}} - \frac{1}{\sqrt{1 + 1/\alpha^2}} \right)$$

Proof. Lemma 1 together with (1) implies that

$$(1 + 1/p_x^2)(a - x)^2 = r^2 \tag{2}$$
$$(1 + p_x^2)(b - y)^2 = r^2 \tag{3}$$

Since we need $p_x = \beta$ if $x = 0$, we can use the first equation to receive $(1+1/\beta^2)a^2 = r^2$ and equivalently $a = r/\sqrt{1 + 1/\beta^2}$ as required. Analogously, from the second equation and $p_x = \alpha$ if $y = 0$ we receive $b = r/\sqrt{1 + \alpha^2}$. The formulas for x^+ and y^+ follow from the values for a and b together with (1) after some simple algebraic transformations. □

1.1 Standard Operations for the CCMM

1.1.1 Initialization from real reserves

To initialize a pool from the real reserves alone, we need to solve (1) for r given x and y. Note that this will then also set a price according to Lemma 1.

Proposition 1. *For any* $0 \leq \alpha < \beta$ *and any* $x, y \geq 0$*, there exists a unique* $r \geq 0$ *such that (1) holds when the values for* a *and* b *are chosen like in Lemma 2. Specifically, let*

[2] This follows essentially by application of the implicit function theorem and the chain rule.

$\mu := \frac{1}{\sqrt{1+1/\beta^2}} = \frac{\beta}{\sqrt{1+\beta^2}}$ *and* $\nu := \frac{1}{\sqrt{1+\alpha^2}}$. *Then*

$$r = \frac{\mu x + \nu y + \sqrt{(1-\nu^2)x^2 + (1-\mu^2)y^2 + 2\mu\nu xy}}{\mu^2 + \nu^2 - 1}.$$

Proof. Observe that $a = \mu r$ and $b = \nu r$. Now (1) is equivalent to

$$\begin{aligned}
& r^2 = (\mu r - x)^2 + (\nu r - y)^2 \\
\Leftrightarrow \quad & 0 = (\mu^2 + \nu^2 - 1)r^2 - 2(\mu x + \nu y)r + x^2 + y^2 =: f(r) \\
\Leftrightarrow \quad & r = \frac{\mu x + \nu y \pm \sqrt{(\mu x + \nu y)^2 - (\mu^2 + \nu^2 - 1)(x^2 + y^2)}}{\mu^2 + \nu^2 - 1} \\
& \quad = \frac{\mu x + \nu y \pm \sqrt{(1-\nu^2)x^2 + (1-\mu^2)y^2 + 2\mu\nu xy}}{\mu^2 + \nu^2 - 1}.
\end{aligned}$$

Note that $\mu^2 = \frac{\beta^2}{1+\beta^2} \in (\frac{1}{2}, 1]$ and also $\nu^2 = \frac{1}{1+\alpha^2} \in (\frac{1}{2}, 1]$. This holds even if we allow $\alpha = 0$ and $\beta = \infty$ (and take the necessary precautions). Now this implies $\mu^2 + \nu^2 - 1 > 0$ and $1 - \nu^2, 1 - \mu^2 \geq 0$. Therefore, the two solutions are always well-defined and non-negative.

For a solution r to this equation to be admissible, we additionally need that $x \leq a$ and $y \leq b$, i.e., $r \geq \frac{x}{\mu}, \frac{y}{\nu}$. We show that this is the case exactly for the "+" solution. Towards this, it is enough to show that $f(\hat{r}) \leq 0$ for $\hat{r} = \max(\frac{x}{\mu}, \frac{y}{\nu})$ (because $f(r) \to \infty$ for $r \to \pm\infty$). Assume WLOG that $\frac{x}{\mu} \geq \frac{y}{\nu}$, so that $\hat{r} = \frac{x}{\mu}$. Then

$$\begin{aligned}
f(\hat{r}) &= (\mu^2 + \nu^2 - 1)\frac{x^2}{\mu^2} - 2(\mu x + \nu y)\frac{x}{\mu} + x^2 + y^2 \\
&= x^2 + x^2\frac{\nu^2}{\mu^2} - x^2\frac{1}{\mu^2} - 2x^2 - 2x\frac{\nu}{\mu}y + x^2 + y^2 \\
&= \left(x\frac{\nu}{\mu} - y\right)^2 - x^2\frac{1}{\mu^2}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
& f(\hat{r}) \leq 0 \\
\Leftrightarrow \quad & \left(x\frac{\nu}{\mu} - y\right)^2 \leq x^2\frac{1}{\mu^2} \\
\Leftrightarrow \quad & x\frac{\nu}{\mu} - y \leq x\frac{1}{\mu} \\
\Leftrightarrow \quad & x\frac{\nu - 1}{\mu} \leq y.
\end{aligned}$$

The equivalence on the third line holds since, by assumption, $\frac{x}{\mu} \geq \frac{y}{\nu}$ and thus the parenthesis is non-negative. The inequality on the last line holds because, as discussed above, $0 \leq \mu, \nu \leq 1$, so that the left-hand side is non-positive, and the right-hand side is

non-negative. □

1.1.2 Initialization from price

We can also initialize a pool from a price and the liquidity invariant r.

Lemma 3. *In a CCMM pool with price bounds $[\alpha, \beta]$, price $p_x \in [\alpha, \beta]$, and liquidity invariant r we have*

$$x = r \cdot \left(\frac{1}{\sqrt{1 + 1/\beta^2}} - \frac{1}{\sqrt{1 + 1/p_x^2}} \right)$$
$$y = r \cdot \left(\frac{1}{\sqrt{1 + \alpha^2}} - \frac{1}{\sqrt{1 + p_x^2}} \right)$$

Proof. Like in the proof of Lemma 2 we have

$$r^2 = (1 + 1/p_x^2)(a - x)^2 \qquad = (1 + 1/p_x^2)(r/\sqrt{1 + 1/\beta^2} - x)^2$$
$$r^2 = (1 + p_x^2)(b - y)^2. \qquad = (1 + p_x^2)(r/\sqrt{1 + \alpha^2} - y)^2.$$

The statement now follows by simple algebraic transformation of the respective line. □

The *portfolio value* at any given state of a pool is

$$V := p_x x + y.$$

The following describes the portfolio value as a function of the current price and the invariant. Note that, like many of the measures above, the portfolio value scales linearly in the invariant r. This is convenient and suggests that we have chosen our invariant in a meaningful way..

