Implicitization in $\not{3}^{2.5}$ Ways

Andrew Biehl and William Taylor

April 29, 2026

Abstract

Implicitization is the act of finding a system of implicit equations for the variety described by a given system of parametric equations. In this paper, we consider the problem of implicitizing rational planar curves in particular. We remind the reader of two methods (namely, via Gröbner bases and resultants) for implicitizing such curves and then present a "third" method, which in some sense combines the previous two ideas with a new one (namely, moving line bases).

-1 The general implicitization problem

Let $V \subseteq \mathbb{A}^n$ be an affine variety over some field $\Bbbk$ (not necessarily algebraically closed). There are two computationally useful ways to describe this variety:

- *implicitly*; that is, as the solution set of some finite system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0, \end{aligned}$$

  which is to say that $V = \mathcal{V}(S)$ for the finite set $S = \{f_1, \ldots, f_m\} \subseteq \Bbbk[x_1, \ldots, x_n]$; and

- *parametrically*; that is, as minimally containing the image set of some system of rational parametric functions

$$\begin{aligned} x_1 &= \frac{g_1(t_1, \ldots, t_l)}{h_1(t_1, \ldots, t_l)} \\ x_2 &= \frac{g_2(t_1, \ldots, t_l)}{h_2(t_1, \ldots, t_l)} \\ &\vdots \\ x_n &= \frac{g_n(t_1, \ldots, t_l)}{h_n(t_1, \ldots, t_l)}, \end{aligned}$$

  which is to say that $V = \overline{\text{im}(F)} = \mathcal{V}(\mathcal{I}(\text{im}(F)))$ for some rational map $F : \mathbb{A}^l \dashrightarrow \mathbb{A}^n$ defined by

$$F = \Big(\frac{g_1}{h_1}, \ldots, \frac{g_n}{h_n}\Big)$$

  (so that $F \in \Bbbk(t_1, \ldots, t_l)^n$).

For example, consider the circle $S^1 = \{(x, y) \in \mathbb{A}^2 \mid x^2 + y^2 = 1\} \subseteq \mathbb{A}^2$ (where $\Bbbk = \mathbb{R}$).

- On one hand, we therefore have that S^1 is *implicitly described* by the single equation $x^2+y^2-1 = 0$. More formally, this is to say that $S^1 = \mathcal{V}(f)$ where $f = x^2 + y^2 - 1 \in \Bbbk[x, y]$.
- On the other hand, consider the rational map $F : \mathbb{A}^1 \dashrightarrow \mathbb{A}^2$ defined by

$$F(t) = \Big(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\Big);$$

this map happens to be the inverse of the stereographic projection of the circle onto the x-axis via the pole $(0,1) \in \mathbb{A}^2$. Hence $\text{im}(F) \subseteq S^1$ and, taking for granted for the moment that in fact $\overline{\text{im}(F)} = S^1$, we therefore say that S^1 is *parametrically described* (i.e. "traced out") by F.

In this example, a couple additional things are worth pointing out. First, note that $(0,1) \in S^1 \setminus \text{im}(F)$, which is to say that this parametric description of S^1 is "imperfect" in some sense. Second, it is clear that, in this case, any rational map $\mathbb{A}^1 \dashrightarrow \mathbb{A}^2$ whose component maps were in fact just polynomials would have an unbounded image in $\mathbb{A}^2$ and therefore would not describe the circle. This latter observation motivates the need in general to consider parametrizations whose components are rational functions, not just polynomials.

These two distinct types of descriptions come with their own trade-offs, including most obviously the following. On one hand, an implicit description of a variety allows one to check for incidence with other varieties (including individual points) easily; namely, just plug your point into the system of implicit equations and check that it satisfies all of them. On the other hand, a parametric description of a variety allows you to easily generate points on the variety by simply traversing the domain of the given parametric function; hence parametric descriptions lend themselves very well to a use case like plotting portions of your variety.

