Rational Distance Sets on Conic Sections

Megan D. Ly  Shawn E. Tsosie  Lyda P. Urresta
Loyola Marymount  UMass Amherst  Union College

July 2010

Abstract

Leonhard Euler noted that there exists an infinite set of rational points on the unit circle such that the pairwise distance of any two is also rational; the same statement is nearly always true for lines and other circles. In 2004, Garikai Campbell considered the question of a rational distance set consisting of four points on a parabola. We introduce new ideas to discuss a rational distance set of four points on a hyperbola. We will also discuss the issues with generalizing to a rational distance set of five points on an arbitrary conic section.

1 Introduction

A rational distance set is a set whose elements are points in $\mathbb{R}^2$ which have pairwise rational distance. Finding these sets is a difficult problem, and the search for rational distance sets with rational coordinates is even more difficult. The search for rational distance sets has a long history. Leonard Euler noted that there exists an infinite set of rational points on the unit circle such that the pairwise distance of any two is also rational.

In 1945 Stanislaw Ulam posed a question about a rational distance set: is there an everywhere dense rational distance set in the plane [2]? Paul Erdős also considered the problem and he conjectured that the only irreducible algebraic curves which have an infinite rational distance set are the line and the circle [4]. This was later proven to be true by Jozsef Solymosi and Frank de Zeeuw [4].

First, we provide the formal definition of a rational distance set:

Definition 1.1. A rational distance set $S$ is a set of elements $P_i = (x_i, y_i) \in \mathbb{R}^2$, $1 \leq i \leq n$, such that for all $P_i, P_j \in S$, $\|P_i - P_j\|$ is a rational number.

We are primarily concerned with finding rational distance sets of rational points. The distance between two points on a graph is $\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$. It will prove useful to rewrite this formula as

$$|x_i - x_j| \sqrt{1 + \left( \frac{y_i - y_j}{x_i - x_j} \right)^2} \quad (1)$$

Now, consider the following lemma:
Lemma 1.2. The rational solutions to the equation

\[ \alpha^2 = 1 + \beta^2 \]  \tag{2} 

can be parameterized by \( \alpha = \frac{m^2 + 1}{2m}, \quad \beta = \frac{m^2 - 1}{2m}, \) for \( m \in \mathbb{Q}, m \neq 0. \)

For the proof, refer to Campbell [1, Lemma 2.1].

2 Main results

2.1 Line

Theorem 2.1. For any line \( L: ax + by + c = 0, \) for \( a, b, c \in \mathbb{Q}, \) there exists a dense rational distance set with rational coordinates if and only if there exists \( m \in \mathbb{Q} \) such that \( a^2 + b^2 = m^2. \)

Proof. Suppose \( L \) has a dense rational distance set with rational coordinates. Then we can express the line \( L \) as \( y = -\frac{a}{b}x - \frac{c}{b}. \) Consider two points on \( L \), \((x_i, y_i)\) and \((x_j, y_j)\). Using Lemma 1.2, we can write the distance between these two points as

\[ |x_i - x_j| \sqrt{1 + \left(\frac{a}{b}\right)^2}. \]  \tag{3} 

The distance is rational only if \( 1 + \frac{a^2}{b^2} = n^2 \) for \( n \in \mathbb{Q}. \) That is, if \( a^2 + b^2 = b^2n^2. \) Hence, we may set \( m = bn. \)

Suppose \( a^2 + b^2 = m^2 \) for \( m \in \mathbb{Q}. \) Then line \( L \) can be written as \( y = -\frac{a}{b}x - \frac{c}{b}. \) The distance between two rational points on \( L \), \((x_i, y_i)\) and \((x_j, y_j)\), is \( |x_i - x_j| \sqrt{1 + \left(\frac{a}{b}\right)^2}. \)

Note that from Lemma 1.2 we can write \( a^2 + b^2 = m^2 \) as \( 1 + \frac{a^2}{b^2} = \frac{m^2}{b^2}. \) Hence, we see \( \sqrt{1 + \frac{a^2}{b^2}} = \frac{m}{b} \), which is rational.

2.2 Circle

To show that there exists a rational distance set of rational points on a circle, we identify the cartesian plane \( \mathbb{R}^2 \) with the complex plane \( \mathbb{C}. \)

Theorem 2.2. Let \( r \in \mathbb{Q} \) with \( r \neq 0 \) and let \( C: \|z - z_0\| = r \) be a circle in the complex plane with \( z_0 = x + iy, \) \( x, y \in \mathbb{Q}. \) Then, there exists a dense rational distance set on \( C \) consisting of rational points.
Sketch of Proof. Consider the vertical line $L$: $\text{Re } z = \frac{1}{2r}$. Let $f: \mathbb{C} \to \mathbb{C}$ be the Möbius transformation defined by

$$f(z) = \frac{(z_0 - r)z - 1}{z}.$$ 

Then $f$ maps the line $L$ into the circle $C$. The following figure shows this for a circle with radius $r < 1$ centered at $z_0$.