Proposition 2. *The portfolio value is equal to*

$$V = r \cdot \left[\frac{p_x}{\sqrt{1 + 1/\beta^2}} + \frac{1}{\sqrt{1 + \alpha^2}} - \sqrt{1 + p_x^2} \right].$$

Proof. Follows by plugging the values for x and y from Lemma 3 into the definition of V and simplifying. For the simplification step, note in particular that $\frac{1}{\sqrt{1+1/p_x^2}} = \frac{p_x}{\sqrt{1+p_x^2}}$. □

1.1.3 Liquidity Update

Updating liquidity is straightforward based on our previous results.

Proposition 3. *Consider the CCMM with price bounds $[\alpha, \beta]$ and assume that (x, y, r)*

satisfy (1) at price p_x. Then $(x + \Delta x, y + \Delta y, r + \Delta r)$ satisfy (1) at price p_x iff

$$\Delta x = \Delta r \cdot \left(\frac{1}{\sqrt{1 + 1/\beta^2}} - \frac{1}{\sqrt{1 + 1/p_x^2}} \right)$$
$$\Delta y = \Delta r \cdot \left(\frac{1}{\sqrt{1 + \alpha^2}} - \frac{1}{\sqrt{1 + p_x^2}} \right).$$

Proof. Follows immediately from Lemma 3 applied to the state before and after the liquidity update, respectively. The factors of r are always the same because the price p_x does not change. □

The preceding results imply that the real reserves x, y are linear in the invariant r. When the reserves are known (as they usually are), we can exploit this to receive a much simpler formula for updating liquidity:

Corollary 1. *Consider the CCMM with price bounds $[\alpha, \beta]$ and assume that (x, y, r) satisfy (1) at price p_x. Then $(x + \Delta x, y + \Delta y, r + \Delta r)$ satisfy (1) at price p_x iff*

$$\frac{\Delta x}{x} = \frac{\Delta y}{y} = \frac{\Delta r}{r}.$$

Proof. This follows immediately by combining Proposition 3 with Lemma 3. The factor that only depends on p_x cancels out. □

1.1.4 Trade (Swap) Execution

The following proposition shows how to execute a swap in the CCMM. Trade execution is simple, but requires taking a square root. There does not seem to be any way around that in general.

Proposition 4. *Assume that (x, y, L) satisfy (1). Then $(x + \Delta x, y + \Delta y, L)$ satisfy (1) iff*

$$\Delta y = b - y - \sqrt{r^2 - (a - x - \Delta x)^2}$$

and, equivalently,

$$\Delta x = a - x - \sqrt{r^2 - (b - y - \Delta y)^2}.$$

Such values exist (in such a way that the square root is well-defined and none of the new reserves $x + \Delta x$ and $y + \Delta y$ are negative) iff $\Delta x \in [-x,\ x^+ - x]$ and $\Delta y \in [-y,\ y^+ - y]$, respectively, where x^+ and y^+ are like in Lemma 2.

1.1.5 Implementation

Some procedures use the values $\sqrt{1 + p_x^2}$ and $\sqrt{1 + 1/p_x^2}$. In a CCMM that is already initialized, these values do not have to be computed but can be inferred since, by (2) and

(3) we have

$$\sqrt{1+p_x^2} = \frac{r}{a-x}$$
$$\sqrt{1+1/p_x^2} = \frac{r}{b-x}.$$

This is useful to reduce gas costs when updating liquidity.

Some numerical analysis techniques may be used to understand the accuracy that is required for the square root during trade execution, to limit gas costs.

2 Elliptical Concentrated Liquidity Pool (E-CLP)

We now expand our analysis to the more general case of a constant ellipse. Observe that an ellipse can be obtained by transforming a circle as follows:

- Consider a circle around the origin with radius r.
- Stretch the circle in (say) x direction by a factor $\lambda \geq 1$. This results in a (general) ellipse with the flat side in the y direction. For $\lambda = 1$ we retain the circle and for $\lambda \to \infty$ we receive a degenerate line. λ thus corresponds to the eccentricity of the ellipse.
- Then rotate the resulting ellipse by an angle φ. In the case we are interested in, we will use $\varphi \in (-90°, 0]$, such that the flatter side of the ellipse is facing the main diagonal.
- Then shift the ellipse by a non-negative vector such that the formerly negative flat side of the ellipse faces the origin and we achieve the price bounds $[\alpha, \beta]$ we want.
- Now only consider the part of the ellipse that is oriented towards the origin, just like we did before for the circle. It is easy to see that this corresponds to only considering the 3rd and 4th quadrant of the original circle.