Given these two distinct descriptions and their relative trade-offs, it is immediately clear that one might care to switch between them. The so-called "implicitization" (or "eliminating the parameter(s)") problem is of course then the problem of how to translate parametric equations into implicit equations; that is:

Given some finite system of rational parametric equations defining a rational map $F : \mathbb{A}^l \dashrightarrow \mathbb{A}^n$ in $\Bbbk(t_1, \ldots, t_l)^n$, provide a finite implicit description of the variety $V = \overline{\text{im}(F)}$.

0 Implicitization of rational planar curves

Although it is technically possible to tackle the implicitization problem in its aforementioned full generality, here we choose for the sake of brevity and simplicity to consider the problem at almost its simplest. Namely, we will consider only the implicitization problem for planar curves over an infinite field; that is, we suppose for the remainder of this expository paper that $\Bbbk$ is infinite and that $F : \mathbb{A}^1 \dashrightarrow \mathbb{A}^2 \in \Bbbk(t)^2$. Moreover, in practice, $\Bbbk$ is usually just a subfield of $\mathbb{C}$.

Now, as $F \in \Bbbk(t)^2$, we have that

$$\left(\frac{a(t)}{c(t)}, \frac{b(t)}{c'(t)}\right) = F(t) = F = \left(\frac{a}{c}, \frac{b}{c'}\right)$$

for some $a, b, c, c' \in \Bbbk[t]$, where both c and c' are nonzero. Moreover, by taking a common denominator and reducing the resulting fractions, we can assume without loss of generality that $c = c'$ and that $\gcd(a, b, c) = 1$. Finally, in this case we have that F is an uninteresting constant function if and only if $a, b, c \in \Bbbk$; hence we further suppose that at least one of a, b, or c is non-constant.

Now we can describe $V = \overline{\text{im}(F)}$ more precisely. In particular, setting

$$J = \langle cx - a, cy - b, cz - 1 \rangle \subseteq \Bbbk[z, t, x, y],$$

the Rational Implicitization Theorem (Theorem 3.3.2 in [CLO15]) then implies that $V = \mathcal{V}(J \cap \Bbbk[x, y])$. However, we will now show that we can do even better than this in our restricted setting, where we have only one parameter, t. In particular, setting also

$$I = \langle cx - a, cy - b \rangle \subseteq \Bbbk[t, x, y],$$

we will show that $I = J \cap \Bbbk[t, x, y]$ so that in turn $V = \mathcal{V}(I \cap \Bbbk[x, y])$. In order to do this, however, we must first establish a few lemmas.

Lemma 1. *We have that c is a unit modulo I.*

Proof. As $\gcd(a,b,c)=1$, it follows that $au+bv+cw=1\in\Bbbk[t]$ for some $u,v,w\in\Bbbk[t]$. Thus

$$c(w+xu+yv)=(au+bv+cw)+(cx-a)u+(cy-b)v\equiv 1 \pmod{I},$$

which is to say that c is indeed a unit modulo I. □

Lemma 2. *For each $f\in\Bbbk[t,x,y]$, there exists some integer $N\geq 0$ and some $g\in\Bbbk[t,x,y]$ such that $c^N f=g(t,cx,cy)$.*

Proof. Indeed, there are multiple ways to establish this. For example, setting $m=\deg_x f$, setting $n=\deg_y f$, and setting $N=m+n$, we then have that

$$f=\sum_{i=0}^{m}\sum_{j=0}^{n}\alpha_{ij}x^i y^j$$

for some such coefficients $\alpha_{ij}\in\Bbbk[t]$. Thus, setting

$$g=\sum_{i=0}^{m}\sum_{j=0}^{n}\alpha_{ij}c^{N-i-j}x^i y^j\in\Bbbk[t,x,y],$$

the result then follows by construction. □

Theorem 3. *We have that $J\cap\Bbbk[t,x,y]=I$.*

Proof. Clearly $I\subseteq J\cap\Bbbk[t,x,y]$; hence we only have left to show that $J\cap\Bbbk[t,x,y]\subseteq I$. To this end, let $f\in J\cap\Bbbk[t,x,y]$ be arbitrary. By lemma 2, there is some integer $N\geq 0$ and some $g\in\Bbbk[t,x,y]$ such that $c^N f=g(t,cx,cy)$. Applying the multivariate division algorithm to g using the lexicographic monomial order with $y>x>t$, it follows that