A dense rational distance set of rational points on $L$ is given by

$$S = \left\{ z = \frac{1}{2r} \left( 1 + i \left( \frac{s^2 - 1}{2s} \right) \right) \mid s \in \mathbb{Q}, \ s \neq 0 \right\}.$$ 

Notice that Lemma 1.2 implies that each $z \in S$ has rational norm $\|z\|$. The codomain $f(S) = \{ f(z) \mid z \in S \}$ will then be a dense set of points on $C$ with rational coordinates.

Finally notice that $f$ is a translation composed with the map $z \mapsto -1/z$. Then, the rationality of the distance between the points on the codomain follows from the identity

$$\left\| \frac{1}{z} - \frac{1}{w} \right\| = \frac{\|z - w\|}{\|z\| \cdot \|w\|}.$$ 

2.3 Rational Distance Set of Three Points on a Parabola

Consider the parabola $y = ax^2 + bx + c$ where $a, b, c \in \mathbb{Q}$.

We provide a geometric intuition of the problem. An important note for this construction is that while the points are at rational distance, the points themselves do not have to be rational. We present a method for constructing a rational distance set of three points on a parabola. Note that we can find a rational distance set using
(a) Two concentric circles with rational radii are centered at some point on the parabola.

(b) Moving the construction along the parabola, we note that the length of segment $P_2P_3$ changes.

Figure 1: While $P_1P_2$ and $P_1P_3$ are rational, we cannot guarantee that $P_2P_3$ is also rational. Since the length of $P_2P_3$ changes, the segment $P_2P_3$ must have a rational length at some point on the parabola.

this method on any conic section. First, we choose some point on the parabola and construct two circles of rational radii around it, as shown in Figure 1.

In Figure 1, we see that the line segments $P_1P_2$ and $P_1P_3$ are rational. All we require now is that $P_2P_3$ be rational. This segment is not necessarily rational. We can, however, make it rational. If we allow the construction to move along the parabola, we notice that the length of segment $P_2P_3$ changes. We see from this construction that the length of segment $P_2P_3$ is a continuous function on an interval. Therefore, we can find some point in the parabola where the segment $P_2P_3$ is rational.

Now we turn to the more difficult problem of finding rational distance sets of rational points on the parabola. By equation 1, the distance $d_{ij}$ between two rational points $P_i$ and $P_j$ on a parabola is

$$d_{ij} = |x_i - x_j|\sqrt{1 + (ax_i + ax_j + b)^2}.$$ 

By Lemma 1.2, $ax_i + ax_j + b = \frac{m^2-1}{2m_{ij}}$. We let $g(m) = \frac{1}{a}(\frac{m^2-1}{2m} - b)$, which leads us to the following theorem:

**Theorem 2.3.** Given a parabola $y = ax^2 + bx + c$, let $S = \{P_1, P_2, P_3\}$. $S$ is a rational distance set of rational points if and only if $1 \leq i < j \leq 3$ we can find a nonzero
rational value $m_{ij}$ such that

\[
\begin{align*}
x_1 &= \frac{g(m_{12}) + g(m_{13}) - g(m_{23})}{2} \\
x_2 &= \frac{g(m_{12}) - g(m_{13}) + g(m_{23})}{2} \\
x_3 &= \frac{-g(m_{12}) + g(m_{13}) + g(m_{23})}{2}
\end{align*}
\]

Proof. For each $1 \leq i < j \leq 3$ where $x_i + x_j = g(m_{ij})$, we have three equations:

\[
\begin{align*}
x_1 + x_2 &= g(m_{12}) \\
x_1 + x_3 &= g(m_{13}) \\
x_2 + x_3 &= g(m_{23})
\end{align*}
\]

This is equivalent to the following row reduced augmented matrix:

\[
\begin{pmatrix}
1 & 0 & 0 & | & \frac{g(m_{12}) + g(m_{13}) - g(m_{23})}{2} \\
0 & 1 & 0 & | & \frac{g(m_{12}) - g(m_{13}) + g(m_{23})}{2} \\
0 & 0 & 1 & | & \frac{-g(m_{12}) + g(m_{13}) + g(m_{23})}{2}
\end{pmatrix}
\]

which gives us our desired values.

\[\square\]

2.4 Rational Distance Set of Four Points on a Parabola

We can follow a similar argument to find a rational distance set of four rational points on a parabola.