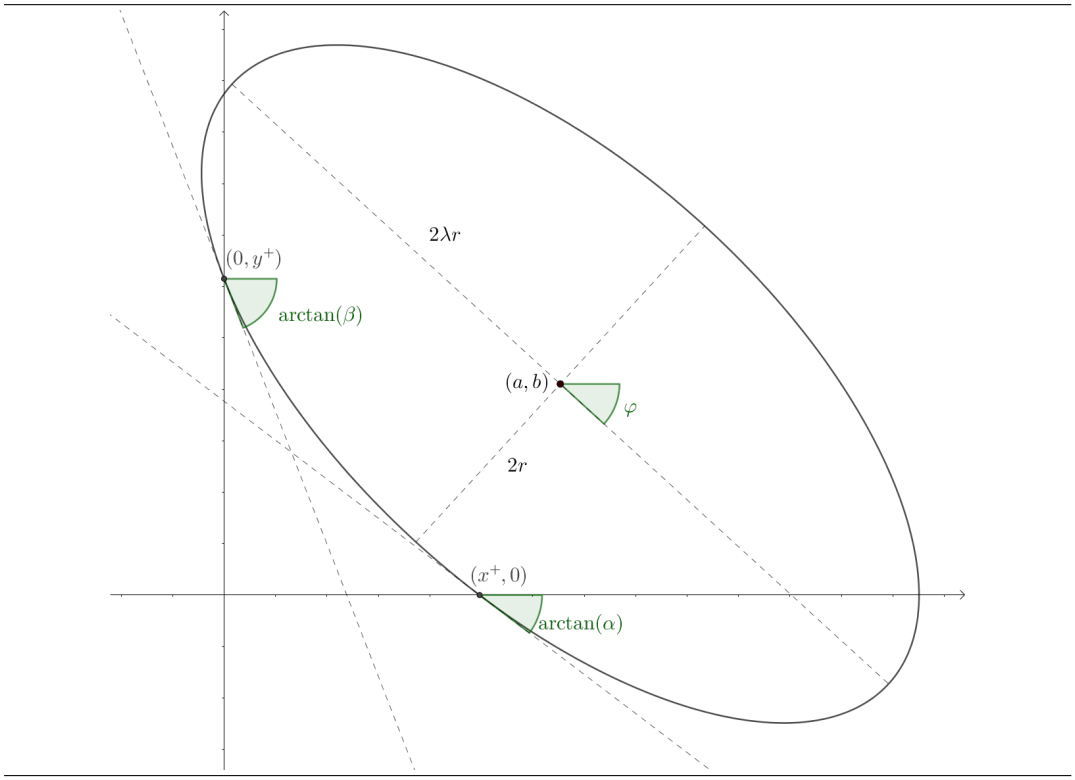
This is a useful way of describing the ellipse because the parameters λ and φ have a natural interpretation. The resulting invariant takes the form

$$(c \circ A \circ v)(x, y) = r^2, \tag{4}$$

where $c(x, y) = x^2 + y^2$, A is a certain linear transformation, and $v(x, y) = (x - a, y - b)$ with offsets a and b that are functions of r to be determined based on the price bounds. We will see later that a and b are linear in r. Regarding the linear transformation A, we need to use $A = \mathrm{Str}(1/\lambda) \cdot \mathrm{Rot}(-\varphi)$, where

$$\mathrm{Str}(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathrm{Rot}(\varphi) = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

Figure 1 Constructed ellipse for certain parameters $\alpha, \beta, \varphi, \lambda$ and a certain invariant level r.



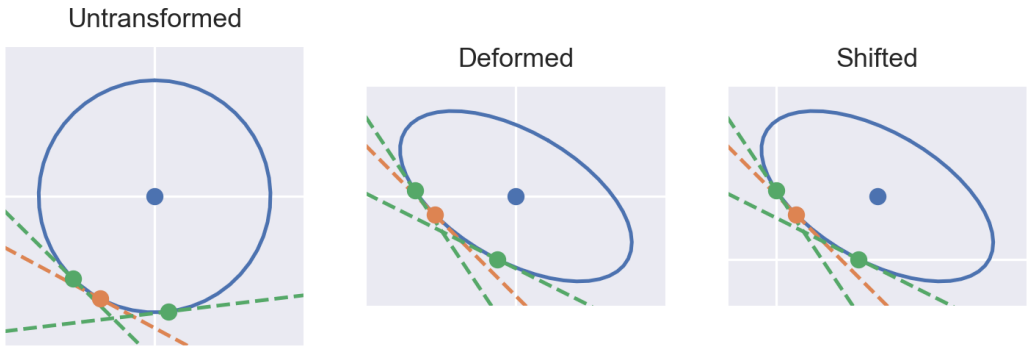
Note that $A^{-1} = \mathrm{Rot}(\varphi) \cdot \mathrm{Str}(\lambda)$ and v shifts a point by a non-positive vector, i.e., downwards and to the left. The aforementioned operations are therefore the inverses of what we want to do to the ellipse. This is because the ellipse should be the *preimage* of the above operation of r^2. More in detail, the original circle around the origin is $c^{-1}(r^2)$ and thus (4) is equivalent to

$$(x, y) \in (v^{-1} \circ A^{-1})(c^{-1}(r^2)) = ((+(a, b)) \circ \mathrm{Rot}(\varphi) \circ \mathrm{Str}(\lambda))(c^{-1}(r^2)),$$

i.e., to the statement that (x, y) lies on the ellipse constructed according to the rules above. Note that, for he offset step and in contrast to the constant-circle construction from Section 1, we use the offsets $(x-a, y-b)$ instead of the transformation $(a-x, b-y)$. This makes it easier to describe our mechanism as we go back and forth between the different levels of the transformation. Finally, note that the transformed values $(A \circ v)(x, y)$ will usually be negative along at least one of the coordinates. This is not problematic.

Figure 1 depicts the final (deformed and shifted) ellipse. The long axis of the ellipse is rotated by the angle φ with respect to the x axis. The shortest diameter of the ellipse is equal to $2r$, i.e., the diameter of the original circle. The longest diameter is $2\lambda r$, so that the ellipse has eccentricity λ. The ellipse is shifted so that its center lies at the offset vector (a, b), and this will be done in such a way that it intersects the x and y axes and that at these points the slopes of the tangents (i.e., the derivatives along the curve) are

Figure 2 The three stages of the transformation: the final (deformed and shifted) ellipse (right), an ellipse that has only been deformed, but not shifted (middle), and the untransformed circle (left). The white lines are the two axes. The blue point is the center of the circle/ellipse. The green points refer to those points where for the final (deformed and shifted) AMM curve, one of the two reserves is at 0. The yellow point is an arbitrarily shown reserve state. The dashed lines are tangents, so that their slopes are negative prices.