$$g=(x-a)p+(y-b)q+r$$

for some $p,q,r\in\Bbbk[t,x,y]$ such that no term of r is divisible by either of $\mathrm{LT}(x-a)=x$ or $\mathrm{LT}(y-b)=y$, and therefore in fact $r\in\Bbbk[t]$. Setting $\widetilde{p}=p(t,cx,cy)\in\Bbbk[t,x,y]$ and $\widetilde{q}=q(t,cx,cy)\in\Bbbk[t,x,y]$, it thus follows that

$$c^N f=(cx-a)\widetilde{p}+(cy-b)\widetilde{q}+r.$$

Evaluating both sides of the previous equation at

$$(z,t,x,y)=\Big(\frac{1}{c(t_0)},t_0,\frac{a(t_0)}{c(t_0)},\frac{b(t_0)}{c(t_0)}\Big)\in\Bbbk^4$$

for each $t_0\in\Bbbk\setminus c^{-1}(0)$ shows that $r(t_0)=0$. Thus, since $c\in\Bbbk[t]$ has finitely many roots and $\Bbbk$ is infinite by assumption, it follows that $r=0$ and therefore $c^N f\equiv 0 \pmod{I}$. Finally, since c is a unit modulo I by lemma 1, it follows that $f\equiv 0 \pmod{I}$, as required. □

With this established, to solve our particular implicitization problem, it is therefore sufficient to find a finite generating set for $I\cap\Bbbk[x,y]$.

1 Implicitization via Gröbner bases

Now that we understand the elimination ideal we are searching for, we can use Gröbner bases to solve our problem completely. In particular, the Elimination Theorem (Theorem 3.1.2 in [CLO15]) gives a direct algorithm for computing any elimination ideal. In this case, simply compute a Gröbner basis with respect to the lexicographic order with $t>x>y$ and then the finite collection of those basis elements that are missing the parameter t implicitly describe the curve.

For example, we can compute such a Gröbner basis corresponding to the earlier example parametrization for $V=S^1$ in *Macaulay2* as follows.

```
i1 : R = QQ[t, x, y, MonomialOrder => Lex];

i2 : {a, b, c} = (2*t, t^2 - 1, t^2 + 1);

i3 : gcd(a, gcd(b, c)) == 1

o3 = true

i4 : I = ideal(c*x - a, c*y - b);

o4 : Ideal of R

i5 : gens gb I

o5 = | x2+y2-1 ty-t+x tx-y-1 |

             1       3
o5 : Matrix R  <--- R
```

Observing that the only element of the computed Gröbner basis that is missing the parameter t is $x^2+y^2-1 \in \mathbb{Q}[x,y]$, it therefore follows that $x^2+y^2-1=0$ is an implicit description for $V=S^1$, as expected.

2 Implicitization via resultants

We can also use the theory of resultants to solve our problem in a slightly different way. Instead of determining a generating set for $I \cap \Bbbk[x,y]$ directly, we merely determine some $r \in \Bbbk[x,y]$ such that $\mathcal{V}(r) = \mathcal{V}(I \cap \Bbbk[x,y]) = V$. Such a polynomial r is called a resultant, and is defined precisely as follows.

Definition 4. *Let $f,g \in \Bbbk[t] \setminus \Bbbk$ be arbitrary, set $m = \deg f$, set $n = \deg g$, and let $L_{f,g}$ denote the $\Bbbk$-linear map defined by*

$$\begin{array}{rccccc} L_{f,g} & : & \Bbbk[t]_{n-1} & \oplus & \Bbbk[t]_{m-1} & \longrightarrow & \Bbbk[t]_{m+n-1} \\ & & h & \oplus & k & \longmapsto & f\,h + g\,k \end{array}$$

