Planar functions and commutative semifields: A status report and beyond

Robert Coulter

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716 USA
coulter@udel.edu

June 2019

Disclaimer

Disclaimer

This talk is a Claude-free zone.

Disclaimer

This talk is a Claude-free zone.

At least, it is in the sense that his name doesn't appear.

Disclaimer

This talk is a Claude-free zone.

At least, it is in the sense that his name doesn't appear.

Except in this slide.

Disclaimer

This talk is a Claude-free zone.

At least, it is in the sense that his name doesn't appear.

Except in this slide.

That said, he has been a model researcher and an inspiration to me from my first timid steps into research as an undergraduate.

Disclaimer

This talk is a Claude-free zone.

At least, it is in the sense that his name doesn't appear.

Except in this slide.

That said, he has been a model researcher and an inspiration to me from my first timid steps into research as an undergraduate.

Claude – thank you.

Key definitions we'd better worry about, part I

Throughout, $q = p^e$ for some odd prime p.

Definition

A polynomial $L \in \mathbb{F}_q[X]$ is called linearised if

$$L(X) = \sum_i a_i X^{p^i}.$$

Such polynomials represent all linear transformations of $\mathbb{F}_q$, where we are viewing $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$.

Equivalently, they represent all group homomorphisms on $(\mathbb{F}_{p^e}, +)$.
In particular, they satisfy $L(x + y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$.

Key definitions we'd better worry about, part II

Definition

A polynomial $f \in \mathbb{F}_q[X]$ is a Dembowski-Ostrom (DO) polynomial if

$$f(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}.$$

These polynomials are closely related to quadratic and bilinear forms, but that wasn't the original reason we studied them.

Key definitions we'd better worry about, part II

Definition

A polynomial $f \in \mathbb{F}_q[X]$ is a Dembowski-Ostrom (DO) polynomial if

$$f(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}.$$

These polynomials are closely related to quadratic and bilinear forms, but that wasn't the original reason we studied them.

Definition

We say $f(X)$ is a permutation polynomial (PP) over $\mathbb{F}_q$ if $f(\mathbb{F}_q) = \mathbb{F}_q$ i.e. f induces a bijection of $\mathbb{F}_q$ under evaluation.

These are wildly popular as a research topic.

A preemptive key definition

For any $f \in \mathbb{F}_q[X]$, we define a "multiplication" $\star$ on $\mathbb{F}_q$ by

$$x \star y = f(x+y) - f(x) - f(y).$$

Notes:

- The multiplication is necessarily commutative.
- In odd characteristic, you have a left and right distributive law with $+$ and $\star$ if and only if f is a DO polynomial.

The key definition

Definition (Dembowski & Ostrom, 1968 – to construct planes)

We say $f \in \mathbb{F}_q[X]$ is planar over $\mathbb{F}_q$ if $X \star a$ is a PP over $\mathbb{F}_q$ for all $a \in \mathbb{F}_q^\star$.

The key definition

Definition (Dembowski & Ostrom, 1968 – to construct planes)

We say $f \in \mathbb{F}_q[X]$ is planar over $\mathbb{F}_q$ if $X \star a$ is a PP over $\mathbb{F}_q$ for all $a \in \mathbb{F}_q^\star$.

Note: adding a constant or a linearised polynomial to $f(X)$ does not change its planarity. For simplicity, it is assumed that there are no constant or linearised terms involved.

Note: composing $f(X)$ with a linearised PP, inside or out, does not change its planarity.

Although planar functions were originally defined in a more general setting, all known examples can be represented by polynomials over finite fields.

Existence

Easy.

Existence

Easy. (Don't get used to it.)

Existence

The monomial $f(X) = X^2$ is planar over $\mathbb{F}_q$ if and only if q is odd.

Existence

The monomial $f(X) = X^2$ is planar over $\mathbb{F}_q$ if and only if q is odd.

For any $a \in \mathbb{F}_q^\star$, we have $X \star a = 2aX$.

If q is odd, then this is a linear polynomial, which is always a PP.

If q is even, then we are in characteristic 2 and so this is the zero map.

Note: The above argument is dependent only on the characteristic; finiteness is not necessary.

Equivalence

Definition

Let f, h be two planar functions over $\mathbb{F}_q$. Then f, h are equivalent if there exists linearised PPs $L, M \in \mathbb{F}_q[X]$ satisfying

$$L(f(X)) \equiv h(M(X)) \bmod (X^q - X).$$

Equivalence

Definition

Let f, h be two planar functions over $\mathbb{F}_q$. Then f, h are equivalent if there exists linearised PPs $L, M \in \mathbb{F}_q[X]$ satisfying

$$L(f(X)) \equiv h(M(X)) \bmod (X^q - X).$$

Yes, this is EA-equivalence.

Equivalence

Definition

Let f, h be two planar functions over $\mathbb{F}_q$. Then f, h are equivalent if there exists linearised PPs $L, M \in \mathbb{F}_q[X]$ satisfying

$$L(f(X)) \equiv h(M(X)) \bmod (X^q - X).$$

Yes, this is EA-equivalence.

CCZ equivalence reduces to EA-equivalence for planar functions Budaghyan & Helleseth (2011).

Equivalence

Definition

Let f, h be two planar functions over $\mathbb{F}_q$. Then f, h are equivalent if there exists linearised PPs $L, M \in \mathbb{F}_q[X]$ satisfying

$$L(f(X)) \equiv h(M(X)) \bmod (X^q - X).$$

Yes, this is EA-equivalence.

CCZ equivalence reduces to EA-equivalence for planar functions Budaghyan & Helleseth (2011). Ooh, I fibbed!

Equivalence

Definition

Let f, h be two planar functions over $\mathbb{F}_q$. Then f, h are equivalent if there exists linearised PPs $L, M \in \mathbb{F}_q[X]$ satisfying

$$L(f(X)) \equiv h(M(X)) \bmod (X^q - X).$$

Yes, this is EA-equivalence.

CCZ equivalence reduces to EA-equivalence for planar functions Budaghyan & Helleseth (2011).

Equivalent planar functions define isomorphic planes. The converse isn't quite as nice...

Classification results

Classification results

Definitively not easy.

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).
- Restricting to monomials X^n only:
  - Over $\mathbb{F}_p$, by Johnson (1987).

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).
- Restricting to monomials X^n only:
  - Over $\mathbb{F}_p$, by Johnson (1987).
  - Over $\mathbb{F}_{p^2}$, by Coulter (2006).
  - Over $\mathbb{F}_{p^4}$, by Coulter & Lazebnik (2012).

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).
- Restricting to monomials X^n only:
  - Over $\mathbb{F}_p$, by Johnson (1987).
  - Over $\mathbb{F}_{p^2}$, by Coulter (2006).
  - Over $\mathbb{F}_{p^4}$, by Coulter & Lazebnik (2012).
  - Over $\mathbb{F}_q$, provided $q > (n-1)^4$ and $p \nmid n$, by Zieve (2013).
    (This is the exceptionality situation.)

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).
- Restricting to monomials X^n only:
  - Over $\mathbb{F}_p$, by Johnson (1987).
  - Over $\mathbb{F}_{p^2}$, by Coulter (2006).
  - Over $\mathbb{F}_{p^4}$, by Coulter & Lazebnik (2012).
  - Over $\mathbb{F}_q$, provided $q > (n-1)^4$ and $p \nmid n$, by Zieve (2013).
    (This is the exceptionality situation.)

No further classification results.

Classification results

- Prime fields – f is planar if and only if $\deg(f) = 2$.
  Established in 3 different ways, and more or less simultaneously, by Rónyai & Szőnyi (1989); Hiramine (1989); and Gluck (1990).
- Restricting to monomials X^n only:
  - Over $\mathbb{F}_p$, by Johnson (1987).
  - Over $\mathbb{F}_{p^2}$, by Coulter (2006).
  - Over $\mathbb{F}_{p^4}$, by Coulter & Lazebnik (2012).
  - Over $\mathbb{F}_q$, provided $q > (n-1)^4$ and $p \nmid n$, by Zieve (2013).
    (This is the exceptionality situation.)

No further classification results. Sort of...

Conjecture

The Dembowski-Ostrom Conjecture (1968, you can guess who.)
If the reduced polynomial $f \in \mathbb{F}_{p^e}[X]$ is planar, then f is a DO polynomial (ignoring constant and linearised terms).

Conjecture

The Dembowski-Ostrom Conjecture (1968, you can guess who.)
If the reduced polynomial $f \in \mathbb{F}_{p^e}[X]$ is planar, then f is a DO polynomial (ignoring constant and linearised terms).

- Established for prime fields.
- False in characteristic 3, the smallest counterexample occurs in $\mathbb{F}_{81}$.
- Open for characteristic at least 5.

Constructions

Known examples.

Constructions

Known examples. There aren't many!

Constructions

Known examples.

- $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd. Dembowski & Ostrom (1968); Coulter & Matthews (1997).
- $X^{(p^\alpha+1)/2}$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $(\alpha, 2e) = 1$. Coulter & Matthews (1997) – this is the class of counterexamples.

Constructions

Known examples.

- $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd.
  Dembowski & Ostrom (1968); Coulter & Matthews (1997).
- $X^{(p^\alpha+1)/2}$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $(\alpha, 2e) = 1$.
  Coulter & Matthews (1997) – this is the class of counterexamples.
- $X^{10} \pm X^6 - X^2$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and e is 2 or odd.
  Coulter & Matthews (1997); Ding & Yuan (2006).

Constructions

Known examples.

- $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd.
  Dembowski & Ostrom (1968); Coulter & Matthews (1997).
- $X^{(p^\alpha+1)/2}$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $(\alpha, 2e) = 1$.
  Coulter & Matthews (1997) – this is the class of counterexamples.
- $X^{10} \pm X^6 - X^2$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and e is 2 or odd.
  Coulter & Matthews (1997); Ding & Yuan (2006).
- A complex looking DO class, details omitted for brevity.
  Budaghyan & Helleseth (2008).

Constructions

Known examples.

- $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd.
  Dembowski & Ostrom (1968); Coulter & Matthews (1997).
- $X^{(p^\alpha+1)/2}$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $(\alpha, 2e) = 1$.
  Coulter & Matthews (1997) – this is the class of counterexamples.
- $X^{10} \pm X^6 - X^2$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and e is 2 or odd.
  Coulter & Matthews (1997); Ding & Yuan (2006).
- A complex looking DO class, details omitted for brevity.
  Budaghyan & Helleseth (2008).

There are quite a number of additional classes known, but all are equivalent to the above.

Constructions

Known examples.

- $X^{p^\alpha+1}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd.
  Dembowski & Ostrom (1968); Coulter & Matthews (1997).
- $X^{(p^\alpha+1)/2}$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and $(\alpha, 2e) = 1$.
  Coulter & Matthews (1997) – this is the class of counterexamples.
- $X^{10} \pm X^6 - X^2$ is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and e is 2 or odd.
  Coulter & Matthews (1997); Ding & Yuan (2006).
- A complex looking DO class, details omitted for brevity.
  Budaghyan & Helleseth (2008).

There are quite a number of additional classes known, but all are equivalent to the above. (I think! We all know how difficult the equivalence issue can be.)

Off on an algebraic tangent

Definition

A finite semifield $\mathcal{R}$ is a finite algebraic system which has all of the standard properties of a finite field except, perhaps, associativity and commutativity of multiplication.

If we do not insist upon the existence of unity, then we talk of a presemifield.

Off on an algebraic tangent

Definition

A finite semifield $\mathcal{R}$ is a finite algebraic system which has all of the standard properties of a finite field except, perhaps, associativity and commutativity of multiplication.

If we do not insist upon the existence of unity, then we talk of a presemifield.

- It is easy to construct commutative presemifields which are not semifields – take any non-prime finite field $\mathbb{F}_q$ and any non-trivial automorphism σ of $\mathbb{F}_q$. Then the elements of $\mathbb{F}_q$, along with field addition and the multiplication $\star$ defined by $x \star y = (xy)^\sigma$ form a presemifield that does not have unity.
- There is a standard method to transform a presemifield into an equivalent semifield which will preserve commutativity if you have it. Consequently, in terms of discussing equivalence issues, you can talk of presemifields and semifields interchangeably (and presemifields are often easier to deal with in an algebraic sense).

Nice fact

The additive structure of a semifield $\mathcal{R}$ is necessarily elementary abelian.

That means the elements of $\mathcal{R}$ can be associated with the elements of a finite field $\mathbb{F}_q$ of the appropriate order.

Under this association, the multiplication $\star$ or $\mathcal{R}$ can be viewed as a bivariate function over $\mathbb{F}_q$, and since we have left and right distributive laws in $\mathcal{R}$, $\star$ must look like

$$x \star y = \sum_{i,j} a_{ij} x^{p^i} y^{p^j}.$$

The Nuclei

Consider the following three subsets of a semifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$:

$$\mathcal{N}_l(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_m(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_r(\mathcal{R}) = \{\alpha \in \mathcal{R} \ : \ (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathcal{R}\}.$$

These are known as the left, middle and right nucleus, respectively.

We also define the nucleus by $\mathcal{N} = \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r$

It is easy to show all of these sets are finite fields.

Any semifield can be viewed as a vector space over its nucleus.

Bilinear/quadratic form idea

When we have a commutative semifield, we can define a polynomial $f \in \mathbb{F}_q[X]$ by $f(X) = \frac{1}{2}(X \star X)$.

Then, using a well-known idea, one can recover $\star$ from f via

$$x \star y = f(x+y) - f(x) - f(y).$$

This is the same "function-defined" multiplication from before, but now we have no zero divisors.

Bilinear/quadratic form idea

When we have a commutative semifield, we can define a polynomial $f \in \mathbb{F}_q[X]$ by $f(X) = \frac{1}{2}(X \star X)$.

Then, using a well-known idea, one can recover $\star$ from f via

$$x \star y = f(x+y) - f(x) - f(y).$$

This is the same "function-defined" multiplication from before, but now we have no zero divisors.

This implies f is a planar DO polynomial.

Key connection

Theorem (Coulter & Henderson, 2008)

- If $f \in \mathbb{F}_q[X]$ is a planar DO polynomial, then $\langle \mathbb{F}_q, +, \star \rangle$ is a commutative presemifield, where

$$x \star y = f(x+y) - f(x) - f(y).$$

- If $\langle \mathbb{F}_q, +, \star \rangle$ is a commutative presemifield, then $f(X) = \frac{1}{2}(X \star X)$ is a planar DO polynomial.

Key connection

Theorem (Coulter & Henderson, 2008)

- If $f \in \mathbb{F}_q[X]$ is a planar DO polynomial, then $\langle \mathbb{F}_q, +, \star \rangle$ is a commutative presemifield, where

$$x \star y = f(x+y) - f(x) - f(y).$$

- If $\langle \mathbb{F}_q, +, \star \rangle$ is a commutative presemifield, then $f(X) = \frac{1}{2}(X \star X)$ is a planar DO polynomial.

So we have an equivalence between commutative semifields of odd order and planar DO polynomials, which means results on commutative semifields have a direct implication to planar DOs.

Some constructions first

I'll list only those predating the planar DO connection, or originally discovered without the use of them.

The connection has meant basically all recently discovered commutative semifields (inequivalent or not) have been established via the planar DOs.

They fall into two types – constructions of dimension 2 over the middle nucleus, and Albert's twisted fields.

Some constructions first

Albert's twisted fields (Albert, 1952).

Let $q = p^e$ be odd with $e \geq 3$. Fix α so that $e/\gcd(\alpha, e)$ is odd, and let θ be the field automorphism $\theta(x) = x^{p^\alpha}$.

Then field addition and the multiplication $\star$ defined by

$$x \star y = xy^\theta + x^\theta y$$

together define a commutative presemifield.

Some constructions first

For the remaining ones, we have a standard format:
Let $\{1, \lambda\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and k a non-square in $\mathbb{F}_q$.

Some constructions first

For the remaining ones, we have a standard format:
Let $\{1, \lambda\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and k a non-square in $\mathbb{F}_q$.

- Dickson (1906)
  For θ a non-trivial automorphism of $\mathbb{F}_q$, define the multiplication by

$$(a + \lambda b) \star (c + \lambda d) = ac + k(bd)^{\theta} + \lambda(ad + bc).$$

Some constructions first

For the remaining ones, we have a standard format:
Let $\{1, \lambda\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and k a non-square in $\mathbb{F}_q$.

- Dickson (1906)
  For θ a non-trivial automorphism of $\mathbb{F}_q$, define the multiplication by
  $$(a + \lambda b) \star (c + \lambda d) = ac + k(bd)^\theta + \lambda(ad + bc).$$
- Cohen & Ganley (1982)
  For $p = 3$ and $e \geq 3$, define the multiplication by
  $$(a + \lambda b) \star (c + \lambda d) = ac + kbd - k^3(bd)^9 + \lambda(ad + bc + k(bd)^3).$$

Some constructions first

For the remaining ones, we have a standard format:
Let $\{1, \lambda\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and k a non-square in $\mathbb{F}_q$.

- Dickson (1906)
  For θ a non-trivial automorphism of $\mathbb{F}_q$, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac + k(bd)^\theta + \lambda(ad+bc).$$
- Cohen & Ganley (1982)
  For $p = 3$ and $e \geq 3$, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac + kbd - k^3(bd)^9 + \lambda(ad+bc+k(bd)^3).$$
- Ganley (1982)
  For $p = 3$ and $e \geq 3$ odd, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac - b^9 d - bd^9 + \lambda(ad+bc+(bd)^3).$$

Some constructions first

For the remaining ones, we have a standard format:
Let $\{1, \lambda\}$ be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and k a non-square in $\mathbb{F}_q$.

- Dickson (1906)
  For θ a non-trivial automorphism of $\mathbb{F}_q$, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac + k(bd)^\theta + \lambda(ad+bc).$$
- Cohen & Ganley (1982)
  For $p=3$ and $e \geq 3$, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac + kbd - k^3(bd)^9 + \lambda(ad+bc+k(bd)^3).$$
- Ganley (1982)
  For $p=3$ and $e \geq 3$ odd, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac - b^9 d - bd^9 + \lambda(ad+bc+(bd)^3).$$
- Penttila & Williams (2000), sporadic of order 3^{10}
  For $p=3$ and $e=10$, define the multiplication by
  $$(a+\lambda b)\star(c+\lambda d) = ac + (bd)^9 + \lambda(ad+bc+(bd)^{27}).$$

Planar DOs from the known commutative semifields

Albert's twisted fields actually correspond to the planar monomial $X^{p^\alpha+1}$, so we know a planar DO that describes each of these.