$-\alpha$ and $-\beta$, respectively. This means that the angles to the horizontal axis are $\arctan(\alpha)$ and $\arctan(\beta)$, respectively. The intersection points with the two axes are labeled $(x^+, 0)$ and $(0, y^+)$. The part of the ellipse that is oriented towards the origin and connects these two points is the trading curve of the AMM, and the rest of the ellipse is not admissible. Note that it is often, but not necessarily, the case that $a, b > 0$, i.e., the center of the ellipse could lie in another quadrant than the first one. In general, only one of the two coordinates needs to be positive.

2.1 General linearly transformed circle AMMs

To manage complexity of the exposition, we first keep the matrix A abstract and describe the theory of circles transformed by *any* invertible linear transformation A.

In the definition of the E-CLP, we need to consider different levels of transformation: A point $t := (x, y)$ is first shifted to yield a point $v(t)$ and then transformed to a point $Av(t)$. Equivalently, a circle centered at the origin is deformed into an ellipse centered at the origin and then shifted. To keep the notation as clear as possible, we use different variables for points that relate to the different levels: real reserves are labeled $t = (x, y)$; shifted reserves, corresponding to points on an ellipse centered at the origin, are labeled $t' = (x', y')$; shifted and transformed reserves, corresponding to points on a circle centered at the origin, are labeled $t'' = (x'', y'')$. For instance, for any point of real reserves t, we could label $t' := v(t)$ and $t'' := At' = Av(t)$. This is purely a naming convention to better tell the different transformation levels apart. Figure 2 depicts the three stages of the transformation for a given point.

We can consider the transformed AMMs at the different levels by their respective invariant functions. Let $f = c \circ A$ and $g = f \circ v = c \circ A \circ v$. Then for any r, $c^{-1}(r)$ is a

circle, $f^{-1}(r)$ is an ellipse centered at the origin, and $g^{-1}(r)$ is an ellipse shifted towards the first quadrant.

We now consider price vectors at the different transformation levels. Let $p_x^c(t'') = \frac{x''}{y''}$ be the price of asset x under the circle c at the point t'' (see Lemma 1), and define the *price vector* $p^c(t'') := (p_x^c(t''), 1)$. Likewise, let $p^f(t')$ to be the price vector under f at t'. Note that it is *not* in general the case that $p_x^f(t') = p_x^c(At')$! Instead, we receive from the general theory of transformed AMMs (Klages-Mundt and Schuldenzucker, 2021) that

$$p_x^f(t') = \frac{p^c(At') \cdot Ae_x}{p^c(At') \cdot Ae_y}, \tag{5}$$

where $e_x = (1, 0)$ and $e_y = (0, 1)$ are the unit vectors. Note that the two multiplications are dot products of vectors. Regarding the price vector at the lowest transformation level, $p^g(t)$, we know from the general theory that constant offsets do not affect prices (beyond the offset itself), so that $p_x^g(t) = p_x^f(v(t))$.

To compute the offsets a and b as well as perform the standard operations of an AMM, we will employ the following technique: we translate the state of the AMM (given by real reserves t and/or a price $p_x = p_x^g(t)$) into the space of the untransformed circle. Here, the required calculations are comparatively easy. We then translate the result back into the space of the transformed ellipse. This transformation is more complex than simply applying the matrices A and A^{-1}. In the following sub-section, we provide the necessary tooling.

2.1.1 From prices to shifted reserves

Our main tool is a way to compute the transformed point $Av(t)$ given the invariant r and a price p_x (where p_x relates to the transformed ellipse). This can be seen as a variant of Lemma 3 for the ellipse shape. In contrast to the case of the circle, we will already use this theorem to compute appropriate offsets a and b. As a first step, we show how to translate prices between the circle and the ellipse. Equality 5 shows how to convert a price in the circle to a price in the (deformed but not shifted) ellipse. The following definition and proposition show how to do the reverse operation.

Definition 1. Let p_x^f be an arbitrary number, interpreted as a price in the deformed-but-not-shifted ellipse. Then the *untransformed price* corresponding to p_x^f is $\zeta(p_x^f)$ where

$$\begin{aligned} \zeta :&\mathbb{R} \to \mathbb{R} \\ \zeta(p_x^f) :=& -\frac{e_y A(-1, p_x^f)}{e_x A(-1, p_x^f)}. \end{aligned}$$

The following proposition shows that ζ transforms prices from the deformed ellipse back to the untransformed circle.

Proposition 5. *Consider the CFMM corresponding to f and let p_x^f be an arbitrary number. Let t' be some point such that $p_x^f(t') = p_x^f$ and let $t'' := At'$. Then*

$$p^c(t'') \cdot A(-1, p_x^f) = 0$$

and, equivalently,

$$p_x^c(t'') = \zeta(p_x^f). \tag{6}$$

Furthermore,

$$x'' = \zeta(p_x^f) \cdot y''.$$

Note that $e_x A(-1, p_x)$ is simply the x coordinate of the vector $A(-1, p_x)$. Also observe how the first equation has a simple geometric interpretation: the non-transformed price vector $p^c(t'')$ must be orthogonal to the transformed vector of marginal exchange rates $(-1, p_x)$. The first two equations in fact hold when c is *any* CFMM function, while the last one only holds when c is the circle.

Proof. The first statement follows by transformation of (5): We have equivalently

$$\begin{aligned} & p_x^f p^c(t'') \cdot Ae_y = p^c(t'') \cdot Ae_x \\ \Leftrightarrow \quad & p^c(t'') \cdot A(p_x^f e_y - e_x) = 0 \\ \Leftrightarrow \quad & p^c(t'') \cdot A(-1, p_x^f) = 0. \end{aligned}$$

Noting that $p^c(t'') = (p_x^c(t''), 1)$ and solving the resulting linear equation for $p_x^c(t'')$ yields the second equation of the proposition. When c is the circle (i.e., $c(x, y) = x^2 + y^2$), we have $p_x^c(t'') = \frac{x''}{y''}$ (see above). This immediately implies the final statement. □

The next step is a result about the circle, namely how to compute an (untransformed) point t'' on the circle based on the invariant (radius) r and the price p_x^c at that point. The following definition and lemma essentially re-state Lemma 3 while also considering negative segments of the circle. Of particular interest is the part of the circle that lies in the 3rd or 4th quadrant (where $y'' \leq 0$ but x'' is unconstrained). This is because, due to the chosen stretching direction and rotation angle, the part of the ellipse that will ultimately face the origin (and become the trading curve) originates from the part of the circle that lies in the 3rd and 4th quadrant.