(where here $\Bbbk[t]_l$ denotes the vector space of polynomials of degree at most l). The Sylvester matrix *of f and g is defined to be the matrix $M \in M_{m+n}(\Bbbk)$ of $L_{f,g}$ with respect to the standard bases of its domain and codomain, and the* (Sylvester) resultant *of f and g, denoted by $\operatorname{Res}(f,g) = \operatorname{Res}(f,g;t)$, is defined to be $\operatorname{Res}(f,g;t) = \det(L_{f,g}) = \det(M) \in \Bbbk$.*

Now let $f,g \in \Bbbk[x_1,\ldots,x_n][t] \subseteq \Bbbk(x_1,\ldots,x_n)[t]$ be non-constant polynomials in t, set $r = \operatorname{Res}(f,g;t) \in \Bbbk(x_1,\ldots,x_n)$, and set $\mathfrak{a} = \langle f,g \rangle \subseteq \Bbbk[x_1,\ldots,x_n][t]$. In this context, we list some important facts about $r = \operatorname{Res}(f,g;t)$.

1. We in fact have that $r \in \Bbbk[x_1,\ldots,x_n]$ (Theorem 2.1.2 in [Sot26]).
2. There exist polynomials $p,q \in \Bbbk[x_1,\ldots,x_n][t]$ such that $\operatorname{Res}(f,g;t) = fp + gq \in \mathfrak{a}$ (Lemma 2.1.6 in [Sot26]).
3. As a consequence of the previous two facts, we therefore have that $r \in \mathfrak{a} \cap \Bbbk[x_1,\ldots,x_n]$ so that in turn $\mathcal{V}(\mathfrak{a} \cap \Bbbk[x_1,\ldots,x_n]) \subseteq \mathcal{V}(r) \subseteq \Bbbk^n$.
4. Most importantly, for each $(a_1,\ldots,a_n) \in \Bbbk^n$, if

   $$\deg_t f(a_1,\ldots,a_n,t) = \deg_t f \qquad \textit{or} \qquad \deg_t g(a_1,\ldots,a_n,t) = \deg_t g$$

   then $r(a_1,\ldots,a_n) = 0$ if and only if $f(a_1,\ldots,a_n,t)$ and $g(a_1,\ldots,a_n,t)$ have a common factor in $\Bbbk[t] \setminus \Bbbk$ (Theorem 2.1.2 in [Sot26]).

Now let us return to our particular problem by setting $f = cx - a \in \Bbbk[t, x, y]$ and $g = cy - b \in \Bbbk[t, x, y]$. Once again, in this restricted setting, we can do better than in general, as demonstrated by the following result.

Theorem 5. *We in fact have that* $V = \mathcal{V}(I \cap \Bbbk[x, y]) = \mathcal{V}(r)$.

Proof. We already have inclusion in one direction; we only have left to show that $\mathcal{V}(r) \subseteq \mathcal{V}(I \cap \Bbbk[x, y])$. Letting $(x_0, y_0) \in \mathcal{V}(r)$ and $h \in I \cap \Bbbk[x, y]$ be arbitrary, we will show that $h(x_0, y_0) = 0$, from which the result follows. First, since $h \in I$, we have that $h = (cx - a)p + (cx - b)q \in \Bbbk[t, x, y]$ for some $p, q \in \Bbbk[t, x, y]$. Setting $\widetilde{p} = p(t, x_0, y_0) \in \Bbbk[t]$ and $\widetilde{q} = q(t, x_0, y_0) \in \Bbbk[t]$, it then follows that

$$(cx_0 - a)\widetilde{p} + (cy_0 - b)\widetilde{q} = h(x_0, y_0) \in \Bbbk \subseteq \Bbbk[t].$$