This wasn't true for the rest until Kosick and I developed a simple method for determining a planar DO that will construct each of these, so simple that the paper was rejected. (Some forms have come up since in other works, but they were all in her thesis – basically it's not that interesting.)

Planar DOs from the known commutative semifields

Albert's twisted fields actually correspond to the planar monomial $X^{p^\alpha+1}$, so we know a planar DO that describes each of these.

This wasn't true for the rest until Kosick and I developed a simple method for determining a planar DO that will construct each of these, so simple that the paper was rejected. (Some forms have come up since in other works, but they were all in her thesis – basically it's not that interesting.)

NOTE: that doesn't mean that we know **all** of the planar DOs that describe these classes... That is interesting, and therein lies a problem.

Equivalence – Isotopism

Let $\mathcal{R}_1 = \langle \mathbb{F}_q, +, \star \rangle$ and $\mathcal{R}_2 = \langle \mathbb{F}_q, +, * \rangle$ be two presemifields.

Then $\mathcal{R}_1$ and $\mathcal{R}_2$ are isotopic if and only if there exists three linearised PPs $L, M, N \in \mathbb{F}_q[X]$ such that

$$\forall x, y \in \mathbb{F}_q \ : \ M(x) \star N(y) = L(x * y).$$

We say that the triple (M, N, L) is an isotopism between $\mathcal{R}_1$ and $\mathcal{R}_2$. If $M = N$, then this is called a strong isotopism.

Isotopism and isomorphism

Theorem (Albert, 1960)
Two presemifields coordinatise isomorphic planes if and only if they are isotopic.

For commutative presemifields and planar DO polynomials, EA-equivalence of the DO polynomials corresponds exactly to the strong isotopism situation.

So isotopism of commutative presemifields is something more general than EA-equivalence.

Isotopism and isomorphism

Theorem (Albert, 1960)
Two presemifields coordinatise isomorphic planes if and only if they are isotopic.

For commutative presemifields and planar DO polynomials, EA-equivalence of the DO polynomials corresponds exactly to the strong isotopism situation.

So isotopism of commutative presemifields is something more general than EA-equivalence. This is why I said earlier that equivalence and isomorphism don't play nicely. One way works – equivalence implies isomorphism – but the other doesn't.

Classification results for commutative semifields

Classification results for commutative semifields

- A commutative semifield of order p is necessarily a finite field.
- A commutative semifield of order p^2 is necessarily a finite field. (Knuth, 1965; probably earlier)

Classification results for commutative semifields

- A commutative semifield of order p is necessarily a finite field.
- A commutative semifield of order p^2 is necessarily a finite field.
  (Knuth, 1965; probably earlier)
- A commutative semifield of dimension 3 over its nucleus is either isotopic to a finite field or Albert's twisted field.
  In particular, a commutative semifield of order p^3 is necessarily a finite field or Albert's twisted field.
  (Menichetti, 1977)

Classification results for commutative semifields

- A commutative semifield of order p is necessarily a finite field.
- A commutative semifield of order p^2 is necessarily a finite field. (Knuth, 1965; probably earlier)
- A commutative semifield of dimension 3 over its nucleus is either isotopic to a finite field or Albert's twisted field.
  In particular, a commutative semifield of order p^3 is necessarily a finite field or Albert's twisted field.
  (Menichetti, 1977)

We can deal with these types completely!

Finite fields and Albert's twisted fields

Theorem (Coulter & Henderson, 2008)
Any planar DO polynomial that represents a finite field or one of Albert's twisted fields of order q is precisely of the form

$$L(M(X)^{p^\alpha+1}) \bmod (X^q - X),$$

where L, M are linearised PPs, and $e/\gcd(\alpha, e)$ is odd.

The case where $\alpha \equiv 0 \bmod e$ corresponds to the finite field, while all other choices of α correspond to a twisted field example.

More classification results for commutative semifields

More classification results for commutative semifields

- If n is prime and q is large enough with respect to n, then any commutative semifield of order q^n with nucleus of order q is isotopic to either a finite field or one of Albert's twisted fields.
  (Menichetti, 1996)

More classification results for commutative semifields

- If n is prime and q is large enough with respect to n, then any commutative semifield of order q^n with nucleus of order q is isotopic to either a finite field or one of Albert's twisted fields.
  (Menichetti, 1996)
- If a commutative semifield is dimension 2 over its middle nucleus and dimension 4 over its nucleus, then it must be a finite field or a Dickson semifield.
  (Cardinali, Polverino & Trombetti, 2006; though predated by. . .)

More classification results for commutative semifields

- If n is prime and q is large enough with respect to n, then any commutative semifield of order q^n with nucleus of order q is isotopic to either a finite field or one of Albert's twisted fields.
  (Menichetti, 1996)
- If a commutative semifield is dimension 2 over its middle nucleus and dimension 4 over its nucleus, then it must be a finite field or a Dickson semifield.
  (Cardinali, Polverino & Trombetti, 2006; though predated by...)
- If a commutative semifield is dimension 2 over its middle nucleus and dimension $2n$ over its nucleus, and $q \geq 4n^2 - 8n + 2$, then it must be a finite field or a Dickson semifield.
  (Blokhuis, Lavrauw & Ball, 2003)

More classification results for commutative semifields

- If n is prime and q is large enough with respect to n, then any commutative semifield of order q^n with nucleus of order q is isotopic to either a finite field or one of Albert's twisted fields.
  (Menichetti, 1996)
- If a commutative semifield is dimension 2 over its middle nucleus and dimension 4 over its nucleus, then it must be a finite field or a Dickson semifield.
  (Cardinali, Polverino & Trombetti, 2006; though predated by...)
- If a commutative semifield is dimension 2 over its middle nucleus and dimension $2n$ over its nucleus, and $q \geq 4n^2 - 8n + 2$, then it must be a finite field or a Dickson semifield.
  (Blokhuis, Lavrauw & Ball, 2003)

Unlike the field and twisted field case, we do not have a good characterisation of all planar DOs that represent a Dickson semifield.

An awkward truth

Theorem (Coulter & Henderson, 2008)
Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields of characteristic p. Suppose the order of the middle nuclei and nuclei of corresponding commutative semifields is p^m and p^n, respectively. One of the following statements must hold.

1. m/n is odd and $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.
2. m/n is even and either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between any two corresponding commutative semifields $\mathcal{R}_1'$ and $\mathcal{R}_2'$ are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1')$.

An awkward truth

Theorem (Coulter & Henderson, 2008)
Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields of characteristic p. Suppose the order of the middle nuclei and nuclei of corresponding commutative semifields is p^m and p^n, respectively. One of the following statements must hold.

1. m/n is odd and $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.
2. m/n is even and either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between any two corresponding commutative semifields $\mathcal{R}_1'$ and $\mathcal{R}_2'$ are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1')$.

The Dickson semifields fall into that second category.

An awkward truth

Theorem (Coulter & Henderson, 2008)
Let $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields of characteristic p. Suppose the order of the middle nuclei and nuclei of corresponding commutative semifields is p^m and p^n, respectively. One of the following statements must hold.

1. m/n is odd and $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic.
2. m/n is even and either $\mathcal{R}_1$ and $\mathcal{R}_2$ are strongly isotopic or the only isotopisms between any two corresponding commutative semifields $\mathcal{R}_1'$ and $\mathcal{R}_2'$ are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $\mathcal{N}_m(\mathcal{R}_1')$.

The Dickson semifields fall into that second category.
This is what I call the strong isotopy problem, and it's the stumbling block in our understanding of isotopy classes for commutative semifields.

The strong isotopy problem

We have an interesting phenomenon occurring.

Some commutative semifield isotopy classes split into two strong isotopy classes.

Some do not.

The strong isotopy problem

We have an interesting phenomenon occurring.

Some commutative semifield isotopy classes split into two strong isotopy classes.

Some do not.

We don't actually know for most known candidate classes.

The strong isotopy problem

We have an interesting phenomenon occurring.

Some commutative semifield isotopy classes split into two strong isotopy classes.

Some do not.

We don't actually know for most known candidate classes.

Problem
Determine why some isotopy classes split into two strong isotopy classes, while others do not. Geometric? Algebraic? Doesn't matter. A test for when it happens would be great.

Is isotopic shifting the key?

There is a promising recent idea...

An isotopic shift of a polynomial f is a polynomial F satisfying

$$F(X) = f(X + L(X)) - f(X) - f(L(X)),$$

where L is a linearised polynomial.

These were recently used to construct new APN functions, and have been shown to be able to jump equivalence classes for planar functions.

My Ph.D. student, Emily Bergman, and I are hoping to find a way of predicting if and when an isotopic shift switches strong isotopy classes within the same isotopy class.

Is isotopic shifting the key?

There is a promising recent idea...

An isotopic shift of a polynomial f is a polynomial F satisfying

$$F(X) = f(X + L(X)) - f(X) - f(L(X)),$$

where L is a linearised polynomial.

These were recently used to construct new APN functions, and have been shown to be able to jump equivalence classes for planar functions.

My Ph.D. student, Emily Bergman, and I are hoping to find a way of predicting if and when an isotopic shift switches strong isotopy classes within the same isotopy class.

I have another direction in mind also... but it needs some explaining!

Off on a geometric tangent

An incidence structure is nothing more than a set of points V and a set L of non-empty subsets of V called lines. We'll deal exclusively with the finite setting here.

Definition

An incidence structure $\mathcal{P}$ is a projective plane if

- Every two points lie on a unique line.
- Every two lines intersect at a unique point or not at all.
- There are at least 4 points, no three of which are collinear.

These axioms force $\mathcal{P}$ to have the same number of points on every line and the same number of lines through every point.
We define the *order* of $\mathcal{P}$ to be n, where $n+1$ is this forced number.

To obtain an affine plane from a projective plane, delete any line and all the points on it.

The classical example

Choose a field $\mathbb{F}_q$. To construct the Desarguesian plane of order q, we first proceed to construct an affine plane...

The points are the elements of $\mathbb{F}_q \times \mathbb{F}_q$, the lines are the symbols $[m, k]$ and $[m]$, with $m, k \in \mathbb{F}_q$, defined by

$$[m, k] = \{(x, mx + k) : x \in \mathbb{F}_q\} \qquad \text{(the lines of slope } m\text{)},$$
$$[m] = \{(m, y) : y \in \mathbb{F}_q\} \qquad \text{(the vertical lines)}.$$

To complete the projective plane, we add one point (m) to each line of slope m, and (∞) to each of the vertical lines.
Finally, we create the line $[\infty]$ consisting of all of these added points.

The classical example

Choose a field $\mathbb{F}_q$. To construct the Desarguesian plane of order q, we first proceed to construct an affine plane...

The points are the elements of $\mathbb{F}_q \times \mathbb{F}_q$, the lines are the symbols $[m, k]$ and $[m]$, with $m, k \in \mathbb{F}_q$, defined by

$$[m, k] = \{(x, mx + k) : x \in \mathbb{F}_q\} \qquad \text{(the lines of slope } m\text{)},$$
$$[m] = \{(m, y) : y \in \mathbb{F}_q\} \qquad \text{(the vertical lines)}.$$

To complete the projective plane, we add one point (m) to each line of slope m, and (∞) to each of the vertical lines.
Finally, we create the line $[\infty]$ consisting of all of these added points.
Note how the field operations are effectively equivalent to the plane – they define the non-vertical lines.

Hall's coordinatisation method

We've understood since at least early in the 20th century, that the field can be replaced with certain other algebraic structures, such as a semifield, and the construction will still produce a projective plane.

However, it wasn't until Hall introduced the coordinatisation method (in the 1940s) that algebraic techniques could be used to study arbitrary planes.

The coordinatisation method – the labelling set

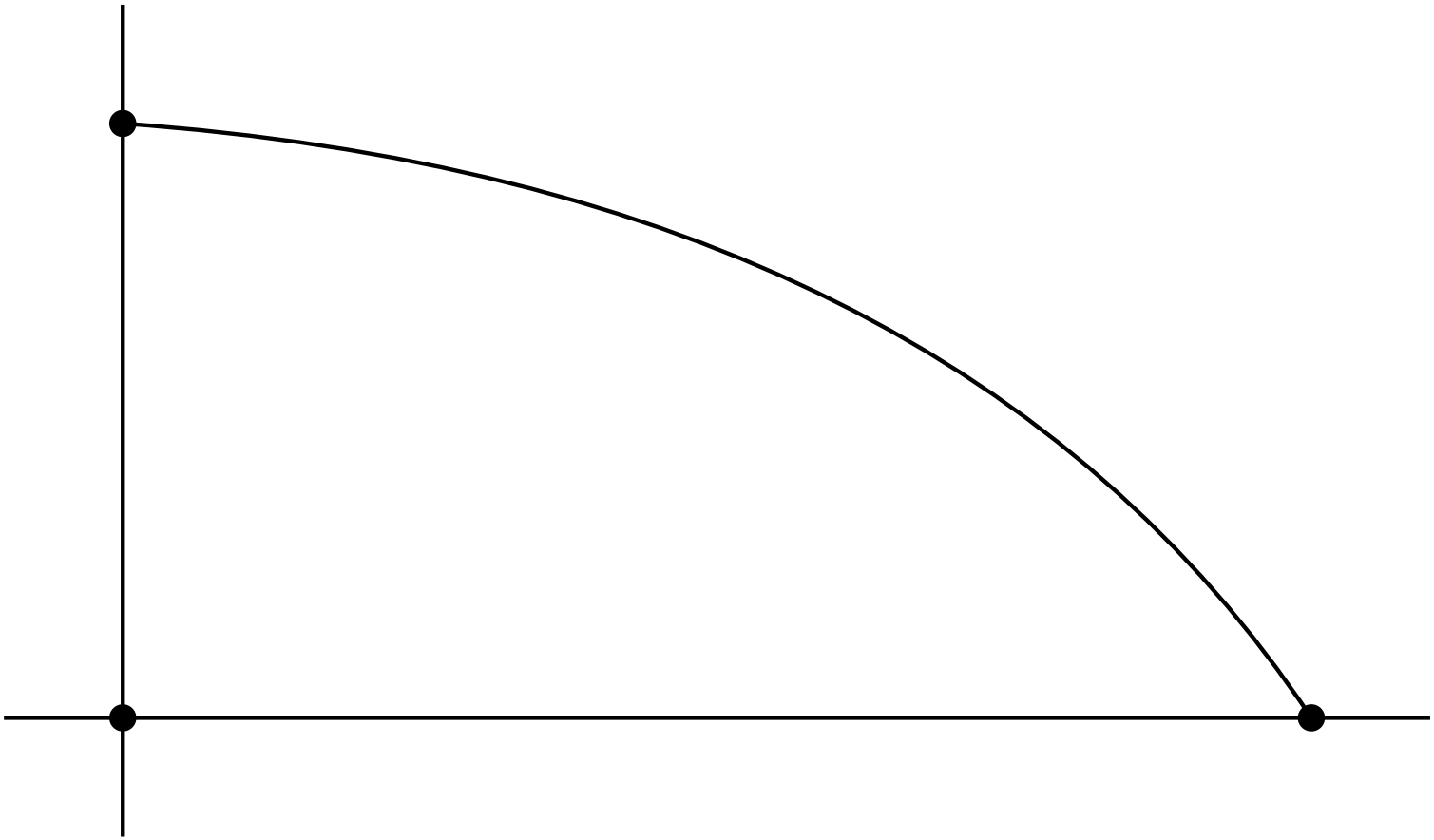
Let $\mathcal{P}$ be a projective plane of order n. To introduce a coordinate system on $\mathcal{P}$ we proceed as follows.

First, select any set $\mathcal{R}$ of cardinality n – this set and the symbol ∞ will be all that is required to produce the coordinate system on $\mathcal{P}$.

We designate two special elements of $\mathcal{R}$ by 0 and 1 for reasons which will become clear.