Remark 1. When considering the untransformed circle, the notion of a price needs to be understood in a generalized sense where the price of x denoted in units of y is defined as $-\frac{\mathrm{d}y}{\mathrm{d}x}$ and the derivative is taken with respect to the curve where the expression $c(t'')$ remains the same. If this values is positive (i.e., y needs to be reduced if x increases to stay on the curve), then this is the standard notion of a price in an AMM. However, in the 4th quadrant of the circle, this value is negative (i.e., y needs to increase when x is increased to stay on the curve). This maybe unintuitive, but works out without problem

mathematically. For the final (transformed and shifted) AMM, all prices will of course be positive.

Definition 2. Let p_x^c be an arbitrary number, interpreted as a price in the untransformed circle, and let $r > 0$. Then the *normalized corresponding point* for p_x^c is $\eta(p_x^c)$ where

$$\begin{aligned} \eta :&\mathbb{R} \to \mathbb{R}^2 \\ \eta(p_x^c) &= \frac{1}{\sqrt{1+(p_x^c)^2}} \cdot \begin{pmatrix} p_x^c \\ 1 \end{pmatrix}. \end{aligned}$$

Lemma 4. *Let $p_x^c \in (-\infty, \infty)$ be arbitrary and let t'' be such that $p_x^c(t'') = p_x^c$. Let r be such that $c(t'') =: r^2$. Then we have*

$$t'' = \pm r \cdot \eta(p_x^c).$$

If, furthermore, t'' is in the 3rd or 4th quadrant (i.e., $y'' \leq 0$), then

$$t'' = -r \cdot \eta(p_x^c).$$

Proof. We have $\nabla c(x'', y'') = (2x'', 2y'')$ and thus (by the general theory) $p_x^c = \frac{x''}{y''}$. Equivalently, $x'' = p_x^c y''$ and $y'' = 1/p_x^c \cdot x''$. Furthermore, the invariant $x''^2 + y''^2 = r^2$ must hold. By replacing y'' we receive

$$\begin{aligned} & & (1 + 1/(p_x^c)^2)x''^2 &= r^2 \\ \Leftrightarrow & & (1 + (p_x^c)^2)x''^2 &= (p_x^c)^2 r^2 \\ \Leftrightarrow & & x'' &= s_x r \frac{p_x^c}{\sqrt{1+(p_x^c)^2}} \end{aligned}$$

where $s_x \in \{-1, 1\}$. The variable s_x simply makes a "$\pm$" symbol explicit. By replacing x'' we receive

$$\begin{aligned} & & (1 + (p_x^c)^2)y''^2 &= r^2 \\ \Leftrightarrow & & y'' &= s_y r \frac{1}{\sqrt{1+(p_x^c)^2}} \end{aligned}$$

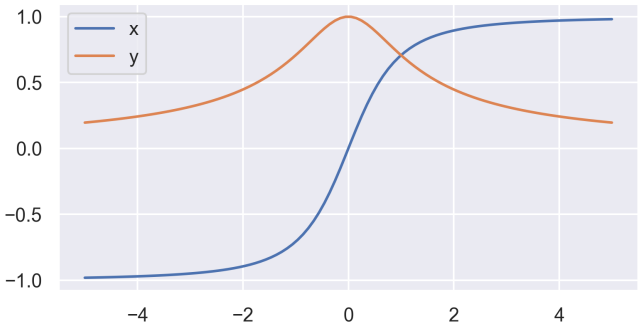
where, again $s_y \in \{-1, 1\}$. The above equations leave the signs s_x and s_y unconstrained. However, we also need

$$p_x^c = \frac{x''}{y''} = \frac{s_x}{s_y} p_x^c$$

and thus $s_x = s_y$, i.e., the two signs must match. This implies the first formula. The last statement if obvious because the y component of $\eta(p_x^c)$ is always non-negative. □

Figure 3 shows the two components of $\eta(p_x^c)$. The x component has a shape somewhat reminiscent of a sigmoid and the y component has a shape somewhat similar to a bell

Figure 3 $\eta(p_x^c)$ from Lemma 4



curve (though of course the two functions are none of those).

We can now connect the previous results to compute the untransformed state t'' from the transformed price p_x^f. From this, we easily also receive the untransformed state (at this point only t' being of interest, we will consider the shifted state t later).

Definition 3. Given a number p_x^f, define the *untransformed normalized corresponding point* as $\tau(p_x^f)$, where

$$\tau : \mathbb{R} \to \mathbb{R}^2$$
$$\tau = \eta \circ \zeta.$$

Proposition 6. *Let p_x^f be an arbitrary number and let t' be such that $p_x^f(t') = p_x^f$. Let r be such that $f(t') = r^2$ and let $t'' = At'$. Assume that $y'' \leq 0$. Then*

$$t'' = -r \cdot \tau(p_x^f).$$

and

$$t' = A^{-1}t'' = -r \cdot A^{-1}\tau(p_x^f).$$

Proof. This follows immediately by plugging the formula for $p_x^c(t'')$ from Proposition 5 into Lemma 4. The last equation follows by definition. □

It is trivial to extend the statement to real reserves, in which case the formula now depends on the offsets a, b:

Corollary 2. *Let p_x^g be an arbitrary number and let t be such that $p_x^g(t) = p_x^g$. Let r be such that $g(t) = r^2$ and let $t'' = Av(t)$. Assume that $y'' \leq 0$. Then*

$$t = (a, b) - r \cdot A^{-1}\tau(p_x^g).$$

Proof. Follows from Proposition 6, noting that $p_x^g(t) = p_x^f(v(t))$ because shifting by a constant does not affect the price (Klages-Mundt and Schuldenzucker, 2021) and $t = t' + (a, b)$ by definition. □