Now, if, on one hand, we have either $\deg_t(cx_0 - a) = \deg_t(cx - a)$ or $\deg_t(cy_0 - b) = \deg_t(cy - b)$ then, as $(x_0, y_0) \in \mathcal{V}(r)$ and thus $r(x_0, y_0) = 0$, it follows that $cx_0 - a$ and $cy_0 - b$ have a common factor in $\Bbbk[t] \setminus \Bbbk$ and in turn a common root $t_0 \in \overline{\Bbbk}$, where $\overline{\Bbbk}$ is any algebraic closure of $\Bbbk$. Thus also $t_0 \in \overline{\Bbbk}$ is a root of

$$(cx_0 - a)\widetilde{p} + (cy_0 - b)\widetilde{q} = h(x_0, y_0) \in \Bbbk \subseteq \Bbbk[t] \subseteq \overline{\Bbbk}[t],$$

implying that indeed $h(x_0, y_0) = 0$, as the only constant polynomial with a root is the zero polynomial.

If, on the other hand, we have that both $\deg_t(cx_0 - a) < \deg_t(cx - a)$ and $\deg_t(cy_0 - b) < \deg_t(cy - b)$ then, setting

$$n = \max\{\deg_t a, \deg_t b, \deg_t c\},$$

it follows that $c_n x_0 - a_n = c_n y_0 - b_n = 0 \in \Bbbk$, where $a_n, b_n, c_n \in \Bbbk$ denote the coefficients of $t^n \in \Bbbk[t]$ in a, b, and c, respectively. Moreover, it cannot be that $c_n = 0$ as this would imply that also $a_n = 0 = b_n$, contradicting the definition of n. Thus defining $a^*(t) = t^n a(1/t) \in \Bbbk[t]$ and defining $b^*, c^* \in \Bbbk[t]$ in an identical manner, we have that

$$x_0 = \frac{a_n}{c_n} = \frac{a^*(0)}{c^*(0)} \in \Bbbk \qquad \text{and} \qquad y_0 = \frac{b_n}{c_n} = \frac{b^*(0)}{c^*(0)} \in \Bbbk.$$

We now define a number of maps. In particular,

- let $\mathrm{ev}_1 : \Bbbk[x, y] \to \Bbbk$ be the evaluation map characterized by $x \mapsto x_0$ and $y \mapsto y_0$,
- let $\mathrm{ev}_2 : \Bbbk[t] \to \Bbbk$ be the evaluation map characterized by $t \mapsto 0$,
- let $\mathrm{ev}_3 : \Bbbk[x, y] \to \Bbbk[t]_{\langle t \rangle}$ be the evaluation map characterized by $x \mapsto a^*(t)/c^*(t)$ and $y \mapsto b^*(t)/c^*(t)$,
- let $\mathrm{ev}_4 : \Bbbk[t, x, y] \to \Bbbk(t)$ be the evaluation map characterized by $t \mapsto 1/t$, $x \mapsto a^*(t)/c^*(t)$, and $y \mapsto b^*(t)/c^*(t)$,

and let i doubly denote the natural injections $\Bbbk[x, y] \to \Bbbk[t, x, y]$ and $\Bbbk[t]_{\langle t \rangle} \to \Bbbk(t)$. Furthermore, since $\ker \mathrm{ev}_2 = \langle t \rangle$, there exists, by the universal property of localization, a unique map $\widetilde{\mathrm{ev}}_2 : \Bbbk[t]_{\langle t \rangle} \to \Bbbk$ such that $\widetilde{\mathrm{ev}}_2 \circ i = \mathrm{ev}_2$.

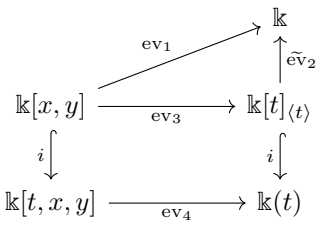
Now, since both

$$(\mathrm{ev}_4 \circ i)(x) = a^*(t)/c^*(t) = (i \circ \mathrm{ev}_3)(x) \qquad \text{and} \qquad \mathrm{ev}_1(x) = x_0 = a^*(0)/c^*(0) = (\widetilde{\mathrm{ev}}_2 \circ \mathrm{ev}_3)(x),$$

and similarly for $y \in \Bbbk[x, y]$, the universal property of polynomial rings implies that both

$$\mathrm{ev}_4 \circ i = i \circ \mathrm{ev}_3 \qquad \text{and} \qquad \mathrm{ev}_1 = \widetilde{\mathrm{ev}}_2 \circ \mathrm{ev}_3.$$

In other words, the following diagram commutes.