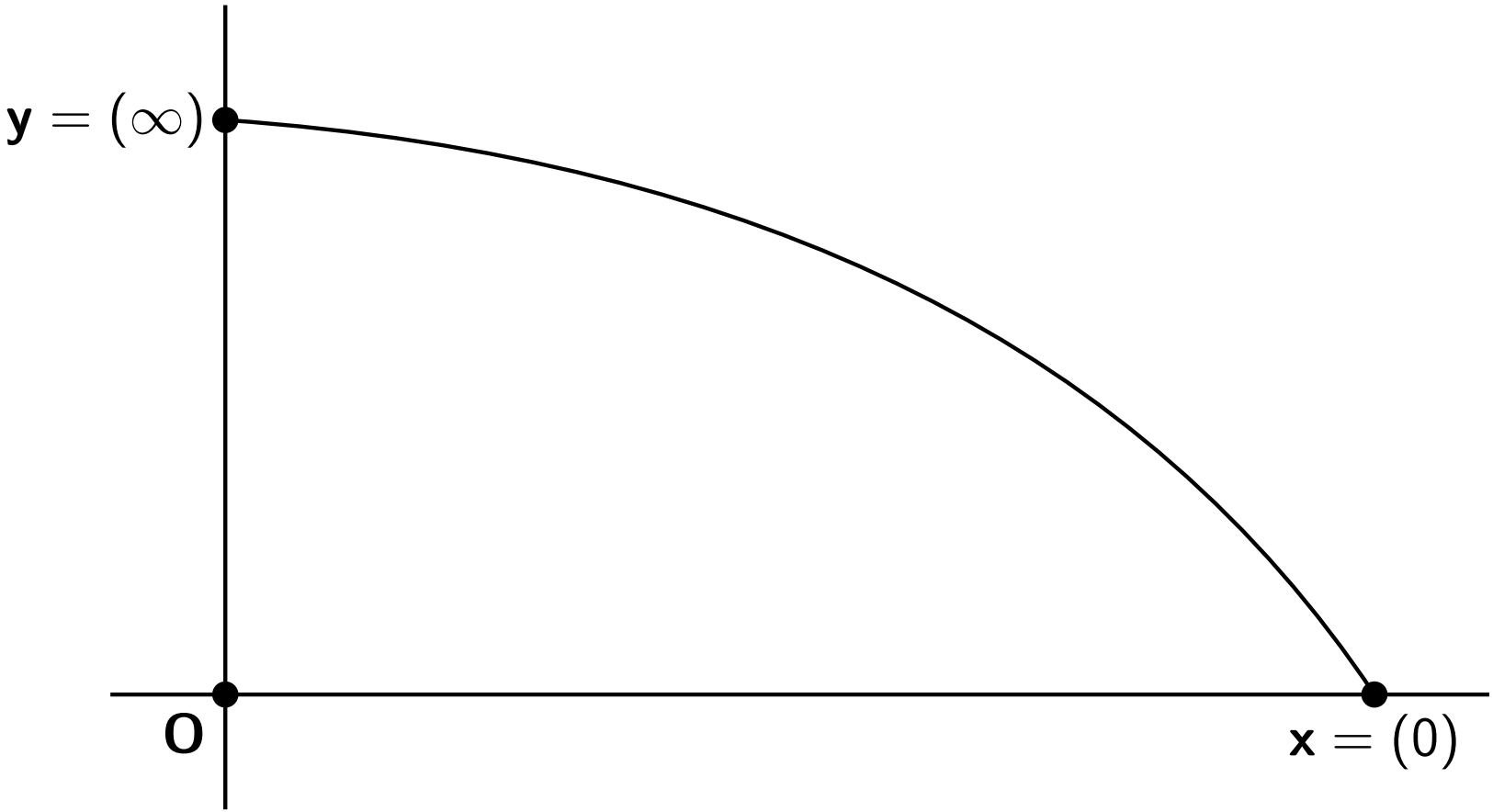
The initial setup

The initial setup



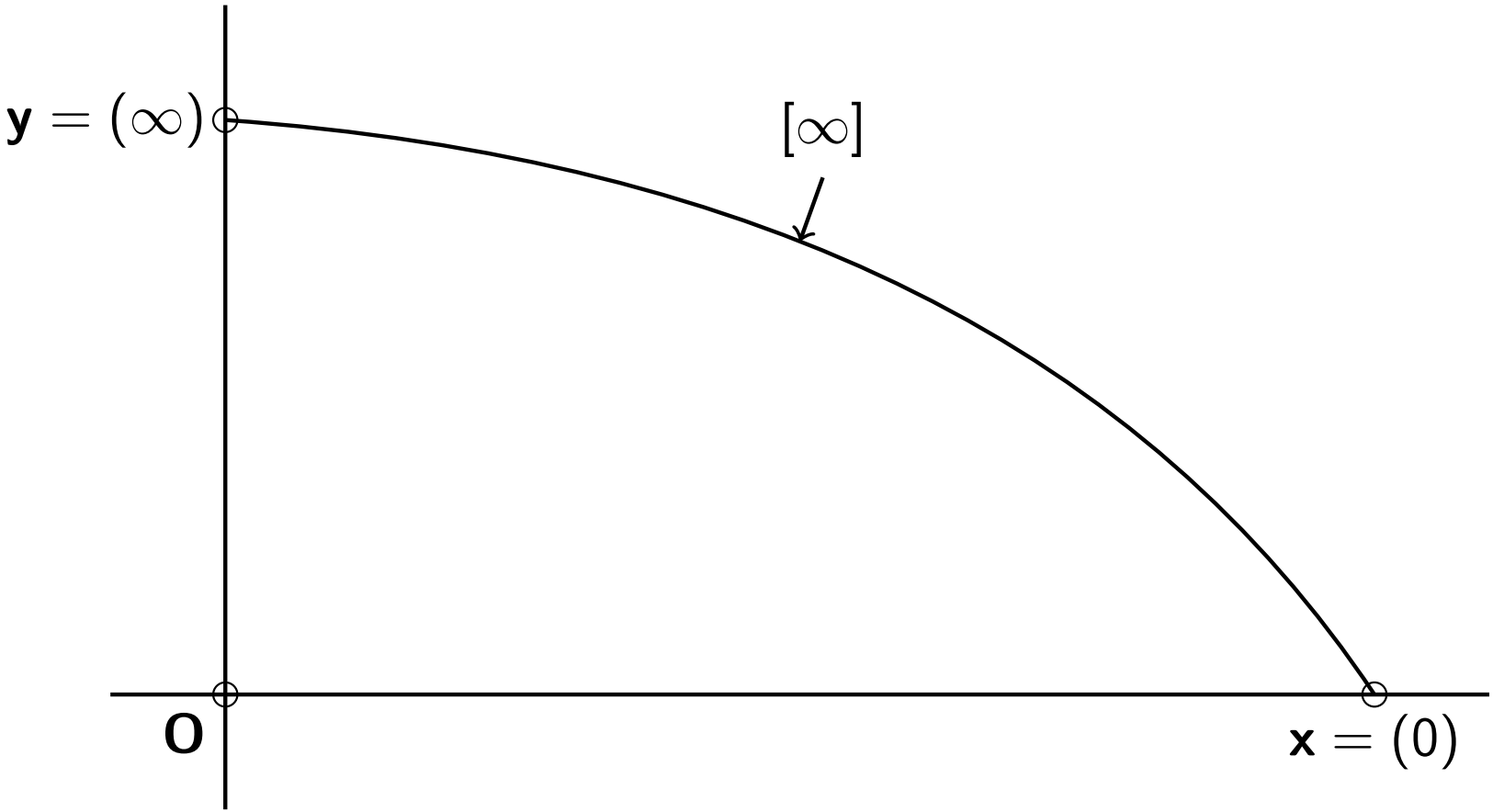
Choose any triangle Δ in the plane.

The initial setup



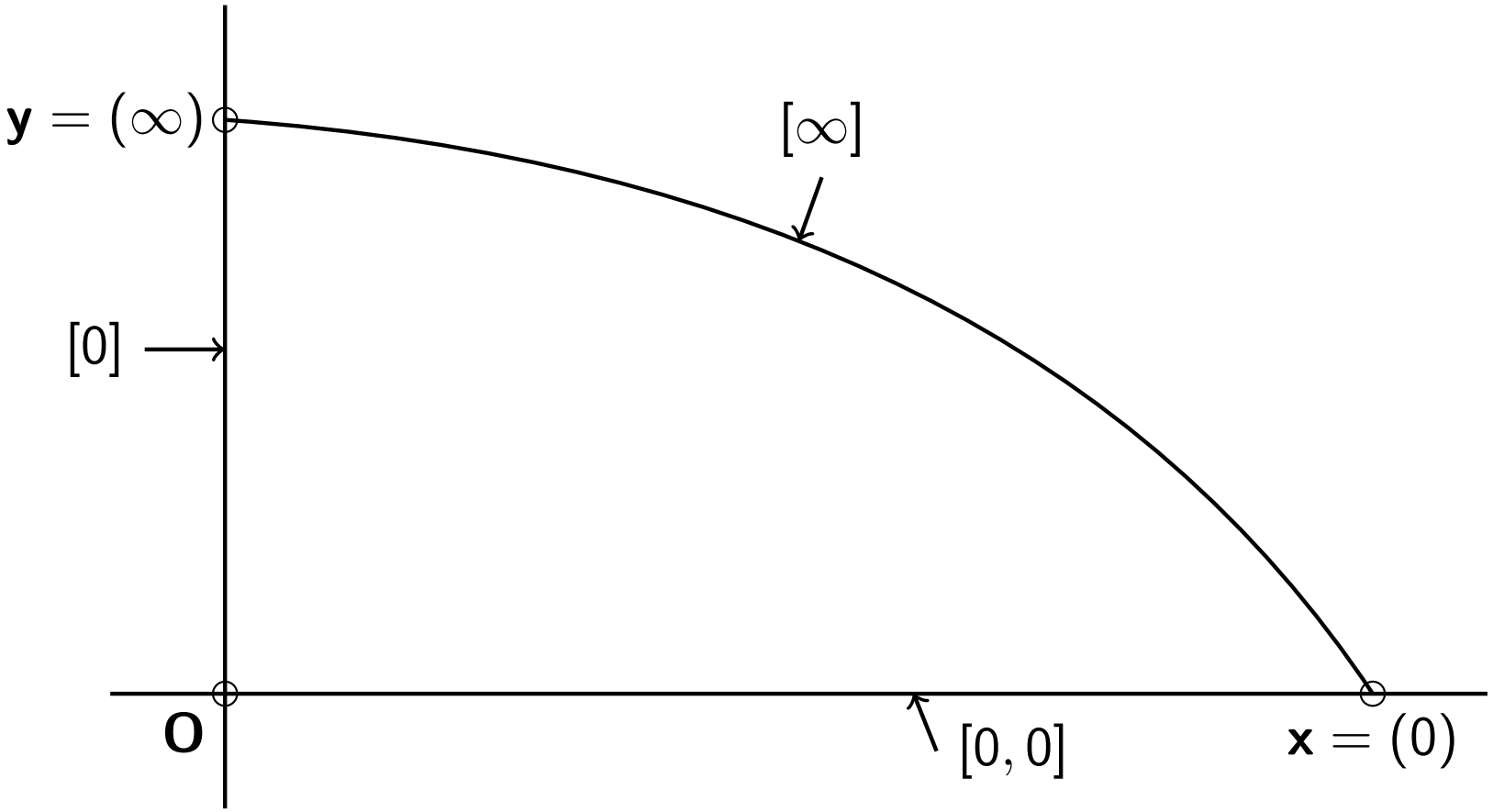
Label $\mathbf{O} = (0, 0)$, $\mathbf{x} = (0)$ and $\mathbf{y} = (\infty)$.

The initial setup



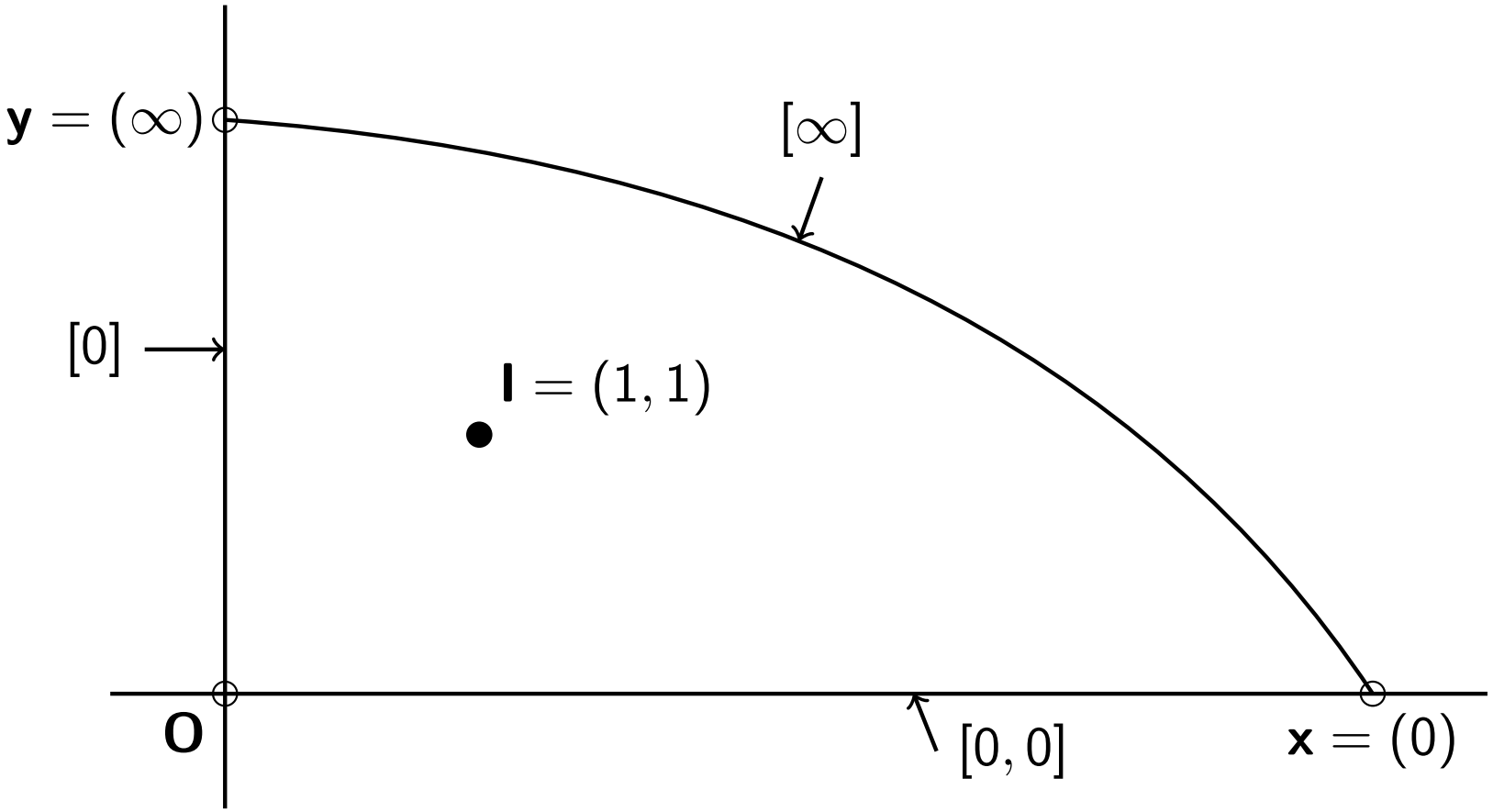
This determines the "line at infinity" $\overline{\mathbf{x}\,\mathbf{y}} = [\infty]$.

The initial setup



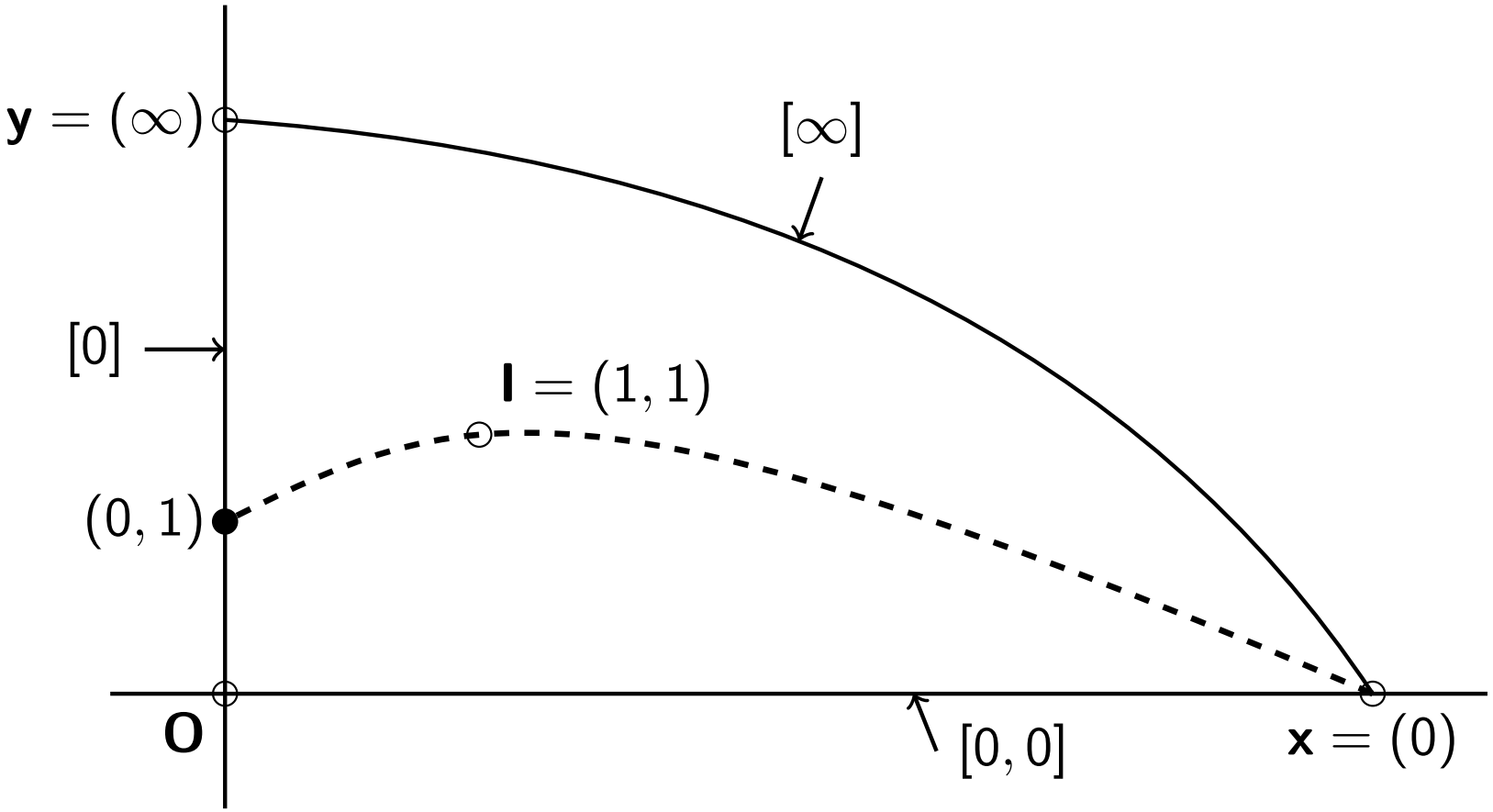
Set $[0] = \overline{\mathbf{O}\,\mathbf{y}}$ (the vertical line) and $[0,0] = \overline{\mathbf{O}\,\mathbf{x}}$.