2.1.2 Computing reserve offsets

We are now ready to choose offsets a, b so that our chosen price bounds $[\alpha, \beta]$ are met:

Proposition 7. *Consider the CFMM according to g and price bounds $[\alpha, \beta]$. Let $r > 0$ and let*

$$(a, -y^{+\prime}) := r \cdot A^{-1}\tau(\beta)$$
$$(-x^{+\prime}, b) := r \cdot A^{-1}\tau(\alpha).$$

Let $x^+ := x^{+'} + a$ and $y^+ := y^{+'} + b$. If a and b are chosen in this way, then the range of values $p_x^g(t)$ across all t where $g(t) = r^2$ is $[\alpha, \beta]$, and this is tight. Furthermore,

$$x = 0 \;\Leftrightarrow\; y = y^+$$
$$y = 0 \;\Leftrightarrow\; x = x^+$$

across those $t = (x, y)$ where $g(t) = r^2$.

Proof. By Corollary 2, we have $p_x^g(t) = \beta$ iff $t = (a, b) - r \cdot A^{-1}\tau(\beta)$. We want to choose a, b such that this is case at $t = (0, y^+)$ and thus we receive $(a, b - y^+) = r \cdot A^{-1}\tau(\beta)$. Likewise, we receive $(a - x^+, b) = r \cdot A^{-1}\tau(\alpha)$. □

2.1.3 Initialization from real reserves

We can initialize a pool from real reserves by solving the invariant (4) for r given x and y. This will also set the price. The following proposition and its proof are similar to Proposition 1 about the CCMM; however, we do not receive existence or uniqueness in the general case for *any* invertible matrix A.

Proposition 8. *For any $0 \leq \alpha < \beta$, any invertible matrix A, and any $x, y \geq 0$, there exists an $r \geq 0$ such that, when a and b are chosen according to Proposition 7, then $f(t + (a, b)) = r^2$. Specifically, let $\chi := (e_x A^{-1}\tau(\beta),\, e_y A^{-1}\tau(\alpha))$. Then*

$$r = \frac{At \cdot A\chi \pm \sqrt{(At \cdot A\chi)^2 - \left((A\chi)^2 - 1\right) \cdot (At)^2}}{(A\chi)^2 - 1},$$

where we squares of vectors refer to the scalar product of the vector with itself.

Proof. Observe that $(a, b) = r\chi$ and note further that $c(t'') = x''^2 + y''^2 = t''^2$ in the

notation from above. Thus, the invariant holds iff

$$\begin{aligned} r^2 &= c\,(A(t - r\chi) \\ &= (A(t - r\chi))^2 = (At - rA\chi)^2 \\ &= (At)^2 - 2At \cdot A\chi \cdot r + (A\chi)^2 \cdot r^2 \\ \Leftrightarrow \qquad 0 &= (At)^2 - 2At \cdot A\chi \cdot r + \left((A\chi)^2 - 1\right) \cdot r^2. \end{aligned}$$

By the quadratic formula, this is the case iff

$$r = \frac{At \cdot A\chi \pm \sqrt{(At \cdot A\chi)^2 - \left((A\chi)^2 - 1\right) \cdot (At)^2}}{(A\chi)^2 - 1}.$$

□

2.1.4 Initialization from prices and portfolio value

By combining the previous results, we can initialize a pool from the price and the liquidity invariant. We write short $p_x = p_x^g(t)$.

Proposition 9. *In a CFMM according to g with price bounds $[\alpha, \beta]$ and liquidity invariant r and price p_x, we have $p_x^g(t) = p_x$ and $g(t) = r^2$ iff*

$$t = r \cdot \left[\begin{pmatrix} e_x A^{-1} \tau(\beta) \\ e_y A^{-1} \tau(\alpha) \end{pmatrix} - A^{-1} \tau(p_x) \right].$$

Proof. Follows from Corollary 2 combined with Proposition 7. □

Note how, according to the preceding proposition, the real reserve vector t is linear in the liquidity invariant r. Using the same technique as above, we can also compute the portfolio value, and it will also be linear in r, just like in the constant-circle case. This makes it easy to initialize the E-CLP with a certain portfolio value, too. Recall that the portfolio value is

$$V = p_x x + y$$

Proposition 10. *Consider the CFMM according to g with price bounds $[\alpha, \beta]$. Then for price p_x and liquidity invariant r, if $p_x^g(t) = p_x$ and $g(t) = r^2$, then*

$$V = r \cdot (p_x, 1) \cdot \left[\begin{pmatrix} e_x A^{-1} \tau(\beta) \\ e_y A^{-1} \tau(\alpha) \end{pmatrix} - A^{-1} \tau(p_x) \right].$$

Proof. This immediately follows from Proposition 9 and the fact that $V = (p_x, 1) \cdot t$. □

Remark 2. Note that Proposition 10 only depends on the price p_x, but it does not directly depend on any other state variables of the mechanism. This is why the proposition can

also be used to calculate how the portfolio value of a pool would change *if* the price were to move to some given price. To do this, simply use some assumed price for p_x, rather than a price computed from the pool state. We can also use the proposition to compute r given p_x and V. This is convenient to compare different pool designs (because the portfolio value is a universal measure that can be applied to any AMM whereas r is specific to a given parameter choice for our specific pool).