Thus, since $i(\mathrm{ev}_3(h)) = (\mathrm{ev}_4 \circ i)(h) = 0$ and i is injective, it follows that $\mathrm{ev}_3(h) = 0$ so that in turn

$$h(x_0, y_0) = \mathrm{ev}_1(h) = (\widetilde{\mathrm{ev}}_2 \circ \mathrm{ev}_3)(h) = \widetilde{\mathrm{ev}}_2(0) = 0$$

once again. □

Thus the implicitization problem in our restricted setting is solved (nearly) perfectly by the resultant, which, moreover, is straightforward to compute as it is just the determinant of an explicit linear map.

For example, we can compute the resultant corresponding to the earlier example parametrization for $V = S^1$ in *Macaulay2* as follows.

```
i1 : R = QQ[t, x, y];

i2 : {a, b, c} = (2*t, t^2 - 1, t^2 + 1);

i3 : M = sylvesterMatrix(c*x - a, c*y - b, t)

o3 = {-4} | x   -2  x   0   |
     {-3} | 0   x   -2  x   |
     {-4} | y-1 0   y+1 0   |
     {-3} | 0   y-1 0   y+1 |

              4       4
o3 : Matrix R  <--- R

i4 : det M

       2     2
o4 = 4x  + 4y  - 4

o4 : R

i5 : resultant(c*x - a, c*y - b, t)

       2     2
o5 = 4x  + 4y  - 4

o5 : R
```

Here we see that the implicit description for V is given by $4x^2 + 4y^2 - 4 = 0$, which is of course equivalent to our previous descriptions.

2.5 Moving line bases and implicitization

In order to present the ~~third~~ 2.5th and final implicitization method, we must first discuss the concept of moving lines and how they can be used for parametrizations and ideal bases.

Intuitively, a *moving line* is a line in affine space that varies with some parameter, say "t". A *moving line parametrization* of a curve is then two moving lines, which always intersect at a (moving) point, which in turn traces out the curve. Let us now formulate this more precisely in our restricted setting. Set $R = \Bbbk[t]$ and set

$$M = \{Ax + By + C \in R[x, y] \mid A, B, C \in R\} \subseteq R[x, y].$$

Thus M is the set of all lines (and constants) in $R[x, y]$; that is, the set of all moving lines in $\Bbbk[t][x, y]$. A moving line parametrization of V is then a pair of triples $(P_1, P_2, P_3), (Q_1, Q_2, Q_3) \in R^3$, corresponding

to a pair of moving lines

$$\left.\begin{array}{l} p = P_1 x + P_2 y + P_3 \\ q = Q_1 x + Q_2 y + Q_3 \end{array}\right\} \in M,$$

such that

$$\mathcal{V}(\langle p, q\rangle \cap \Bbbk[x, y]) = V.$$

And since, in our case, we have that $V = \mathcal{V}(I \cap \Bbbk[x, y])$, to show that some such p and q parametrize V, it suffices to show that $I = \langle p, q\rangle$. In this case, the pair (p, q) therefore forms an ideal "basis" (i.e. generating set) for I and so, since these elements are moving lines, we unsurprisingly call it a *moving line basis* for I.

In fact we already have a moving line basis for I; namely, the original generating set $(cx - a, cy - b)$ for I is precisely a set of moving lines, which we can visualize as always being parallel to the y- and x-axes, respectively, and whose intersection we concluded (via theorem 3) traces out V. The question, however, is whether it is possible to "do better"; namely, does there exist a moving line basis (p, q) for I where p and q have smaller degrees in t than $cx - a$ and $cy - b$? The answer turns out to be yes. In particular, setting $n = \max\{\deg a, \deg b, \deg c\}$, there then exist $p, q \in \Bbbk[t, x, y]$ with $I = \langle p, q\rangle$, such that

$$\deg_t p + \deg_t q = n = \max\{\deg_t(cx - a),\ \deg_t(cy - b)\},$$

as we will now show via the following results. First, we establish a lemma whose consequences are both important and illuminating.