**Theorem 2.4.** Given a parabola $y = ax^2 + bx + c$, let $S = \{P_1, P_2, P_3, P_4\}$. $S$ is a rational distance set of rational points if and only if there are rational values $m_{ij}$, $1 \leq i < j \leq 4$ such that

\[
\begin{align*}
x_1 &= \frac{1}{2}(g(m_{12}) + g(m_{13}) - g(m_{23})) \\
x_2 &= \frac{1}{2}(g(m_{12}) - g(m_{13}) + g(m_{23})) \\
x_3 &= \frac{1}{2}(-g(m_{12}) + g(m_{13}) + g(m_{23})) \\
x_4 &= \frac{1}{2}(-g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{14}))
\end{align*}
\]

and $g(m_{13}) + g(m_{24}) = g(m_{23}) + g(m_{14}) = g(m_{12}) + g(m_{34})$
Proof. For each $1 \leq i < j \leq 4$ where $x_i + x_j = g(m_{ij})$, we have six equations:

\[
\begin{align*}
    x_1 + x_2 &= g(m_{12}) \\
    x_1 + x_3 &= g(m_{13}) \\
    x_1 + x_4 &= g(m_{14}) \\
    x_2 + x_3 &= g(m_{23}) \\
    x_2 + x_4 &= g(m_{24}) \\
    x_3 + x_4 &= g(m_{34})
\end{align*}
\]

This is equivalent to the following row reduced augmented matrix:

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & | & g(m_{12}) + g(m_{13}) - g(m_{23}) \\
0 & 1 & 0 & 0 & | & g(m_{12}) - g(m_{13}) + g(m_{23}) \\
0 & 0 & 1 & 0 & | & -g(m_{12}) + g(m_{13}) + g(m_{23}) \\
0 & 0 & 0 & 1 & | & -g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{14}) \\
0 & 0 & 0 & 0 & | & g(m_{13}) + g(m_{24}) - g(m_{23}) - g(m_{14}) \\
0 & 0 & 0 & 0 & | & g(m_{12}) + g(m_{34}) - g(m_{23}) - g(m_{14})
\end{pmatrix}
\]

which gives us our desired equations. \hfill \Box

We know that any three points lie on a common circle. However, in the case of four points, this does not always occur.

**Definition 2.5.** A set of points is **concyclic** if they lie on a common circle. Similarly, a set of points is **nonconcyclic** if one cannot construct a common circle through them.

We will now examine the cases of concyclic and nonconcyclic points on a parabola.

### 2.5 Concyclic Points on a Parabola

**Proposition 2.6.** Let $P_i = (x_i, ax_i^2 + bx_i + c)$ for $1 \leq i \leq 4$ be four rational points. Then they are concyclic if and only if $x_1 + x_2 + x_3 + x_4 = -\frac{2b}{a}$.

**Proof.** Let $C_{\alpha,\beta,\rho}$ be the circle $(x - \alpha)^2 + (y - \beta)^2 = \rho^2$, where $\alpha, \beta, \rho \in \mathbb{R}$. This circle intersects the parabola $y = ax^2 + bx + c$ at the points whose $x$-coordinates are the roots of

\[
(x - \alpha)^2 + (ax^2 + bx + c - \beta)^2 - \rho^2 = 0
\]

\[
= a^2x^4 + 2abx^3 + (2a(c - \beta) + b^2 + 1)x^2 + 2b(c - \beta)x + (c - \beta)^2 + \alpha^2 - \rho^2
\]

Since the coefficient of $x^3$ is $2ab$, then $-a^2(x_1 + x_2 + x_3 + x_4) = 2ab$. Thus, $x_1 + x_2 + x_3 + x_4 = -\frac{2b}{a}$.

Conversely, if we have $x_i$, $1 \leq i \leq 4$ such that $x_1 + x_2 + x_3 + x_4 = -\frac{2b}{a}$, we can solve:

\[
a^2(x - x_1)(x - x_2)(x - x_3)(x - x_4) =
\]
\[ a^2 x^4 + 2abx^3 + (2a(c - \beta) + b^2 + 1)x^2 + 2b(c - \beta)x + (c - \beta)^2 + \alpha^2 - \rho^2 \]

for some \( \alpha, \beta, \) and \( \rho \).

**Theorem 2.7.** Suppose that \( P_1, P_2, P_3, \) and \( P_4 \) are rational and concyclic points on the parabola \( y = ax^2 + bx + c \). Then, these points are at rational distance if and only if there are nonzero rational values \( m_{12}, m_{13}, \) and \( m_{23} \) such that the equations of Theorem 2.4 hold. If we have this condition, then \( x_4 = -\frac{1}{2}(g(m_{12}) + g(m_{13}) + g(m_{23}) + \frac{4b}{a}) \).