2.1.5 Liquidity Update

Updating liquidity is straightforward using the same technique as above, too:

Proposition 11. *Consider the CFMM according to $g(t) = r^2$ with price bounds $[\alpha, \beta]$ and let $g(t) =: r^2$ and $p_x^g(t) =: p_x$. Then $g(t + \Delta t) = (r + \Delta r)^2$ and $p_x^g(t + \Delta t) = p_x$ iff*

$$\Delta t = \Delta r \cdot \left[\begin{pmatrix} e_x A^{-1} \tau(\beta) \\ e_y A^{-1} \tau(\alpha) \end{pmatrix} - A^{-1} \tau(p_x) \right].$$

Proof. This follows from Proposition 9. As p_x is meant to stay constant going from (t, r) to $(t + \Delta t, r + \Delta r)$, t is simply a scaling of a certain constant vector by r for the purpose of this proposition. The claim now immediately follows. □

Just like for the constant-circle market maker, if the values of the reserve are known, we receive a much simpler formula via linearity:

Corollary 3. *Consider the CFMM according to $g(t) = r^2$ with price bounds $[\alpha, \beta]$ and let $g(t) =: r^2$ and $p_x^g(t) =: p_x$. Then $g(t + \Delta t) = (r + \Delta r)^2$ and $p_x^g(t + \Delta t) = p_x$ iff*

$$\frac{\Delta x}{x} = \frac{\Delta y}{y} = \frac{\Delta r}{r},$$

where $t = (x, y)$ and $\Delta t = (\Delta x, \Delta y)$.

Proof. Let $\kappa = \begin{pmatrix} e_x A^{-1} \tau(\beta) \\ e_y A^{-1} \tau(\alpha) \end{pmatrix} - A^{-1} \tau(p_x)$. Then by Proposition 9 $t = r\kappa$ and by Proposition 11 $\Delta t = \Delta r \kappa$. Thus,

$$\frac{\Delta x}{x} = \frac{\Delta r e_x \kappa}{r e_x \kappa} = \frac{\Delta r}{r}$$

and likewise for y. □

2.1.6 Computing Prices

Determining the current instantaneous price of the AMM is not trivial, but straightforward using the theory outlined at the beginning of this section:

Proposition 12. *In a CFMM according to g and for a reserve state t, we have*

$$p_x^g(t) = \frac{p^c(t'') \cdot Ae_x}{p^c(t'') \cdot Ae_y}$$

where $$p^c(t'') = \left(\frac{x''}{y''}, 1\right)$$

and $$(x'', y'') = t'' = Av(t)$$

Proof. Follows immediately from the theory outlined at the beginning of this section. □

2.1.7 Implementation

While the operations in the transformed-circle market maker may look slightly more complex compared to other AMM designs (such as the constant-product market maker with virtual reserves), most of the calculations are simple and consist of linear operations and division. Calculation of the values $\tau(p_x)$ in addition requires calculation of the expressions $\sqrt{1 + \zeta(p_x^f)^2}$, where $\zeta(p_x)$ is again easy to compute but the square root implies some computational effort. These terms have to be computed explicitly when initializing the pool at a given price. We also need to compute $\tau(\alpha)$ and $\tau(\beta)$; however, since these values are constant over the execution of the mechanism, this only has to be done once, or these values could be calculated off-chain and only verified by the mechanism upon initialization. The same applies for the matrix inverse A^{-1}. In case of the E-CLP, A^{-1} is even easy to compute analytically.

The value $\sqrt{1 + \zeta(p_x^f)^2}$ is also required when liquidity is to be updated. However, we can leverage the result from Section 1.1.5 to infer this value from the reserve state because (noting that $p_x^f(v(t)) = p_x^g(t)$) and letting $t'' := Av(t)$)

$$\sqrt{1 + \zeta(p_x^g(t))^2} = \sqrt{1 + p_x^c(t'')^2} = \frac{r}{-y''} = -\frac{r}{e_y A(v(t))} \tag{7}$$

by a transformed version of Equation (3).

Remark 3. Our analysis can be conducted for arbitrary functions c and matrices A. Depending on c, the construction of a, b might be more complicated, though. If A is replaced by a nonlinear transformation F in the definition of f, then Ae_x and Ae_y in (5) need to be replaced by the vector derivatives $\frac{\partial F(t')}{\partial x'}$ and $\frac{\partial F(t')}{\partial y'}$, respectively. This would make our analysis significantly more complicated because it introduces a separate dependency on t' in addition to the dependency on $F(t')$. If the transformation A (or F) is not invertible, this may lead to non-unique values for x'' and y'' in Proposition 5, which is likely not desirable.

Remark 4. We are not aware of a general technique to perform *trade execution*, i.e., to solve $f(x', y') = r^2$ for y' (and thus also compute y given x, since the offsets a, b are known) based on the knowledge we have about c. The most promising approach is also

the simplest one: explicitly construct the equation $c(A(x', y')) = r^2$ and solve it for y'. Note that, since A is linear, this will not increase the degree of the equation and thus keep it quadratic. This is what we do below.

2.2 Instantiation for the E-CLP

We now instantiate the general methodology developed above to the E-CLP, where $c(x, y) = x^2 + y^2$ and

$$A = \mathrm{Str}(1/\lambda) \cdot \mathrm{Rot}(-\varphi) = \begin{pmatrix} c/\lambda & -s/\lambda \\ s & c \end{pmatrix},$$

where $c := \cos(-\varphi)$ and $s := \sin(-\varphi)$. Since we assume $\varphi \in (-90°, 0]$, we have $s, c \geq 0$. We furthermore have $\cos(\varphi) = \cos(-\varphi) = c$ and $\sin(\varphi) = -\sin(-\varphi) = -s$ and thus

$$A^{-1} = \mathrm{Rot}(\varphi) \cdot \mathrm{Str}(\lambda) = \begin{pmatrix} c\lambda & s \\ -s\lambda & c \end{pmatrix}.$$

This immediately implies that

$$\zeta(p_x) = \lambda \frac{-s + cp_x}{c + sp_x}.$$

In practice, one will likely want to use s, c themselves as parameters instead of φ, to avoid unnecessary computation of the trigonometric functions on-chain. Clearly, there is a 1:1 correspondence between angles $\varphi \in (-90°, 0]$ and points (s, c) in the first quadrant of the unit circle, i.e, with the set of $s, c \geq 0$ where $s^2 + c^2 = 1$. The parameters can thus easily be verified on-chain.

Note that $\zeta(p_x)$ can be negative because this is a "price" that relates to the original circle centered at the origin. It is easy to see that the points corresponding to the invariant curve (i.e., the part of the transformed ellipse oriented towards the origin) originate from the parts of the untransformed circle that lies in the 3rd and 4th quadrant; in the 4th quadrant, the "prices" $-\frac{\mathrm{d}y}{\mathrm{d}x}$ are negative.