Lemma 6. *For all $(A, B, C) \in R^3$, we have that $Ax + By + C \in I \iff Aa + Bb + Cc = 0 \in R$.*

Proof. Let $A, B, C \in R = \Bbbk[t]$ be arbitrary.

($\Longrightarrow$) Assume that $Ax+By+C \in I$ and consider the evaluation map $\operatorname{ev} : \Bbbk[t, x, y] \to \Bbbk(t)$ characterized by $x \mapsto a/c$, $y \mapsto b/c$, and $t \mapsto t$. By construction and the fact that $I = \langle cx - a, cy - b\rangle$, it follows that $I \subseteq \ker \operatorname{ev}$; thus

$$A\frac{a}{c} + B\frac{b}{c} + C = \operatorname{ev}(Ax + By + C) \in \operatorname{ev}(I) \subseteq \{0\}.$$

Multiplying through by $c \in \Bbbk(t)$ implies that also $Aa + Bb + Cc = 0 \in \Bbbk(t)$. Thus we in fact have $Aa + Bb + Cc = 0 \in \Bbbk[t]$, as required.

($\Longleftarrow$) Assume that $Aa + Bb + Cc = 0 \in R$, so that

$$c(Ax + By + C) = A(cx - a) + B(cy - b) + (Aa + Bb + Cc) \equiv 0 \pmod{I}.$$

As c is a unit modulo I by lemma 1, it follows that $Ax + By + C \equiv 0 \pmod{I}$, as required. □

Now observe that $M \subseteq R[x, y]$ is in fact a free R-module with R-basis $(x, y, 1)$ in $R[x, y]$; thus we have an R-module isomorphism

$$\begin{array}{rccc} \varphi \ : & R^3 & \xrightarrow{\sim} & M \\ & (A, B, C) & \longmapsto & Ax + By + C. \end{array}$$

Moreover, as a direct consequence of the previous result, we in turn have an R-module isomorphism

$$\varphi|_{\operatorname{Syz}(a,b,c)} : \operatorname{Syz}(a, b, c) \xrightarrow{\sim} I \cap M;$$

in other words, setting $\mathfrak{i} = \langle a, b, c\rangle \subseteq R$, it follows that $I \cap M$ is just a geometric manifestation of the syzygies of the generators a, b, and c for $\mathfrak{i}$.

We now homogenize everything. Set $\widetilde{R} = R[s] = \Bbbk[t, s]$, set $\widetilde{a} = s^n a(\frac{t}{s}) \in \widetilde{R}$, and define $\widetilde{b}, \widetilde{c} \in \widetilde{R}$ in an identical manner; thus $\widetilde{a}$, $\widetilde{b}$, and $\widetilde{c}$ are homogeneous polynomials of degree n. Set also $\widetilde{\mathfrak{i}} = \langle \widetilde{a}, \widetilde{b}, \widetilde{c}\rangle \subseteq \widetilde{R}$.

Lemma 7. *We have that $\mathcal{V}(\widetilde{a}, \widetilde{b}, \widetilde{c}) = \{(0, 0)\} \subseteq \mathbb{A}^2_{\overline{\Bbbk}}$ (note that this is affine space over $\overline{\Bbbk}$).*

Proof. On one hand, that $(0,0) \in \mathcal{V}(\widetilde{a},\widetilde{b},\widetilde{c})$ follows from the fact that $\widetilde{a}$, $\widetilde{b}$, and $\widetilde{c}$ are all homogeneous of degree $n > 0$.

On the other hand, let $(t_0, s_0) \in \mathcal{V}(\widetilde{a},\widetilde{b},\widetilde{c}) \subseteq \mathbb{A}^2_{\overline{\Bbbk}}$ be arbitrary.