The initial setup



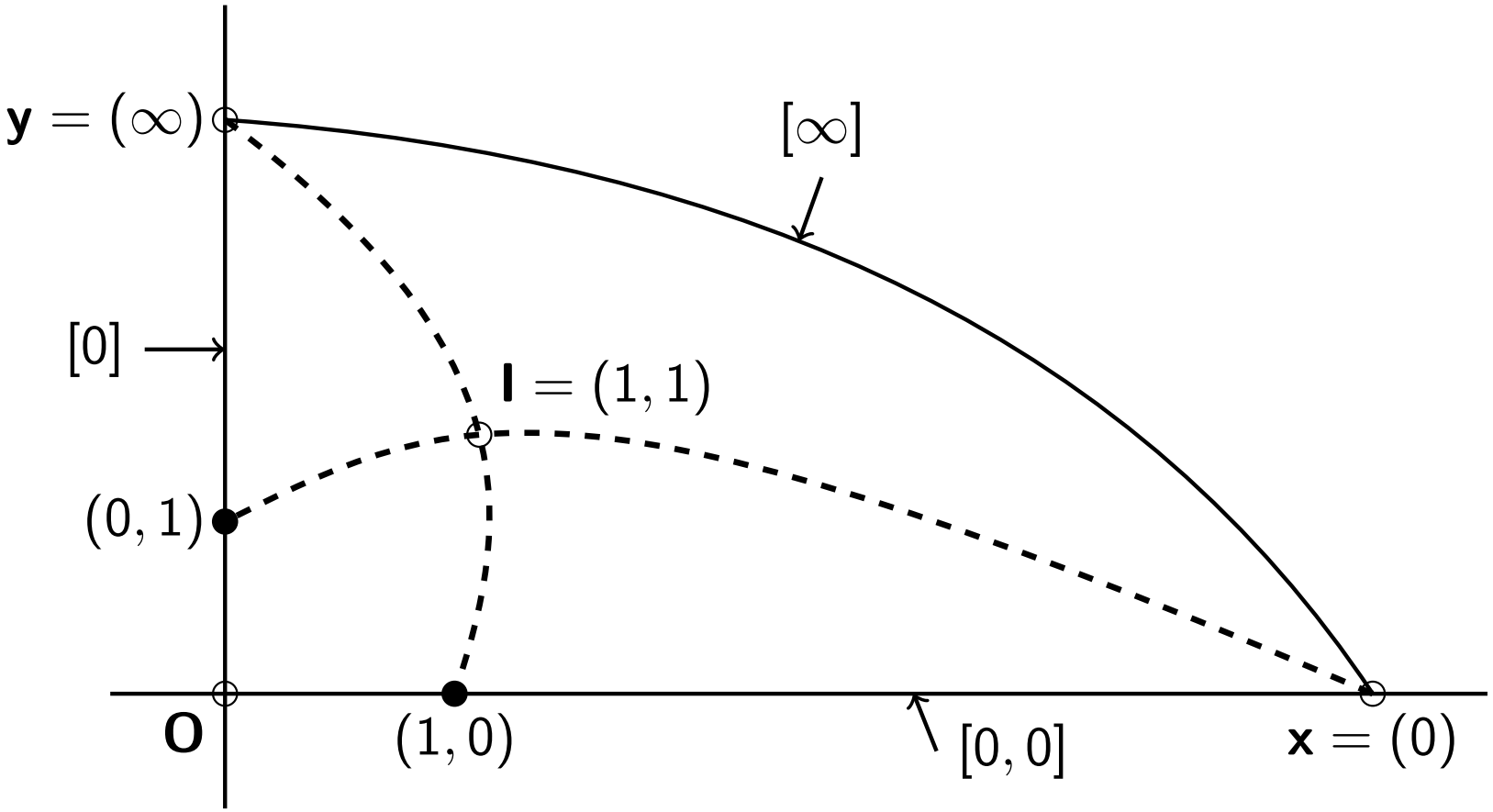
Select a fourth point $\mathbf{I} = (1, 1)$ to create the initial quadrangle.

The initial setup



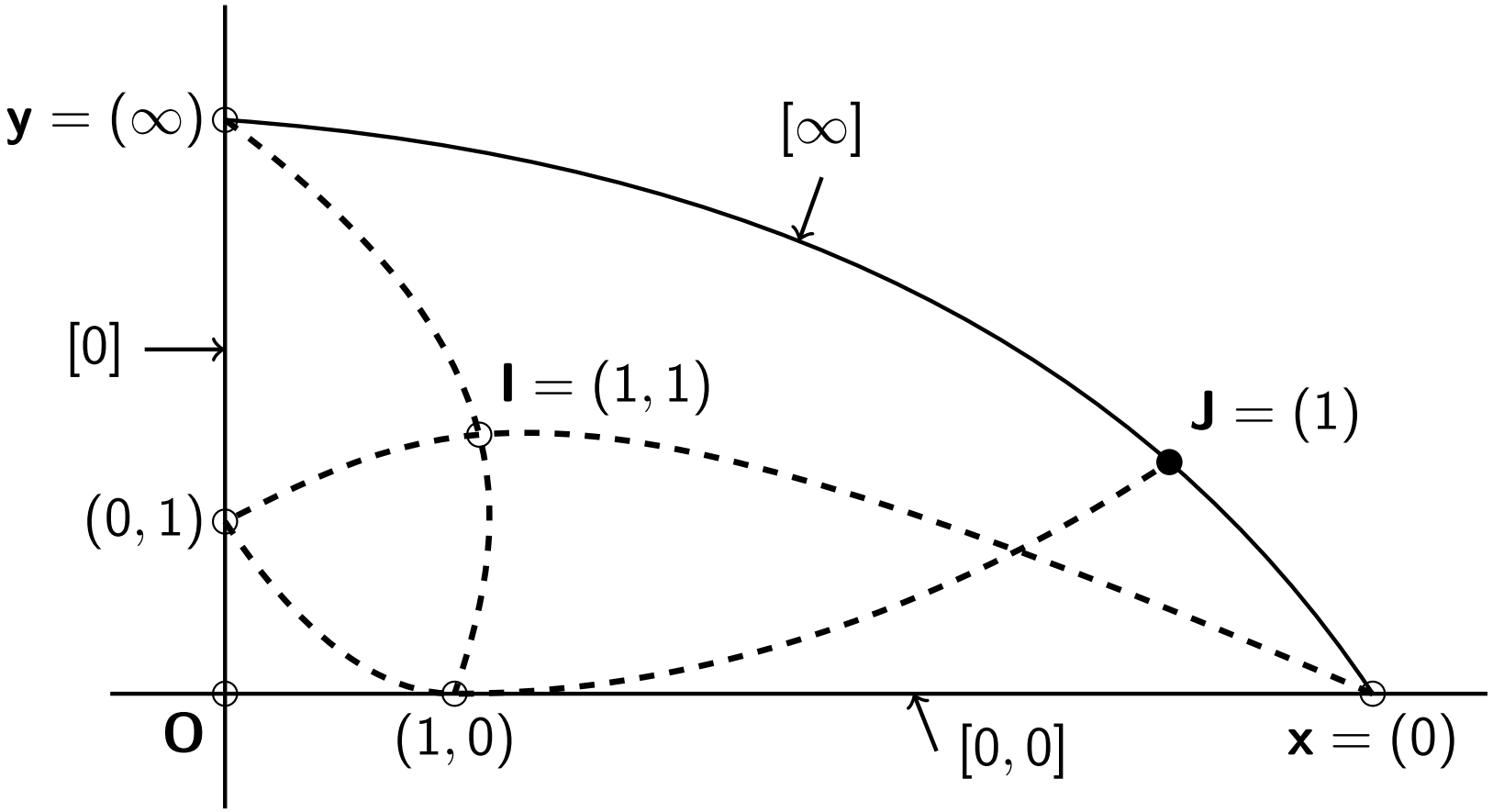
Set $\overline{\mathbf{x}\,\mathbf{I}} \cap [0] = (0, 1)$.

The initial setup



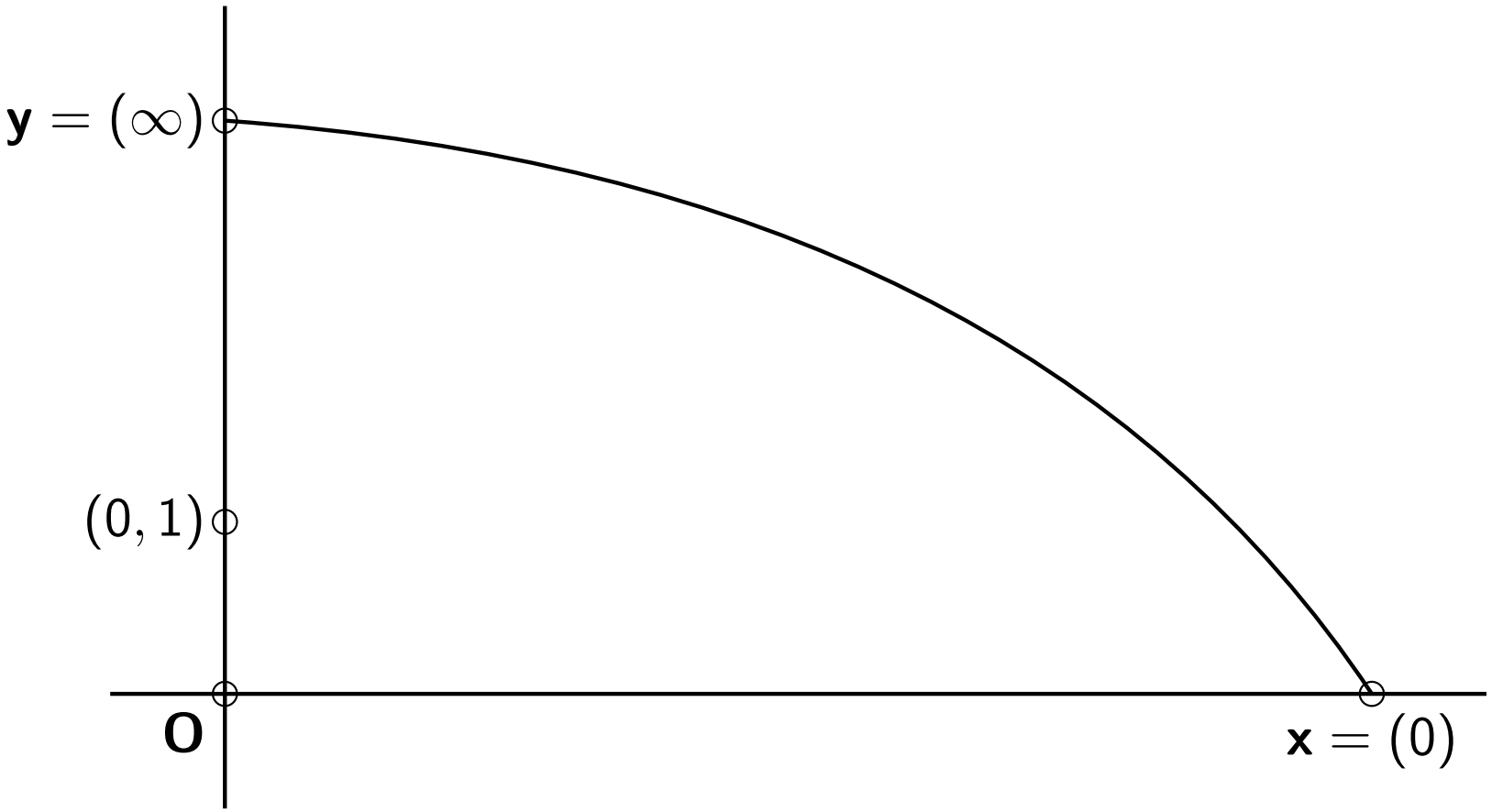
Set $\overline{\mathbf{y}\,\mathbf{l}} \cap [0,0] = (1,0)$.

The initial setup



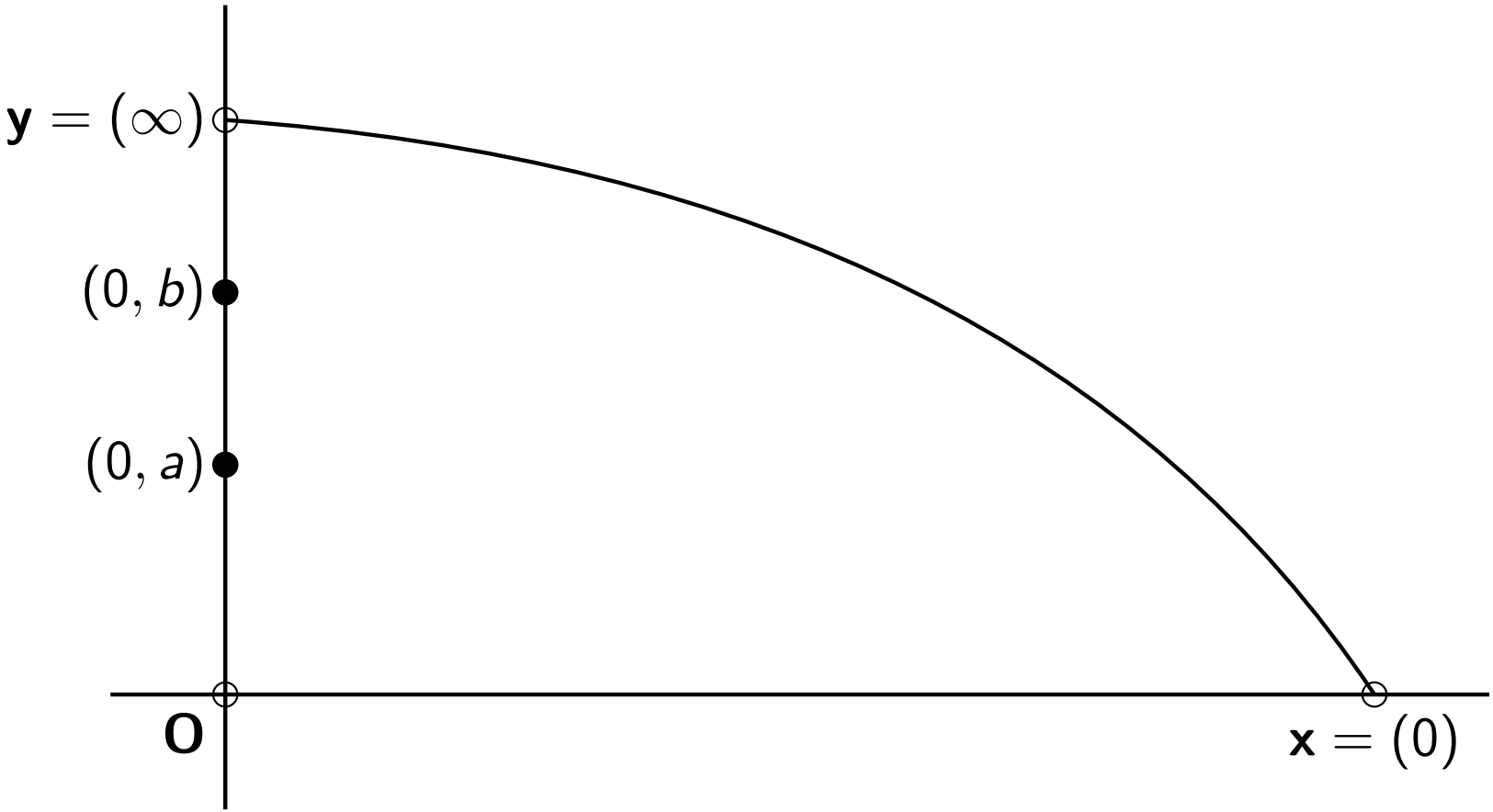
Set $\overline{(1,0)(0,1)} \cap [\infty] = \mathbf{J} = (1)$.

Point labelling



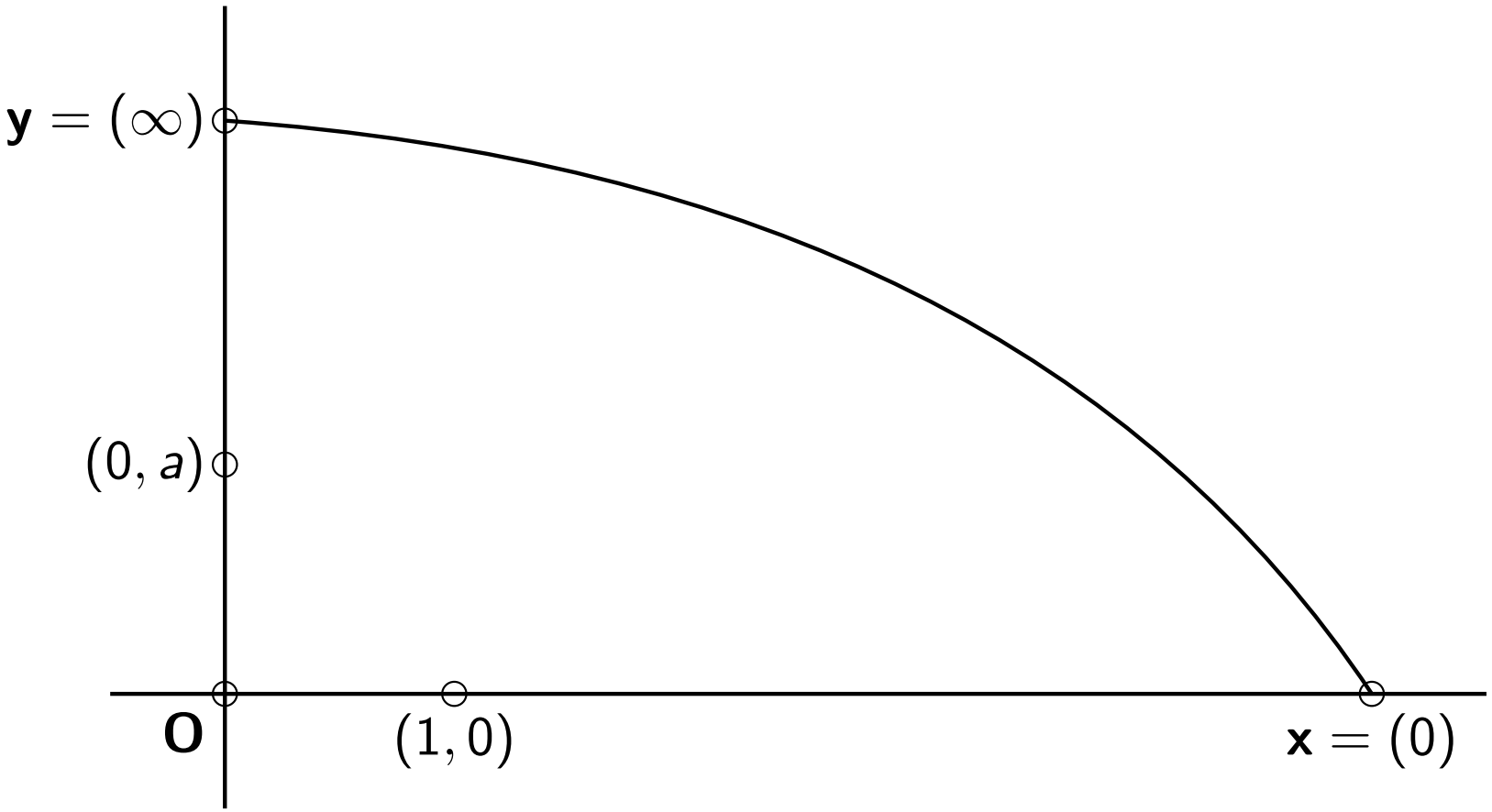
There are $n - 2$ points remaining on [0] that are unlabelled.