**Proof.** By Proposition 2.6, \( x_4 = -(x_1 + x_2 + x_3 + \frac{2b}{a}) \). Therefore, we can directly solve for \( x_4 \) using the values given for the \( x_1, x_2, x_3 \). Inputting our values, we get \( x_4 = -\frac{1}{2}(g(m_{12}) + g(m_{13}) + g(m_{23}) + \frac{4b}{a}) \). \( \square \)

### 2.6 Non-Concyclic Points on a Parabola

We now explore the more difficult case of finding a rational distance set of four nonconcyclic rational points on the parabola. We therefore need to examine the last condition of Theorem 2.4:

\[ g(m_{13}) + g(m_{24}) = g(m_{23}) + g(m_{14}) = g(m_{12}) + g(m_{34}), \]

in order to find our six \( m_{ij} \) values. Consider the surface \( g(m_{ij}) + g(m_{kl}) = t \) where \( t \) is an arbitrary rational number. We can make the following substitutions:

\[ m_{ij} = \frac{X^2 + X}{Y - TX}, \quad m_{kl} = \frac{X + 1}{Y - TX}, \quad t = \frac{T - 2b}{a}, \]

to obtain the elliptic curve \( E : Y^2 = X^3 + \frac{241}{36}X^2 + X \). Thus if we find rational points on the elliptic curve we can find rational \( m_{ij} \) values that satisfy the last condition.

### 2.7 Examples

In order to illustrate this process, we include the following example:

Given the parabola \( y = x^2 \), let \( T = \frac{13}{6} \) in order to get the following elliptic curve \( E : Y^2 = X^3 + \frac{241}{36}X^2 + X \). We chose \( T = \frac{13}{6} \) because it is a small rational value that gives us an elliptic curve of positive rank.

We get the rational points \( Q_1 = (6: 19: 18), Q_2 = (3: 13: 36), Q_3 = (30: 169: 750) \) on \( E \). Now our \( m_{ij} \) have the following values: \( m_{12} = \frac{3}{10}, m_{13} = \frac{1}{2}, m_{23} = \frac{4}{3}, m_{14} = 4, m_{24} = 6, m_{34} = 15/2 \). Which yields the following rational distance set:

\[ \left\{ \left( \frac{307}{240}, \frac{94249}{57600} \right), \left( \frac{19}{80}, \frac{361}{6400} \right), \left( \frac{127}{240}, \frac{16129}{57600} \right), \left( \frac{757}{240}, \frac{573049}{57600} \right) \right\}. \]

We illustrate this in the following figure:

We now show an example of a rational distance set on the parabola \( y = x^2 + 2x \). If we let \( T = \frac{13}{6} \) then we get the same elliptic curve as in Example 1: \( E : Y^2 = \)
Figure 2: Rational distance set of four points on a parabola $y = x^2$.

We get the rational points $Q_1 = (6 : 19 : 18), Q_2 = (3 : 13 : 36), Q_3 = (30 : 169 : 750)$ on $\mathcal{E}$. Now our $m_{ij}$ have the following values: $m_{12} = 3/10$, $m_{13} = 1/2$, $m_{23} = 4/3$, $m_{14} = 4$, $m_{24} = 6$, $m_{34} = 15/2$.

This gives us different values for $g(m_{ij})$:

$$g(m_{12}) = -\frac{211}{60}, \quad g(m_{13}) = -\frac{11}{4}, \quad g(m_{14}) = -\frac{41}{24},$$

$$g(m_{23}) = -\frac{1}{8}, \quad g(m_{24}) = \frac{11}{12}, \quad g(m_{34}) = \frac{101}{60}.$$ 

These values give us the following rational distance set:

$$\left\{ \left(-\frac{737}{240}, \frac{189409}{57600}\right), \left(-\frac{107}{240}, \frac{39911}{57600}\right), \left(\frac{77}{240}, \frac{42889}{57600}\right), \left(\frac{109}{80}, \frac{29321}{6400}\right) \right\}.$$ 

We can see this in the following figure:

2.8 Rational Distance Set of Five Points on a Parabola

Next, we provide the necessary conditions for a rational distance set of five rational points on a parabola.

**Theorem 2.8.** Given a parabola $y = ax^2 + bx + c$, let $S = \{P_1, P_2, P_3, P_4, P_5\}$. $S$ is a rational distance set of rational points if and only if there are rational values $m_{ij}$,
Figure 3: Rational distance set of four points on a parabola $y = x^2 + 2x$.