Note also that either of the offsets a, b can be negative (but they cannot both be negative). In this case, the midpoint of the ellipse lies to the left or below the origin. This depends on how the price bounds α, β relate to the parameters φ and λ.

The offsets a, b can be obtained by applying Proposition 7 and we can initialize a pool using Propositions 9 and 10 and perform liquidity updates using Corollary 3.

2.2.1 Initialization from Real Reserves

To initialize a pool from real reserves, we can special-case Proposition 8 as follows.

Proposition 13. *In the notation of Proposition 8, we have*

$$r = \frac{At \cdot A\chi + \sqrt{(At \cdot A\chi)^2 - \left((A\chi)^2 - 1\right) \cdot (At)^2}}{(A\chi)^2 - 1}.$$

Proof Outline. We need to show two statements beyond Proposition 8: that a solution does, in fact, exist, and that only the "$+$" solution is admissible and the "$-$" solution is not. The reason why this is the case is similar to the proof of Proposition 1, but the argument is complicated by the deformations introduced by the matrix A.

The statement can be seen geometrically. Consider the line through the origin and the point t and consider ellipses of successively greater radius r that are otherwise fit to the parameters $\alpha, \beta, \varphi, \lambda$. For any r, the ellipse intersects the line at two points. For sufficiently small r, both of these points lie before (i.e., closer to the origin than) t. For $r \to \infty$, they both go to infinity, and they are continuous in r. This implies existence of an r such that t lies on the ellipse; specifically, there are two r values where this is the case. These are the two solutions in Proposition 8. Note now that for the first (smaller) r where this happens, t intersects the ellipse on its higher (outer) part, which is not part of the actual AMM curve. We therefore need to take the second (larger) r where t lies on the ellipse; here, t lies on the lower (inner) part of the ellipse, which also forms the corresponding AMM curve. □

2.2.2 Trade Execution

To execute a trade, we need to solve the equation $c(A(x', y')) = 0$ for y' given x' (or vice versa). Since A is linear and c is a polynomial of degree 2, this transformed equation is also a polynomial of degree 2 and can be solved by taking a single square root. The following result makes it explicit how to do this. The result is stated in terms of the shifted reserves t'. From this, we easily receive the result in terms of real reserves by shifting by (a, b) via Proposition 7.

Proposition 14. *Assume that $f(t') = r^2$. Let $\underline{\lambda} := 1 - 1/\lambda^2$. Then*

$$y' = \frac{-sc\underline{\lambda}x' - \sqrt{s^2c^2\underline{\lambda}^2x'^2 - (1 - \underline{\lambda}s^2) \cdot [(1 - \underline{\lambda}c^2)x'^2 - r^2]}}{1 - \underline{\lambda}s^2}$$
$$x' = \frac{-sc\underline{\lambda}y' - \sqrt{s^2c^2\underline{\lambda}^2y'^2 - (1 - \underline{\lambda}c^2) \cdot [(1 - \underline{\lambda}s^2)y'^2 - r^2]}}{1 - \underline{\lambda}c^2}.$$

Proof. These formulas follow by solving the invariant

$$(e_x A(x', y'))^2 + (e_y A(x', y'))^2 = r^2, \tag{8}$$

which is equivalent to (4), for y' and x', respectively. More in detail, it follows via the

definition of A from above that (8) is equivalent to

$$\begin{aligned}
& & \left(c/\lambda x' - s/\lambda y'\right)^2 + \left(sx' + cy'\right)^2 &= r^2 \\
\Leftrightarrow & & c^2/\lambda^2 x'^2 + s^2/\lambda^2 y'^2 - 2sc/\lambda^2 x'y' + s^2 x'^2 + c^2 y'^2 + 2scx'y' - r^2 &= 0 \\
\Leftrightarrow & & (s^2/\lambda^2 + c^2)y'^2 + (2sc - 2sc/\lambda^2)x'y' + (c^2/\lambda^2 + s^2)x'^2 - r^2 &= 0 \\
\Leftrightarrow & & (1 - \underline{\lambda} s^2)y'^2 + 2\underline{\lambda} scx'y' + (1 - \underline{\lambda} c^2)x'^2 - r^2 &= 0,
\end{aligned}$$

where, in the last line, we exploited the fact that $s^2 + c^2 = 1$. By the quadratic formula, we now receive

$$\begin{aligned}
y' &= \frac{-sc\underline{\lambda}x' \pm \sqrt{s^2c^2\underline{\lambda}^2x'^2 - (1 - \underline{\lambda}s^2) \cdot [(1 - \underline{\lambda}c^2)x'^2 - r^2]}}{1 - \underline{\lambda}s^2} \\
x' &= \frac{-sc\underline{\lambda}y' \pm \sqrt{s^2c^2\underline{\lambda}^2y'^2 - (1 - \underline{\lambda}c^2) \cdot [(1 - \underline{\lambda}s^2)y'^2 - r^2]}}{1 - \underline{\lambda}c^2}.
\end{aligned}$$

It remains to show that the "$-$" solution is always the unique acceptable one. This is easy to see geometrically; for the sake of concreteness, consider the first case, where we solved for y' as a function of x'. The two solutions of (8) for y' correspond to the two points on the ellipse that have the given x' value. However, the mechanism's trading curve only consists of the "lower half" of the ellipse, which originated from the half-circle below the origin via rotation and stretching. Since we rotated by less than 90 degrees, this is also the half with the lower y' (and x', respectively) values. □

References

Ariah Klages-Mundt and Steffen Schuldenzucker. Prices in higher-dimensional and transformed constant-function market makers. mimeo, 2021.

Yongge Wang. Automated market makers for decentralized finance (defi). 2020. URL `https://arxiv.org/abs/2009.01676`.

Yongge Wang. Implementing automated market makers with constant circle. 2021. URL `https://arxiv.org/abs/2103.03699`.