Point labelling



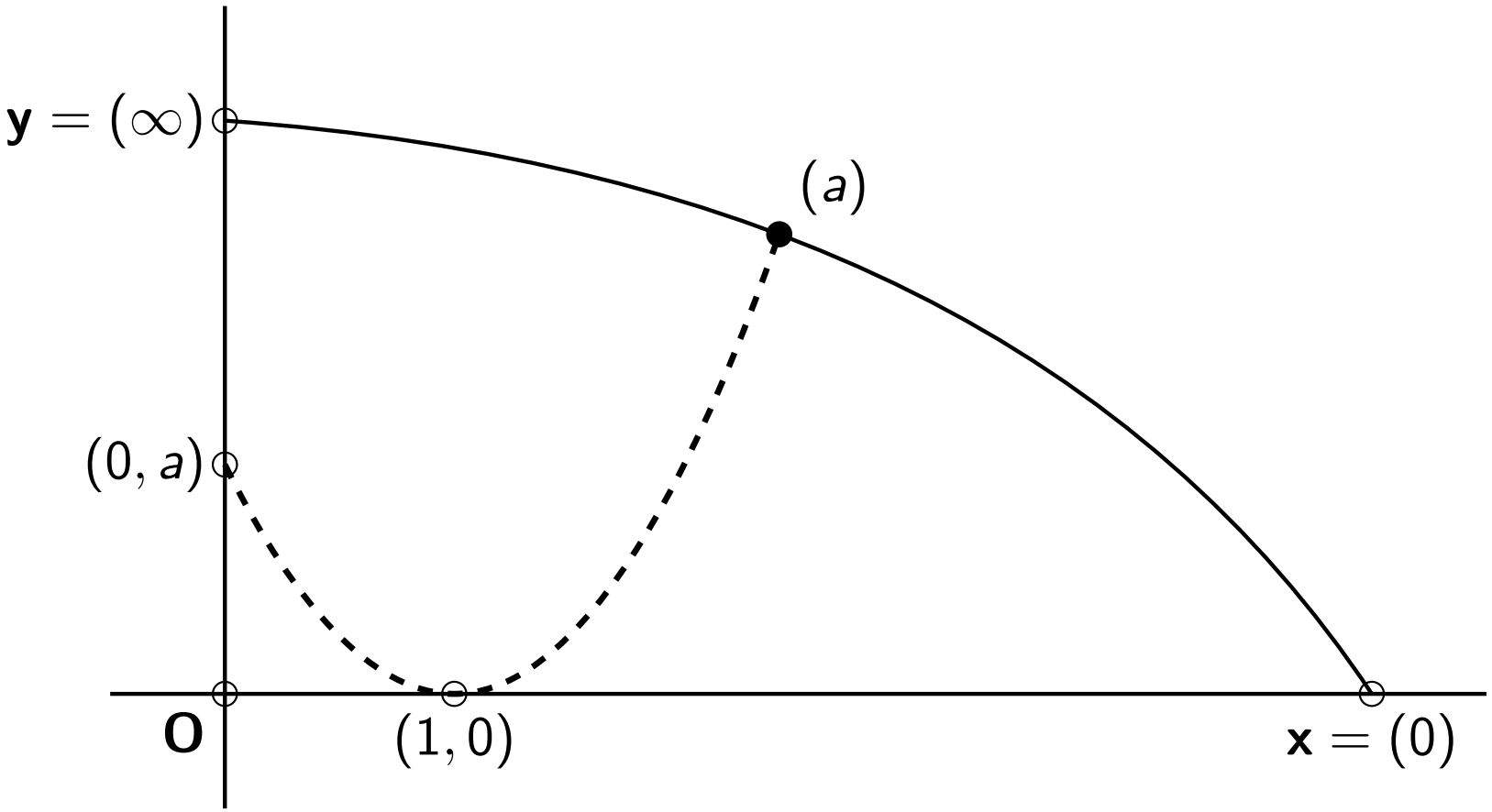
Arbitrarily label them as $(0, a), (0, b)$, etc, $a, b \in \mathcal{R} \setminus \{0, 1\}$.

Point labelling



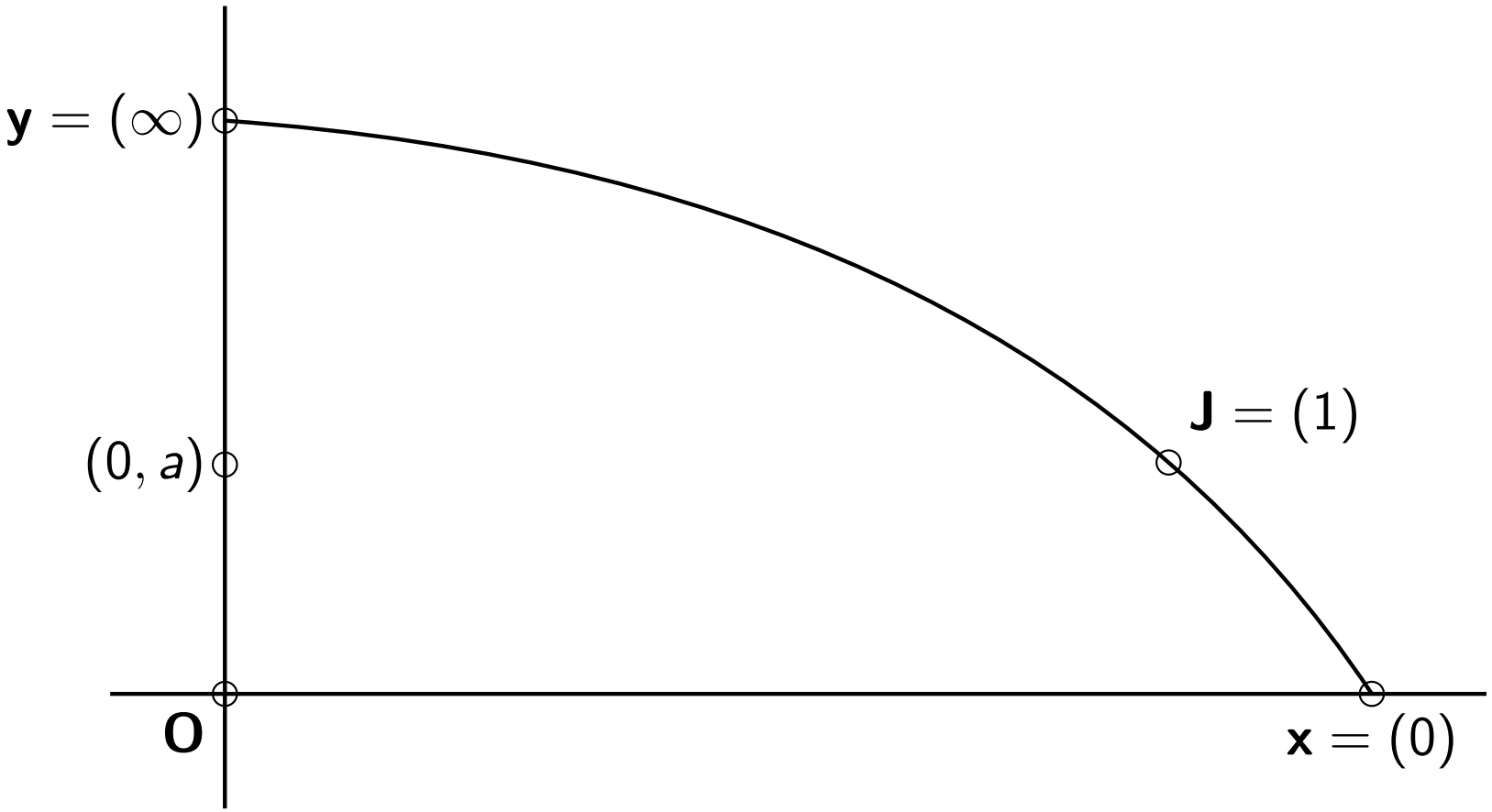
Labelling the points of $[\infty]$:

Point labelling



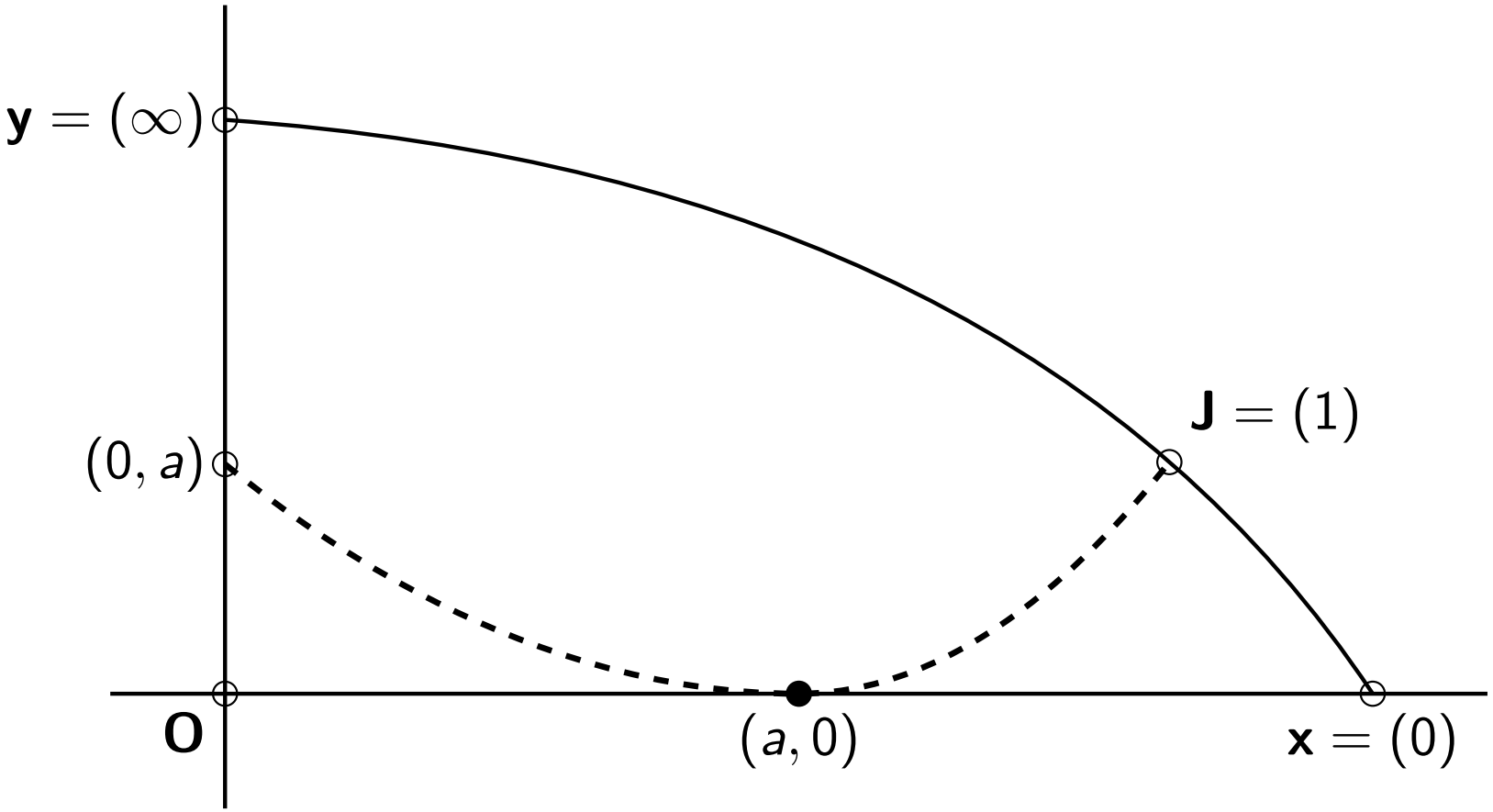
Labelling the points of $[\infty]$: set $\overline{(0, a)(1, 0)} \cap [\infty] = (a)$.

Point labelling



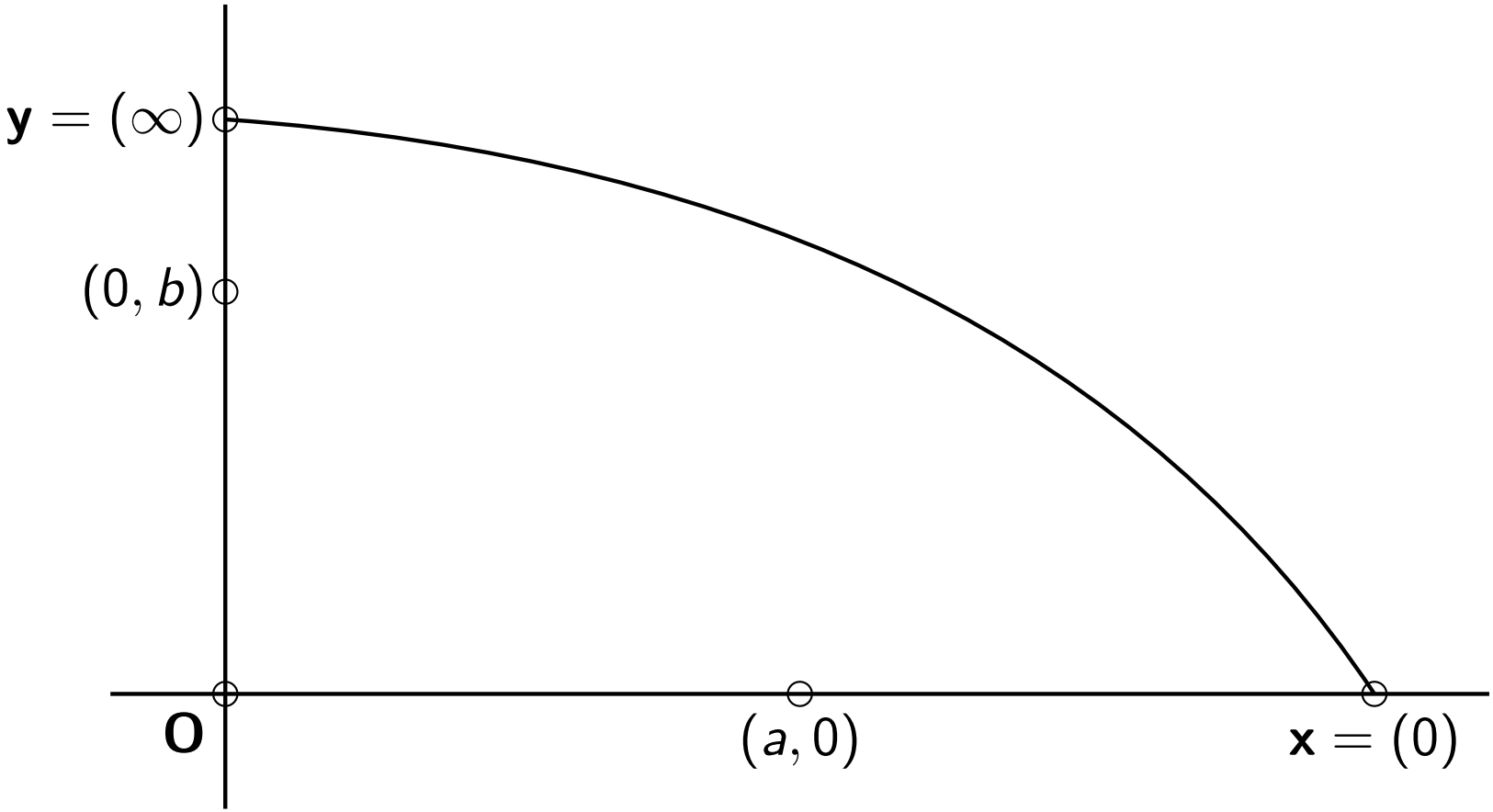
Labelling the points of $[0, 0]$:

Point labelling



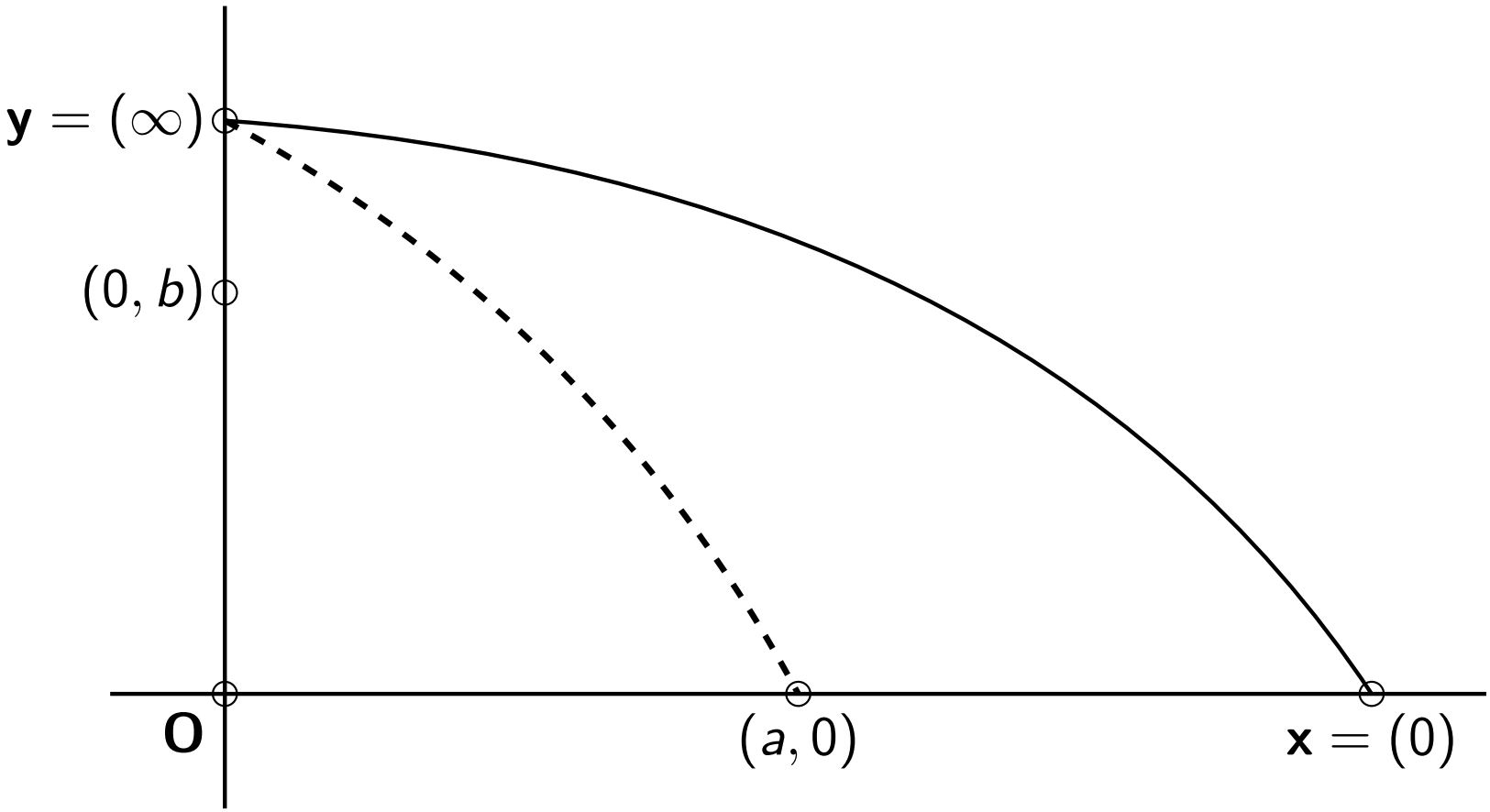
Labelling the points of $[0, 0]$: set $\overline{(0, a)\,\mathbf{J}} \cap [0, 0] = (a, 0)$.