$1 \leq i < j \leq 5$ such that

\[
\begin{align*}
  x_1 &= \frac{g(m_{12}) + g(m_{13}) - g(m_{23})}{2} \\
  x_2 &= \frac{g(m_{12}) - g(m_{13}) + g(m_{23})}{2} \\
  x_3 &= \frac{-g(m_{12}) + g(m_{13}) + g(m_{23})}{2} \\
  x_4 &= \frac{-g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{14})}{2} \\
  x_5 &= \frac{-g(m_{12}) - g(m_{13}) + g(m_{23}) + 2g(m_{15})}{2}
\end{align*}
\]

as well as,

\[
\begin{align*}
  g(m_{13}) + g(m_{24}) &= g(m_{14}) + g(m_{23}) \\
  g(m_{13}) + g(m_{25}) &= g(m_{15}) + g(m_{23}) \\
  g(m_{12}) + g(m_{34}) &= g(m_{14}) + g(m_{23}) \\
  g(m_{12}) + g(m_{35}) &= g(m_{15}) + g(m_{23}) \\
  g(m_{12}) + g(m_{13}) + g(m_{45}) &= g(m_{14}) + g(m_{15}) + g(m_{23})
\end{align*}
\]
Proof. For each $1 \leq i < j \leq 5$ where $x_i + x_j = g(m_{ij})$, we have ten equations:

\[
\begin{align*}
x_1 + x_2 &= g(m_{12}) \\
x_1 + x_3 &= g(m_{13}) \\
x_1 + x_4 &= g(m_{14}) \\
x_1 + x_5 &= g(m_{15}) \\
x_2 + x_3 &= g(m_{23}) \\
x_2 + x_4 &= g(m_{24}) \\
x_2 + x_5 &= g(m_{25}) \\
x_3 + x_4 &= g(m_{34}) \\
x_3 + x_5 &= g(m_{35}) \\
x_4 + x_5 &= g(m_{45})
\end{align*}
\]

This is equivalent to the following row reduced augmented matrix:

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \frac{g(m_{12})+g(m_{13})-g(m_{23})}{2} \\
0 & 1 & 0 & 0 & 0 & \frac{g(m_{12})-g(m_{13})+g(m_{23})}{2} \\
0 & 0 & 1 & 0 & 0 & -g(m_{12})+g(m_{13})+g(m_{23}) \\
0 & 0 & 0 & 1 & 0 & -g(m_{12})-g(m_{13})+g(m_{23})+2g(m_{14}) \\
0 & 0 & 0 & 0 & 1 & -g(m_{12})-g(m_{13})-g(m_{23})+2g(m_{15}) \\
0 & 0 & 0 & 0 & 0 & g(m_{13})-g(m_{14})-g(m_{23})+g(m_{24}) \\
0 & 0 & 0 & 0 & 0 & g(m_{13})-g(m_{15})-g(m_{23})+g(m_{25}) \\
0 & 0 & 0 & 0 & 0 & g(m_{12})-g(m_{14})-g(m_{23})+g(m_{34}) \\
0 & 0 & 0 & 0 & 0 & g(m_{12})-g(m_{15})-g(m_{23})+g(m_{35}) \\
0 & 0 & 0 & 0 & 0 & g(m_{12})+g(m_{13})-g(m_{14})-g(m_{15})-g(m_{23})+g(m_{45})
\end{pmatrix}
\]

which gives us our desired equations. \qed

### 2.9 Rational Distance Sets of Three Points on a Hyperbola

At this point, we would like to examine a rational distance set of three rational points on a hyperbola.

**Theorem 2.9.** Let $a, b, c, d \in \mathbb{Q}$ such that $a(ad-bc) \neq 0$. Then there exists a rational distance set of three rational points, $S = \{P_1, P_2, P_3\}$ on the hyperbola $axy + bx + cy + d = 0$.

**Proof.** The proof proceeds in several parts. First, we rewrite the distance formula as in Equation 1. So, $\frac{y_i - y_j}{x_i - x_j}$ can be parameterized as $\frac{y_i - y_j}{x_i - x_j} = m_{ij}^2 - \frac{1}{2m_{ij}}$.

Then, we solve for $y$ in our hyperbola equation to get the expression: $y = -\frac{bx + d}{ax + c}$. Substituting $y$ into our modified distance formula yields

\[
\frac{2(ad-bc)}{(ax_i + c)(ax_j + c)} = 2 \frac{y_i - y_j}{x_i - x_j} = \frac{m_{ij}^2 - 1}{m_{ij}}.
\]
Define $D = 2(ad - bc)$ and let $\frac{m^2 - 1}{m} = Dn^2$. Making the substitutions $m = \frac{X}{D}$ and $n = \frac{Y}{DX}$ gives us the elliptic curve $E(D)$: $Y^2 = X^3 - D^2X$. Note that we can also obtain the expression $\frac{m^2 - 1}{m} = Dn^2$ from $E(D)$ with the substitutions $X = Dm$ and $Y = D^2mn$.