Point labelling



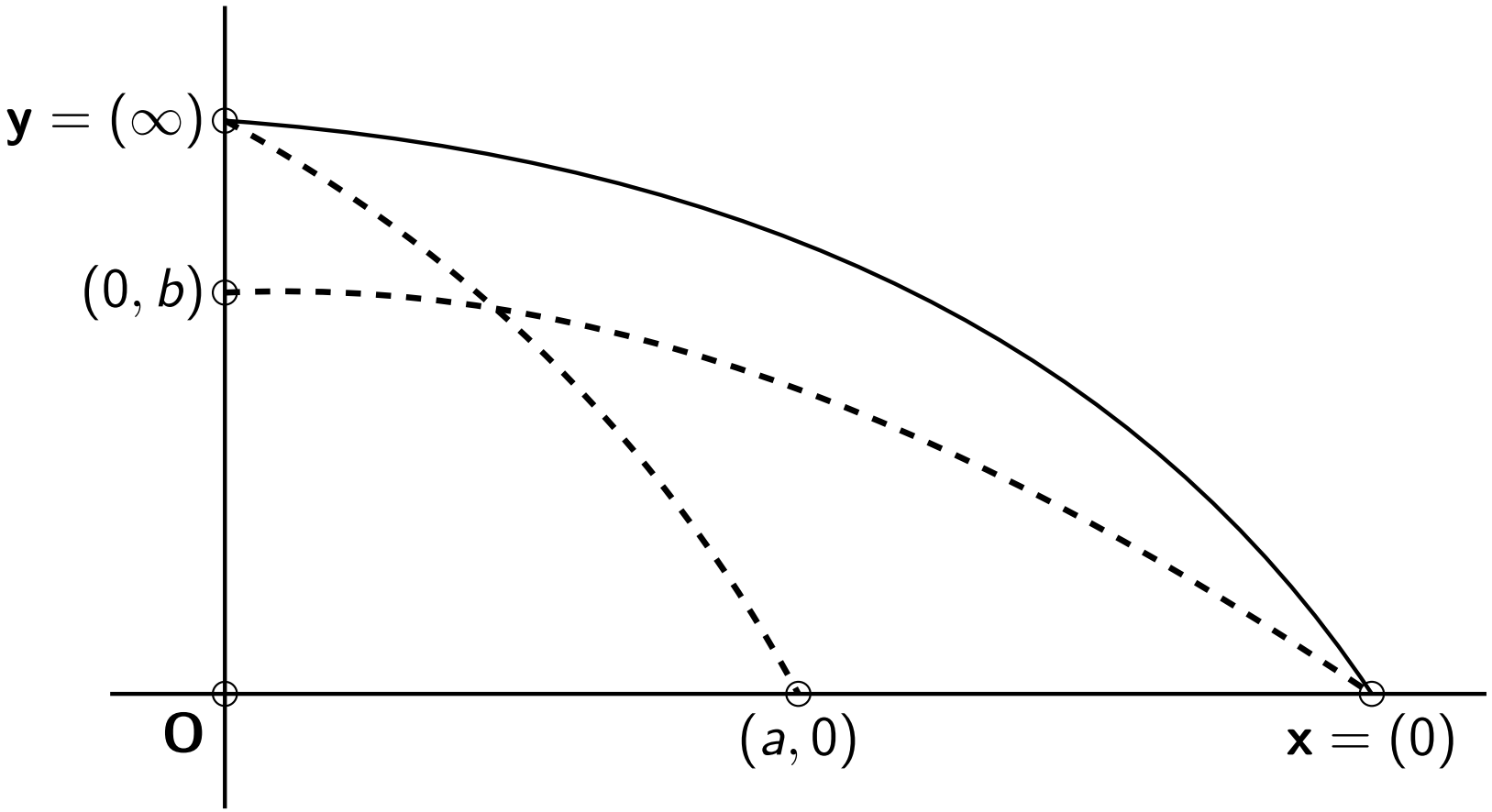
Labelling the "affine" points:

Point labelling



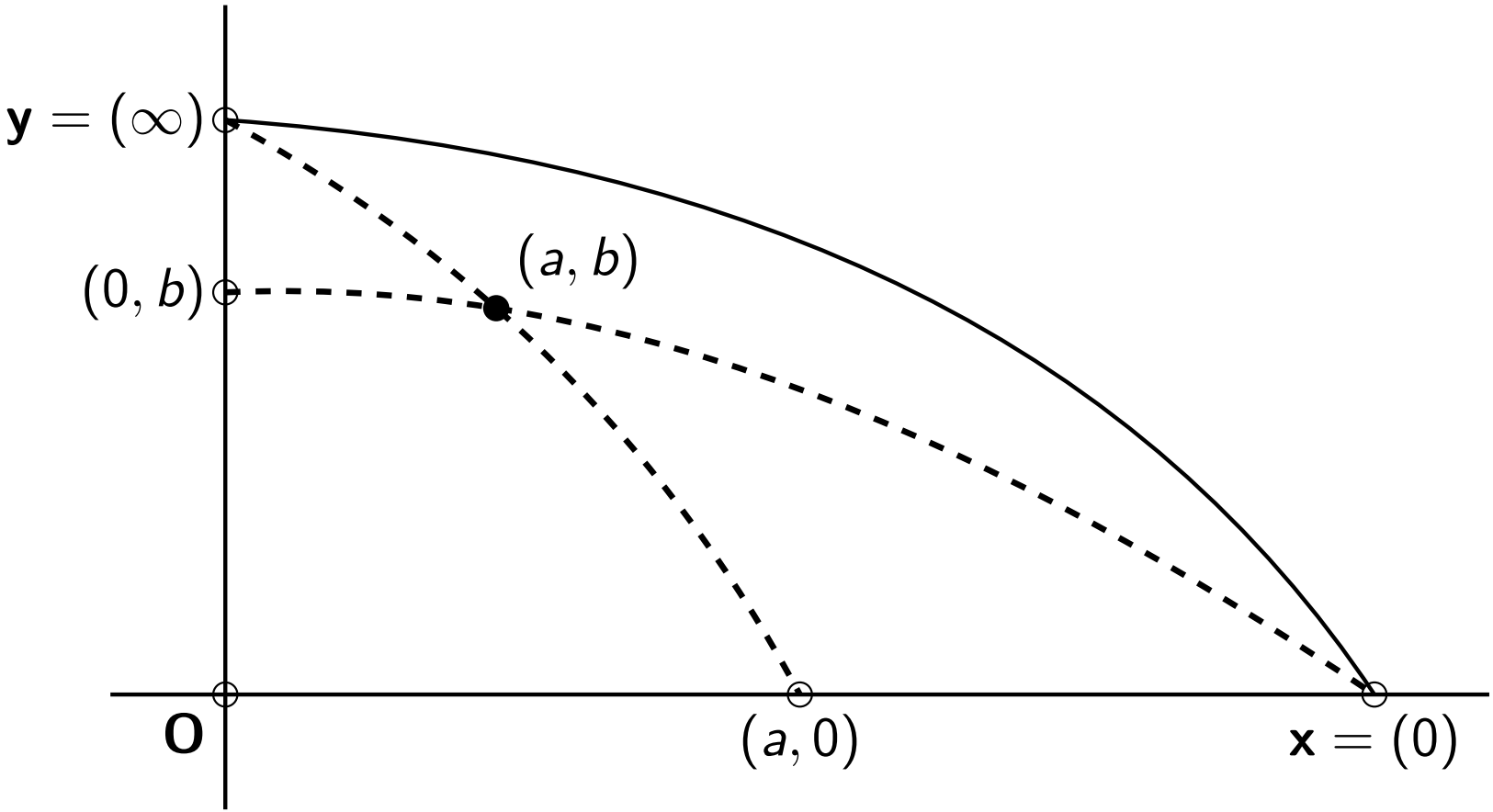
Labelling the "affine" points: set $\overline{(a,0)\,\mathbf{y}} \cap \overline{(0,b)\,\mathbf{x}} = (a,b)$.

Point labelling



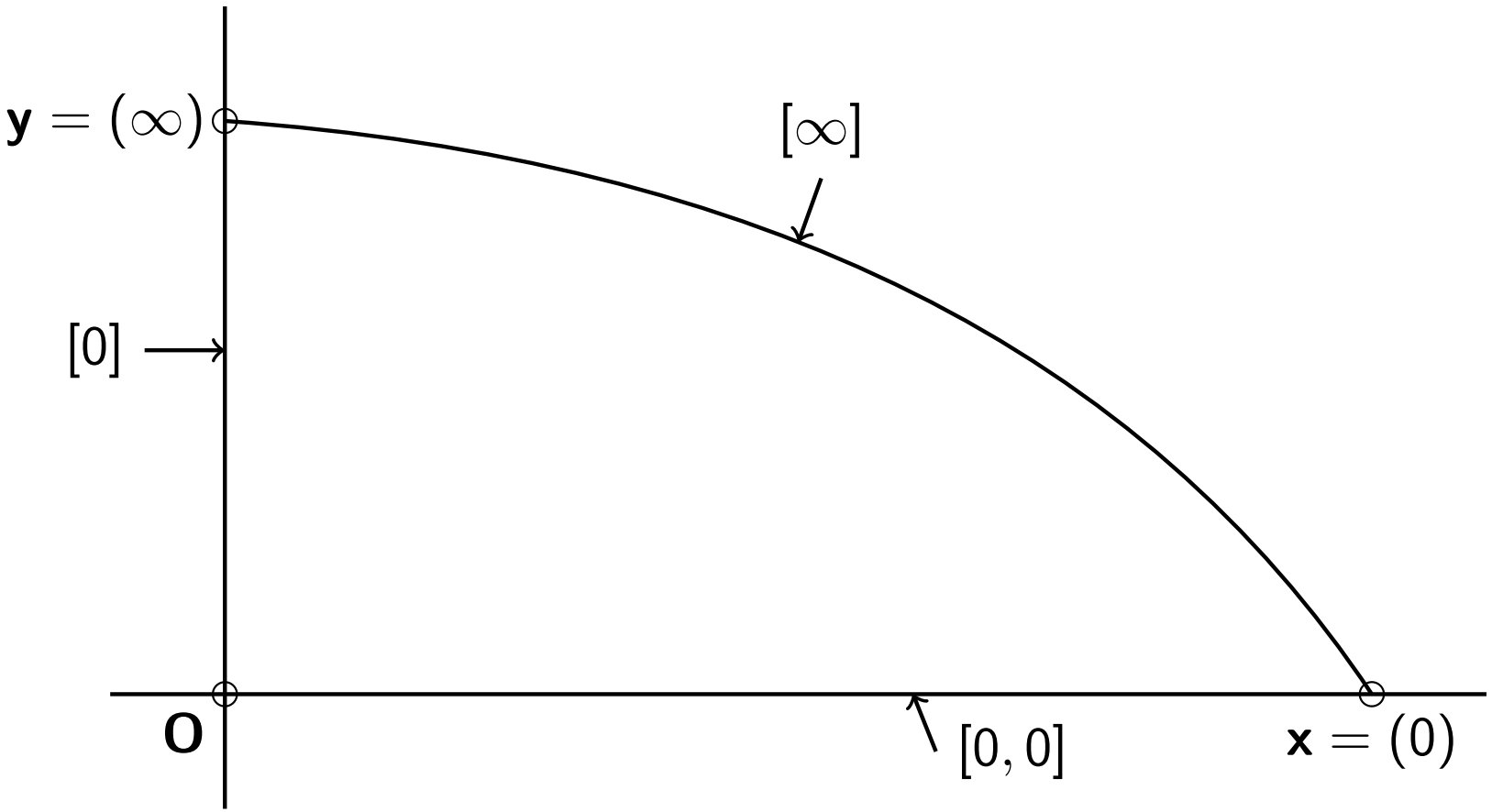
Labelling the "affine" points: set $\overline{(a,0)\,\mathbf{y}} \cap \overline{(0,b)\,\mathbf{x}} = (a,b)$.

Point labelling



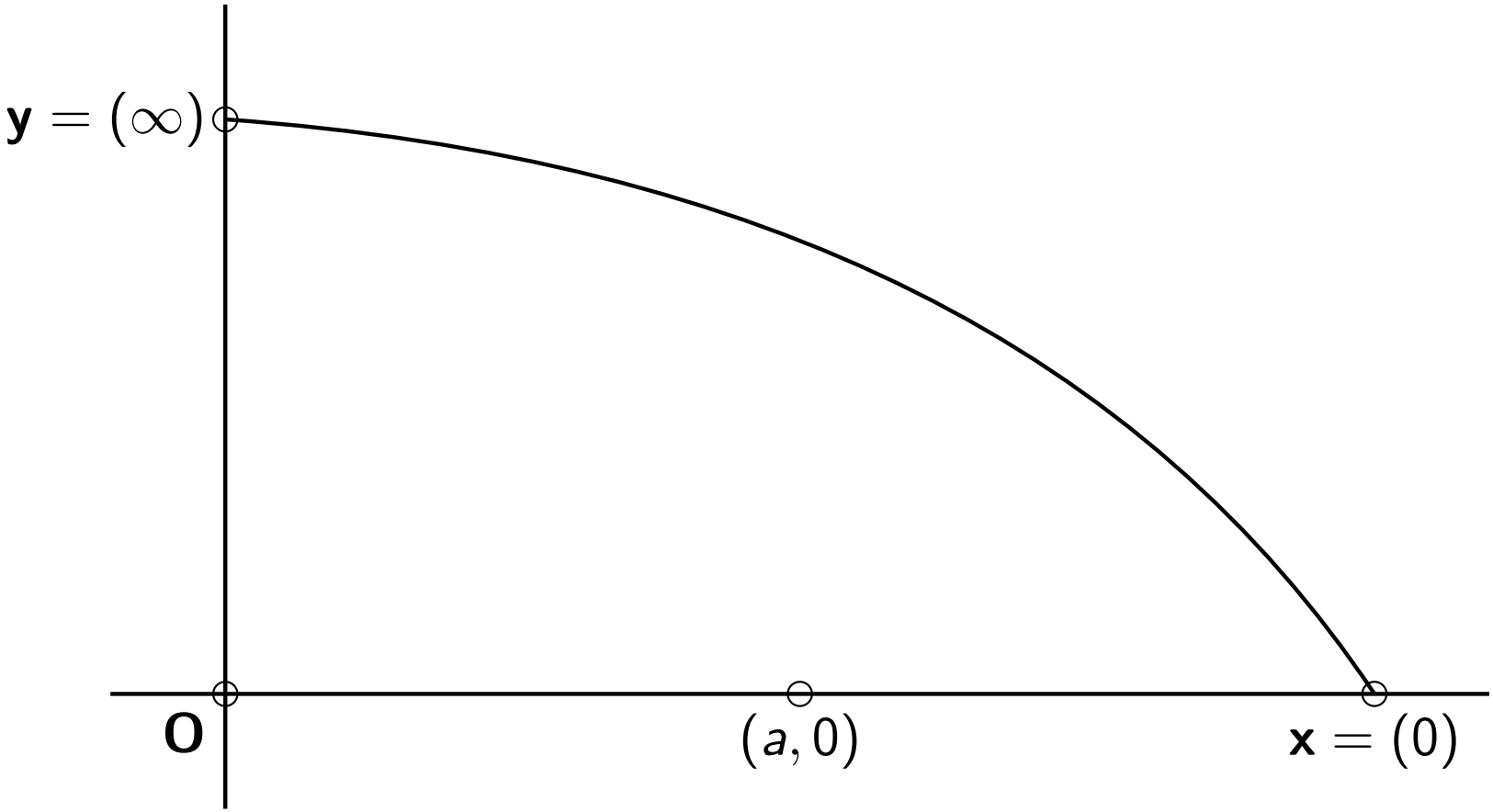
Labelling the "affine" points: set $\overline{(a,0)\,\mathbf{y}} \cap \overline{(0,b)\,\mathbf{x}} = (a,b)$.

Line labelling



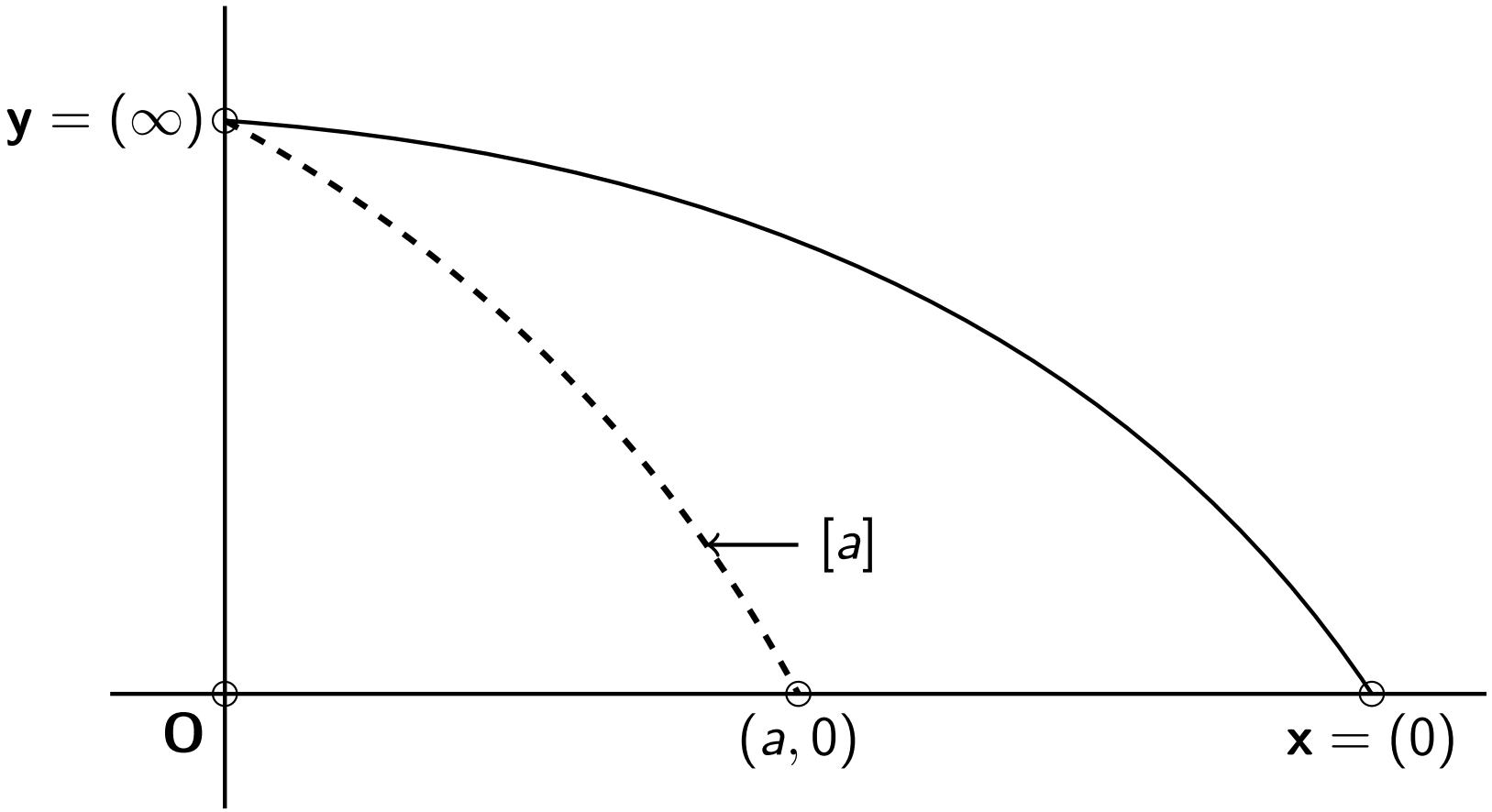
It remains only to complete the labelling of lines.

Line labelling



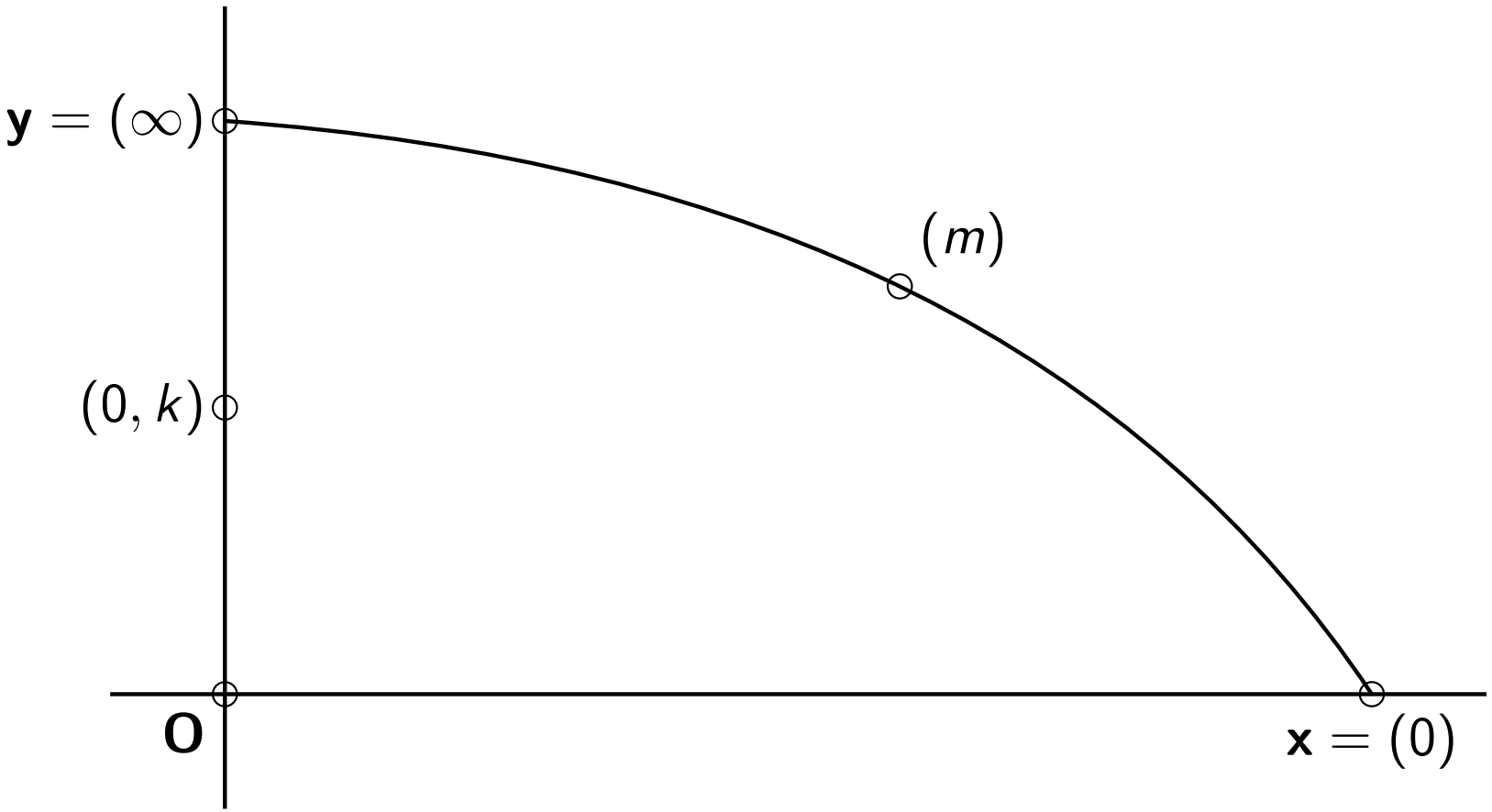
Labelling the "vertical" lines:

Line labelling



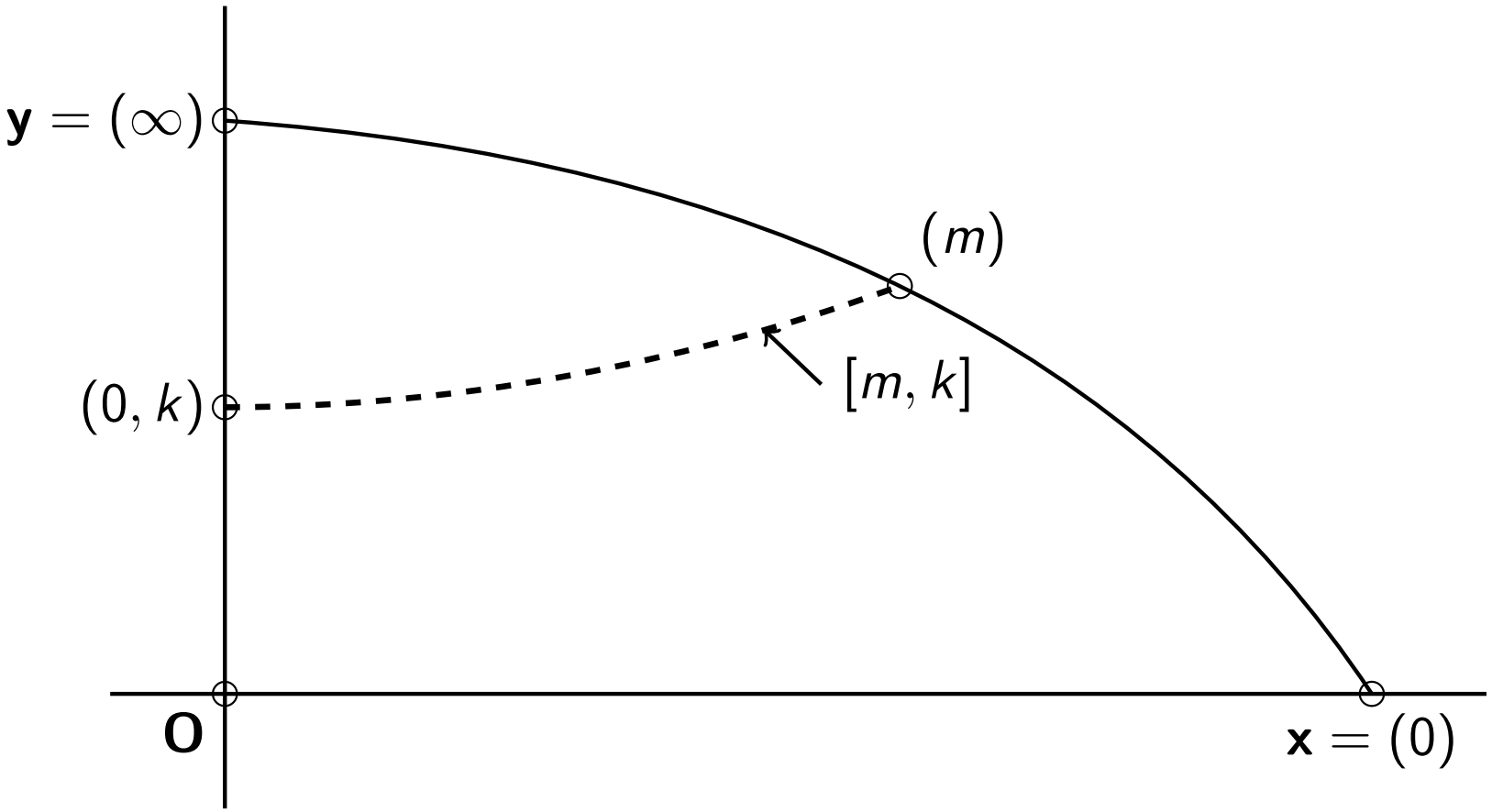
Labelling the "vertical" lines: set $\overline{(a,0)\,\mathbf{y}} = [a]$.

Line labelling



Labelling the "lines of slope m":

Line labelling



Labelling the "lines of slope m": set $\overline{(m)(0,k)} = [m, k]$.

Coordinatisation complete...

With all points and lines of the plane $\mathcal{P}$ now labelled, the task that remains is to produce an algebraic system equivalent to $\mathcal{P}$ that allows meaningful study.
This is achieved via the construction of a trivariate function on $\mathcal{R}$.

Coordinatisation complete...

With all points and lines of the plane $\mathcal{P}$ now labelled, the task that remains is to produce an algebraic system equivalent to $\mathcal{P}$ that allows meaningful study.
This is achieved via the construction of a trivariate function on $\mathcal{R}$.

A *planar ternary ring (PTR)* T is a trivariate function $T : \mathcal{R}^3 \to \mathcal{R}$ obtained from a coordinatised plane $\mathcal{P}$ via the defining rule

$$T(m, x, y) = k \text{ if and only if } (x, y) \in [m, k].$$

It cannot be over emphasised that any one $\mathcal{P}$ can yield many different PTRs through choosing different quadrangles $\mathbf{O\,x\,y\,I}$, or even through choosing a different labelling of the line [0].

Hall's Equivalence of PTRs and projective planes

Theorem (Hall, 1943)
Let $\mathcal{P}$ be a projective plane of n and $\mathcal{R}$ be any set of cardinality n. Let $T : \mathcal{R}^3 \to \mathcal{R}$ be a PTR obtained from coordinatising $\mathcal{P}$. Then T must satisfy 5 specific properties (details irrelevant for this talk).

Hall's Equivalence of PTRs and projective planes

Theorem (Hall, 1943)
Let $\mathcal{P}$ be a projective plane of n and $\mathcal{R}$ be any set of cardinality n. Let $T : \mathcal{R}^3 \to \mathcal{R}$ be a PTR obtained from coordinatising $\mathcal{P}$. Then T must satisfy 5 specific properties (details irrelevant for this talk).
Conversely, any tri-variate function T defined on $\mathcal{R}$ which satisfies those 5 properties can be used to define an affine plane $\mathcal{A}_T$ of order n as follows:

- the points of $\mathcal{A}$ are (x, y), with $x, y \in \mathcal{R}$;
- the lines of $\mathcal{A}$ are the symbols $[m, k]$, with $m, k \in \mathcal{R}$, defined by

$$[m, k] = \{(x, y) \in \mathcal{R} \times \mathcal{R} : k = T(m, x, y)\},$$

and the symbols $[a]$, with $a \in \mathcal{R}$, defined by

$$[a] = \{(a, y) : y \in \mathbb{F}_q\}.$$

Note how the PTR is used to define the non-vertical lines.

Binary operations from the PTR

The addition and multiplication come from the PTR: specifically

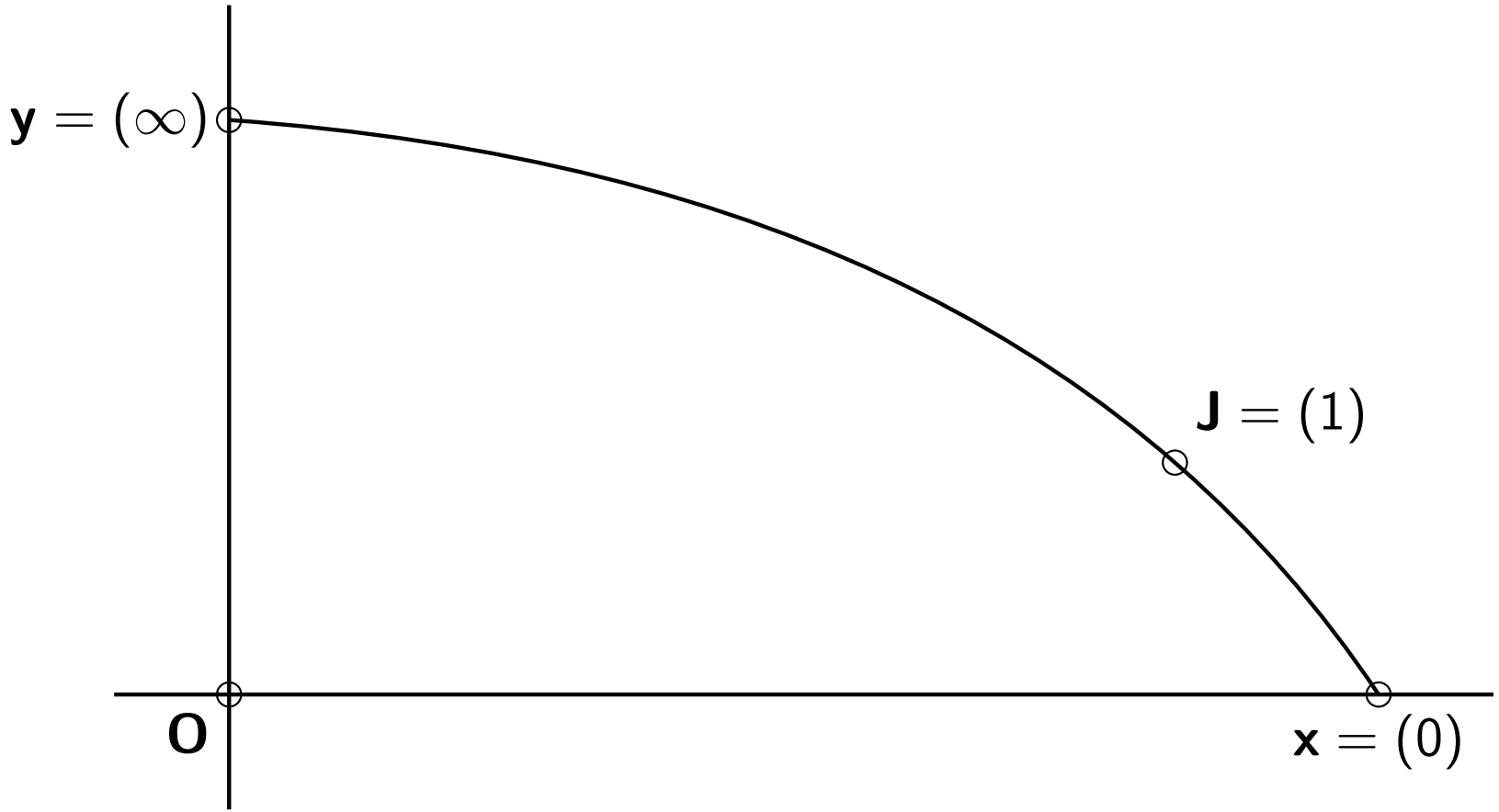
$$x \oplus y = T(1, x, y),$$
$$x \odot y = T(x, y, 0),$$

for all $x, y \in \mathcal{R}$.