Letting $Q_i = (X_i: Y_i: 1)$ be rational points on $E(D)$, we define the following rational points:

$$n_{23} = \frac{Y_1}{DX_1}, \quad n_{13} = \frac{Y_2}{DX_2}, \quad n_{12} = \frac{Y_3}{DX_3}$$

in order to allow the following relation to hold:

$$D = \frac{(ax_i + c)(ax_j + c)}{(ax_i + c)(ax_j + c)} = Dn_{ij}^2 = \frac{m_{ij}^2 - 1}{m_{ij}}.$$

We can now define an explicit formula for a rational distance set of three rational points on a hyperbola:

$$P_1 = \left(\frac{n_{23}}{an_{12}n_{13}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{12}n_{13}}{n_{23}}\right)$$

$$P_2 = \left(\frac{n_{13}}{an_{12}n_{23}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{12}n_{23}}{n_{13}}\right)$$

$$P_3 = \left(\frac{n_{12}}{an_{13}n_{23}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{13}n_{23}}{n_{12}}\right)$$

2.10 Example

In order to illustrate this process, we include the following example:

Given the hyperbola $2xy + x + y + 2 = 0$, we get the following elliptic curve $E(6)$: $Y^2 = X^3 - 36X$.

From this curve, we get the rational points $Q_1 = (-3: 9: 1), Q_2 = (50: -35: 8), Q_3 = (-58719: -321057: 50653)$. Now our $n_{ij}$ have the following values: $n_{23} = -1/2, n_{13} = -7/60, n_{12} = 1551/1709$. This yields the following rational distance set:

$$\left\{\left(\frac{40203}{21714}, \frac{27877}{3040}\right), \left(\frac{-8654}{23265}, \frac{-37876}{5957}\right), \left(\frac{87103}{11914}, \frac{-36977}{62040}\right)\right\}.$$  

We show this in the following figure:

2.11 Rational Distance Set of Four Points on a Hyperbola

The system of equations we derive to find a rational distance set of four rational points on a hyperbola will be overdetermined, as in the four point parabola case. In order to handle the extra constraints, we must consider a new result. Before launching into the proposition, however, we should first state some relevant definitions:
Figure 4: The hyperbola $2xy + x + y + 2 = 0$ with a rational distance set of rational points.

**Definition 2.10.** Let $X,Y,Z$ be groups and $f : X \to Z$ and $g : Y \to Z$ be two homomorphisms. Then the fibered of $f$ and $g$ is the subgroup $X \times Y$ consisting of all pairs $(X,Y), x \in X, y \in Y$ such that $f(X) = g(Y)[3]$.

**Definition 2.11.** Given two curves $E : f(x,y) = 0$ and $D : g(u,v) = 0$ a map $\phi : E \to D$ is called a rational map if there exist polynomials $r(x,y), s(x,y), t(x,y)$ such that $u = r(x,y) t(x,y)$ and $v = s(x,y) t(x,y)$.

Moreover, we say that $E$ and $D$ are birationally equivalent if there exist two rational maps $\phi : E \to D$ and $\psi : D \to E$ such that the following two conditions hold:

a. $\psi \circ \phi = id_E$, that is the composition of $\psi$ and $\phi$ is the identity on $E$.

b. $\phi \circ \psi = id_D$, that is the composition of $\phi$ and $\psi$ is the identity on $D$.

With these definitions in hand, we introduce the following proposition:

**Proposition 2.12.** Fix a rational number $T$, and consider the curve

$$E_T = \left\{ (X_i, Y_i, X_j, Y_j) \in \mathbb{A}^4 \middle| \begin{array}{l} Y_i^2 = X_i^3 - D^2 X_i \\ Y_j^2 = X_j^3 - D^2 X_j \text{ and } 2D \frac{X_i X_j}{Y_i Y_j} = T \end{array} \right\} \quad (4)$$

a. The curve $E_T \simeq \pi^{-1}(\{T\})$ is a fiber over the product $E^{(D)} \times \pi E^{(D)}$ associated to the morphism $\pi : E^{(D)} \times E^{(D)} \to \mathbb{P}^1$, which sends

$$((X_i : Y_i : 1), (X_j : Y_j : 1)) \mapsto 2D \frac{X_i X_j}{Y_i Y_j}.$$

b. Additionally, $E_T$ is birationally equivalent to the curve

$$E'_T : y^4 = x(x + D^2)(x + D^2 T^4)(x - D^2 T^2)(x + D^2 T^2)^2.$$
Proof. Part (a) is clear from the definition of a fiber product. For part (b), we consider a point \((x, y)\) on the curve, and define