From Hall's result you can show that both $\oplus$ and $\odot$ form loops with identities 0 and 1 over $\mathcal{R}$ and $\mathcal{R}^*$, respectively.

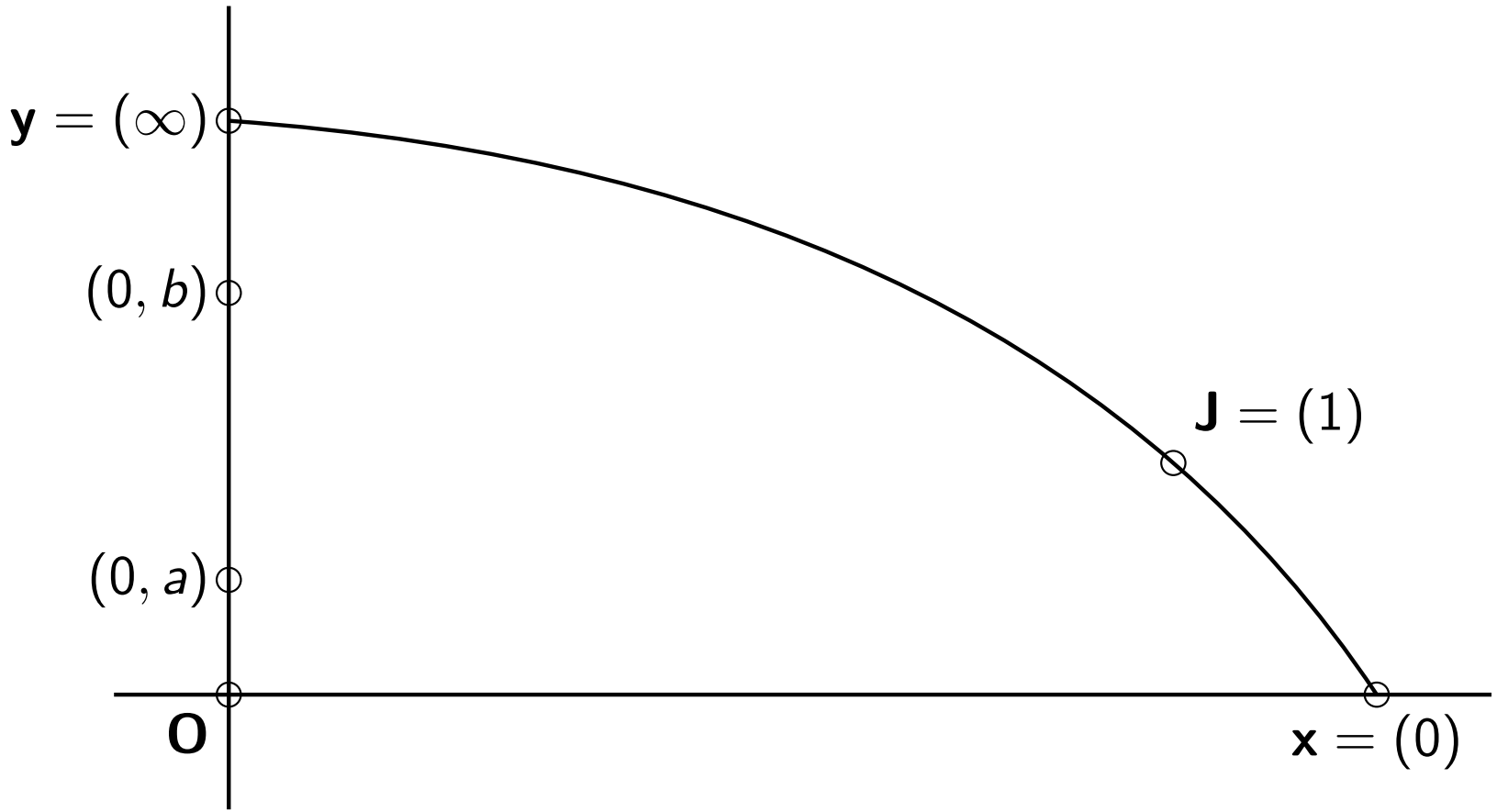
A little while ago, I realised that you can actually determine how the operations act on the plane.

The action of $\oplus$ on the vertical line



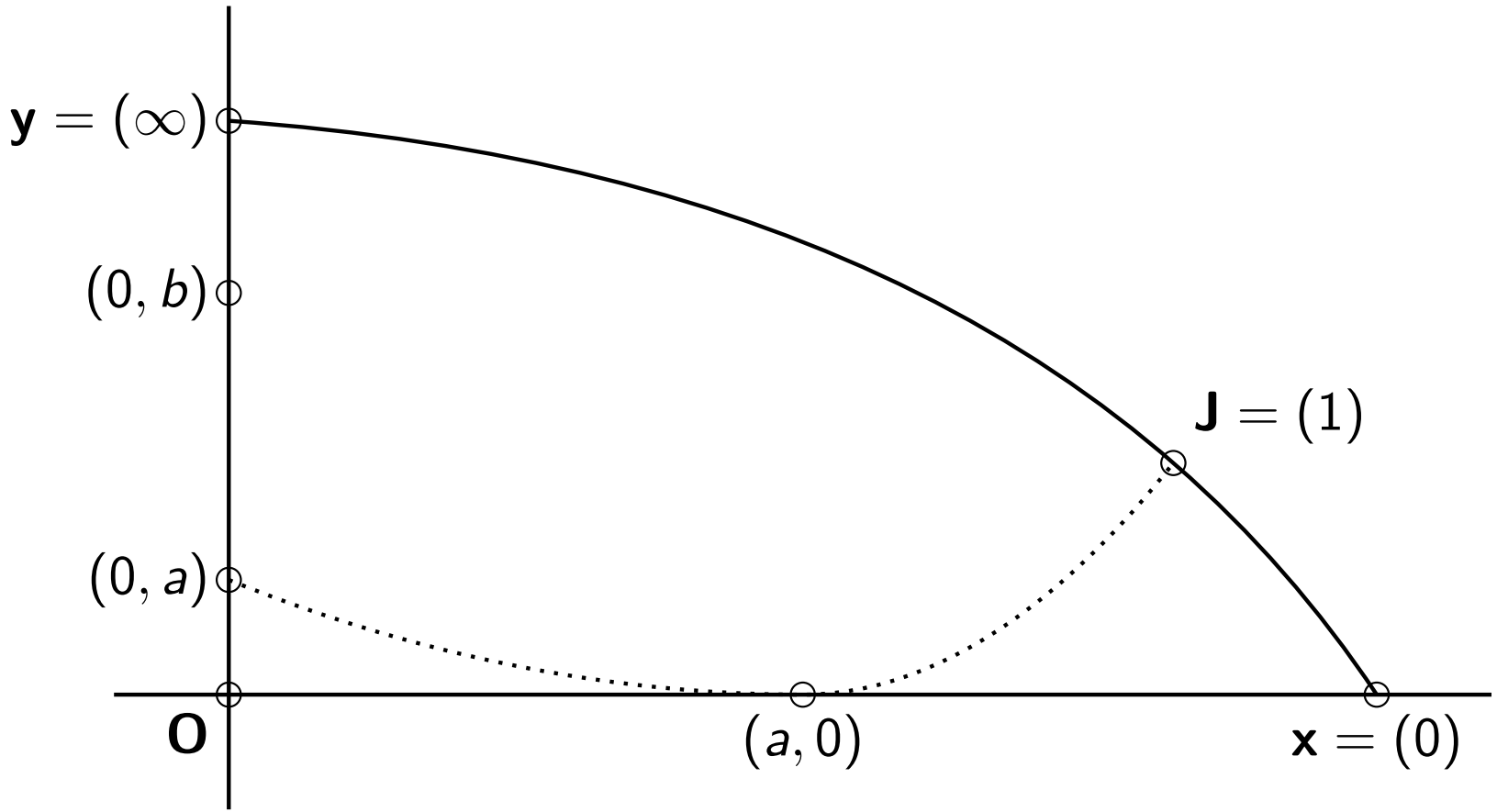
The action is anchored on the triangle $\Delta\,\mathbf{O}\,\mathbf{x}\,\mathbf{y}$ and point $\mathbf{J} = (1)$.

The action of $\oplus$ on the vertical line



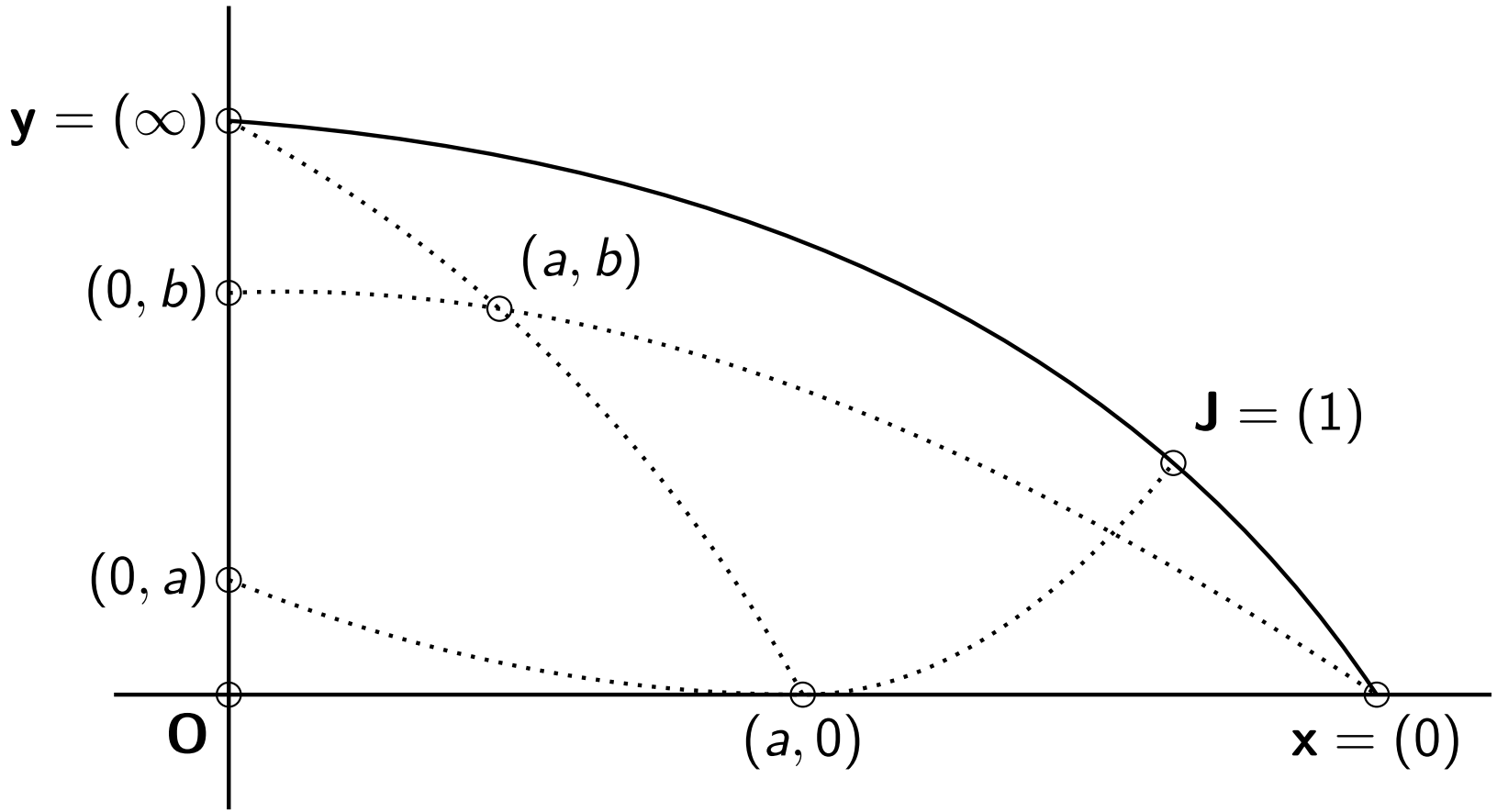
Choose two points $(0, a), (0, b)$ on $\overline{\mathbf{O}\,\mathbf{y}} = [0]$. What is $(0, a \oplus b)$?

The action of $\oplus$ on the vertical line



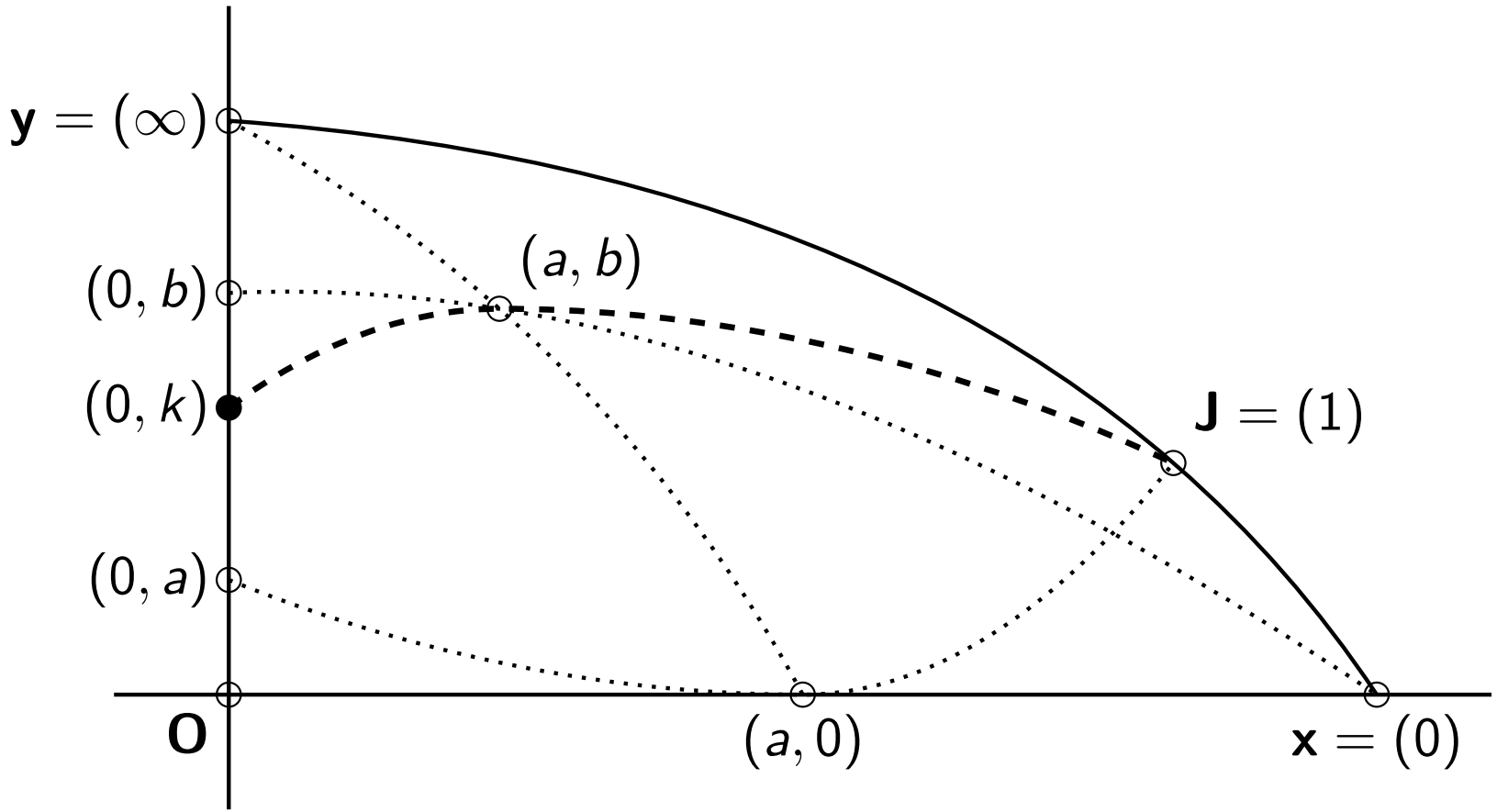
Create the point $(a, 0) = \overline{(0, a)\,\mathbf{J}} \cap \overline{\mathbf{O}\,\mathbf{x}}$.

The action of $\oplus$ on the vertical line



Now create the point $(a, b) = \overline{(a, 0)\,\mathbf{y})} \cap \overline{(0, b)\,\mathbf{x}}$.

The action of $\oplus$ on the vertical line



Now $(0, k) = \overline{\mathbf{J}(a, b)} \cap \overline{\mathbf{O}\,\mathbf{y}} = (0, a \oplus b)$.

Why care?

There are a lot of semifield planes known through computation (mostly by Eric Moorhouse).

All of these have the same additive structure as a finite field, so you can label the vertical line so that the addition **IS** the field addition.

The resulting multiplication must be a semifield multiplication, and so you can derive planar DOs from it.

Why care?

There are a lot of semifield planes known through computation (mostly by Eric Moorhouse).

All of these have the same additive structure as a finite field, so you can label the vertical line so that the addition **IS** the field addition.

The resulting multiplication must be a semifield multiplication, and so you can derive planar DOs from it.

This hasn't been done before.

Thus, we can find more planar DOs that represent previously anonymous commutative semifield planes.

And this construction covers the full isotopy class, whether it splits into two strong isotopy classes or not.

That's my newest Ph.D. student's research project.

Why care?

There are a lot of semifield planes known through computation (mostly by Eric Moorhouse).

All of these have the same additive structure as a finite field, so you can label the vertical line so that the addition **IS** the field addition.

The resulting multiplication must be a semifield multiplication, and so you can derive planar DOs from it.

This hasn't been done before.

Thus, we can find more planar DOs that represent previously anonymous commutative semifield planes.

And this construction covers the full isotopy class, whether it splits into two strong isotopy classes or not.

That's my newest Ph.D. student's research project. So we might have to wait a few years.

Thanks for your time.