\[
X_i = -\frac{1}{T^2} \frac{y^2}{(x + D^2)(x + D^2T^2)(x - D^2T^2)}
\]
\[
Y_i = -\frac{1}{T^3} \frac{y}{x + D^2}
\]
\[
X_j = D \frac{2Dy^2 - (x - D^2T^2)(x + D^2T^2)(x^2 + 2D^2x + D^4T^4)}{(x - D^2T^2)^2(x + D^2T^2)^2}
\]
\[
Y_j = 2D^2 \frac{2Dy^2 - (x - D^2T^2)(x + D^2T^2)(x^2 + 2D^2x + D^4T^4)}{(x - D^2T^2)^3(x + D^2T^2)^3}
\]

From the substitutions, we see that this point is on \(E_T\). Conversely, we consider a point \((X_i, Y_i, X_j, Y_j)\) on \(E_T\), and define

\[
x = -4D^3 \frac{X_i^3X_j^3(X_j - D)}{Y_i^2Y_j^4}
\]
\[
y = 8D^5 \frac{X_i^3X_j^3(4D^3X_i^3X_j^3 - 8D^2X_i^3X_j^4 + 4DX_i^3X_j^5 - Y_i^2Y_j^4)}{Y_i^2Y_j^4}
\]

Again, from the substitutions we see that this point is on the curve \(E_T\). \(\square\)

We are now ready to examine a method for finding a rational distance set of four rational points on a hyperbola.

**Theorem 2.13.** Let \(a, b, c, d \in \mathbb{Q}\) such that \(a(ad - bc) \neq 0\). There exists a rational distance set of four rational points on the hyperbola \(axy + bx + cy + d = 0\) if and only if we can find three rational points on the curve

\[
E_T : y^4 = x(x + D^2)(x + D^2T^2)^2(x - D^2T^2)^2(x + D^2T^2)^2.
\]

**Proof.** This proof is similar to that of a rational distance set of three rational points on a hyperbola. First, we express the distance formula as in Equation 1. So, \(\frac{y_i - y_j}{x_i - x_j}\) can be parameterized as \(\frac{y_i - y_j}{x_i - x_j} = \frac{m_{ij}^2 - 1}{2m_{ij}}\).

Then, we solve for \(y\) in our hyperbola equation to get \(y = -\frac{bx + d}{ax + c}\). Substituting \(y\) into our modified distance formula yields

\[
\frac{2(ad - bc)}{(ax_i + c)(ax_j + c)} = \frac{2y_i - y_j}{x_i - x_j} = \frac{m_{ij}^2 - 1}{m_{ij}}.
\]

Define \(D = 2(ad - bc)\) and let \(\frac{m_{ij}^2 - 1}{m_{ij}} = Dn^2\). Making the substutions \(m = \frac{X}{D}\) and \(n = \frac{Y}{DX}\) gives us the elliptic curve \(E(D) : Y^2 = X^3 - D^2X\). Note that we can also obtain the expression \(\frac{m_{ij}^2 - 1}{m_{ij}} = Dn^2\) from \(E(D)\) with the substitutions \(X = Dm\) and \(Y = D^2mn\).

13
Letting $Q_i = (X_i: Y_i: 1)$ be rational points on $E^{(D)}$, we define the rational values

\[ n_{13} = \frac{Y_1}{DX_1}, \quad n_{24} = \frac{Y_2}{DX_2}, \quad n_{23} = \frac{Y_3}{DX_3}, \quad n_{14} = \frac{Y_4}{DX_4}, \quad n_{12} = \frac{Y_5}{DX_5}, \quad n_{34} = \frac{Y_6}{DX_6}, \]

such that the following relation holds:

\[ \frac{D}{(ax_i + c)(ax_j + c)} = \frac{Dn_{ij}^2}{m_{ij}} = \frac{m_{ij}^2 - 1}{m_{ij}}. \]

Therefore, the four rational points in the rational distance set must be in the form:

\[ P_1 = \left( \frac{n_{23}}{an_{12}n_{13}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{12}n_{13}}{n_{23}} \right) \]
\[ P_2 = \left( \frac{n_{13}}{an_{12}n_{23}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{12}n_{23}}{n_{13}} \right) \]
\[ P_3 = \left( \frac{n_{12}}{an_{13}n_{23}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{13}n_{23}}{n_{12}} \right) \]
\[ P_4 = \left( \frac{n_{23}}{an_{24}n_{34}} - \frac{c}{a}, -\frac{b}{a} - \frac{D}{2a} \frac{n_{24}n_{34}}{n_{23}} \right) \]

Additionally, we have the constraint $n_{13}n_{24} = n_{23}n_{14} = n_{12}n_{34}$. In order to satisfy this constraint, we want to find six rational points on $E^{(D)}$ satisfying the relation:

\[ \frac{Y_1}{DX_1} \frac{Y_2}{DX_2} = \frac{Y_3}{DX_3} \frac{Y_4}{DX_4} = \frac{Y_5}{DX_5} \frac{Y_6}{DX_6}. \]

To solve any pair of such equations, we look for rational points on $E_T$, defined in Equation 4. Recall Proposition 2.12, which states that $E_T$ is birationally equivalent to the curve

\[ E_T': y^4 = x(x + D^2)(x + D^2 T^4)(x - D^2 T^2)^2(x + D^2 T^2)^2. \]

Thus in order to find a six rational points on $E^{(D)}$, it suffices to find a set of three rational points on the curve $E_T'$. \hfill \Box

One way to find rational points on the curve $E_T'$ is to consider the superelliptic curve

\[ E_T: w^4 = 2D^2 z(z^2 + T^4)(z^2 + 2z + T^4)(z^2 + 2T^4 z + T^4). \]

**Definition 2.14.** A superelliptic curve is a curve of the form $w^n = f(z)$, where $f(z)$ is a polynomial with no repeated roots and the exponent $n$ is relatively prime to the degree of $f(z)$.

Let $(z_p : w_p : 1)$ and $(z_q : w_q : 1)$ be two rational points on the superelliptic curve. Upon defining the rational numbers
\[ n_{ij} = \frac{Y_{ij}}{DX_{ij}} = \frac{1}{T} \frac{z_p^2 - T^4}{w_p} \quad n_{ik} = \frac{Y_{ik}}{DX_{ik}} = \frac{1}{T} \frac{z_p^2 - T^4}{w_p} \]
\[ n_{kl} = \frac{Y_{kl}}{DX_{kl}} = \frac{2}{D} \frac{w_p}{z_p^2 - T^4} \quad n_{jl} = \frac{Y_{jl}}{DX_{jl}} = \frac{2}{D} \frac{w_p}{z_p^2 - T^4} \]

we have the relation
\[ n_{ij} n_{kl} = \frac{Y_{ij} Y_{kl}}{DX_{ij} DX_{kl}} = \frac{2}{D} \frac{Y_{ik} Y_{jl}}{DX_{ik} DX_{jl}} = n_{ik} n_{jl}. \]

Finally, we want to show that finding three rational points on \( E_T \) corresponds to finding at least three rational points on \( E_T' \).

**Proof.** Using the morphism \( \phi : E_T \to E_T' \) defined by
\[
(z : w : 1) \mapsto (2D^2(T^4 + z^2)z : D^3(T^4 - z^2)w : 4z^2)
\]
along with the substitutions above, we have that \( (X_{ij}, Y_{ij}, X_{kl}, Y_{kl}) \), where
\[
X_{ij} = \frac{1}{2T^2} \frac{w^2}{z(z^2 + 2z + T^4)} \\
Y_{ij} = \frac{D}{2T^3} \frac{w(z^2 - T^4)}{z(z^2 + 2z + T^4)} \\
X_{kl} = \frac{2w^2 - D(z^4 + 4z^3 + 6T^4z^2 + 4T^4z + T^8)}{(z^2 - T^4)^2} \\
Y_{kl} = \frac{2w^2 - D(z^4 + 4z^3 + 6T^4z^2 + 4T^4z + T^8)}{(z^2 - T^4)^3}
\]
is a rational point on \( E_T \). The rest follows. \( \square \)

This result asserts that one way to find three rational points on \( E_T' \) is to find three rational points on \( E_T \). There is a simple way of finding all rational points \( R = (z : w : 1) \) on \( E_T \). A theorem by Gerd Faltings states that if the genus of a curve is greater than one then \( E_T(\mathbb{Q}) \) is a finite set for any fixed rational \( T \) where \( T \neq -1, 0, 1 \). Our curve has a genus of nine. Hence one can use software such as SAGE to find all of them.

## 3 Acknowledgments

This work was conducted during the 2010 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP), a program supported by the National Science Foundation (grant No. DMS-0754872) and the National Security Agency (grant No. H98230-10-1-0233). We also thank Dr. Edray Goins, Dr. Luis Lomelí, Dr. Duane Cooper, Katie Ansaldi, Ebony Harvey, and the MSRI staff.
References

[1] Campbell, Garikai. “‘Points on $y = x^2$ at Rational Distance’”. Mathematics of Computation.