We first show that $s_0 = 0$. Assuming for the sake of contradiction that $s_0 \neq 0$ then, since $\gcd(a,b,c) = 1$, it follows that $\mathcal{V}(a,b,c) = \mathcal{V}(1) = \emptyset \subseteq \mathbb{A}_{\overline{\Bbbk}}$; that is, we have that a, b, and c have no common roots in $\overline{\Bbbk}$. Thus one of

$$a(t_0/s_0), \quad b(t_0/s_0), \quad c(t_0/s_0) \quad \in \overline{\Bbbk}$$

is nonzero, so that also one of

$$\widetilde{a}(t_0,s_0) = s_0^n a(t_0/s_0), \qquad \widetilde{b}(t_0,s_0) = s_0^n b(t_0/s_0), \qquad \widetilde{c}(t_0,s_0) = s_0^n c(t_0/s_0)$$

is nonzero, contradicting the fact that $(t_0,s_0) \in \mathcal{V}(\widetilde{a},\widetilde{b},\widetilde{c})$.

Therefore indeed $s_0 = 0$. Now, since (at least) one of a, b, and c has degree n in t, it follows that (at least) one of $\widetilde{a}(t,s_0)$, $\widetilde{b}(t,s_0)$, $\widetilde{c}(t,s_0)$ is of the form $\alpha t^n \in \overline{\Bbbk}[t]$ for some $0 \neq \alpha \in \overline{\Bbbk}$. Since $(t_0,s_0) \in \mathcal{V}(\widetilde{a},\widetilde{b},\widetilde{c})$, it follows that $\alpha t_0^n = 0$, so that in turn $t_0 = 0$, as required. □

Lemma 8. *We have that $\widetilde{R}/\widetilde{\mathfrak{i}}$ is finite dimensional as a vector space over $\Bbbk$.*

Proof. Letting $G \subseteq \widetilde{\mathfrak{i}}$ be a Gröbner basis for $\widetilde{\mathfrak{i}}$, it follows that also G is a Gröbner basis for $\langle \widetilde{\mathfrak{i}} \rangle \subseteq \overline{\Bbbk}[t,s]$. Thus the $\overline{\Bbbk}$-basis of standard monomials for $\overline{\Bbbk}[t,s]/\langle \widetilde{\mathfrak{i}} \rangle$ is the same as the $\Bbbk$-basis of standard monomials for $\Bbbk[t,s]/\widetilde{\mathfrak{i}}$. Finally, since $\mathcal{V}(\langle \widetilde{\mathfrak{i}} \rangle)$ is a finite subset of $\mathbb{A}^2_{\overline{\Bbbk}}$ by lemma 7, the Finiteness Theorem (Theorem 5.3.6 in [CLO15]) implies that this collection of standard monomials is finite, and the result follows. □

We can now prove the main result.

Theorem 9. *There exist $p, q \in R[x,y]$ such that both $I = \langle p, q \rangle$ and $\deg_t p + \deg_t q = n$.*

Proof. First, by lemma 8, we have that $\widetilde{R}/\widetilde{\mathfrak{i}}$ is finite dimensional as a vector space over $\Bbbk$; thus there exists some integer $K \geq 0$ such that $\dim_{\Bbbk}((\widetilde{R}/\widetilde{\mathfrak{i}})_k) = 0$ for all integers $k \geq K$. Letting $\pi : \widetilde{R} \to \widetilde{R}/\widetilde{\mathfrak{i}}$ denote the projection map – which is a zero-degree graded map – it follows in particular for each integer $k \geq K$ that

$$\begin{aligned} k+1 = \binom{k+1}{1} &= \dim_{\Bbbk}(\widetilde{R}_k) \\ &= \dim_{\Bbbk}(\ker \pi_k) + \dim_{\Bbbk}(\operatorname{im} \pi_k) \\ &= \dim_{\Bbbk}(\widetilde{\mathfrak{i}}_k) + \dim_{\Bbbk}((\widetilde{R}/\widetilde{\mathfrak{i}})_k) \\ &= \dim_{\Bbbk}(\widetilde{\mathfrak{i}}_k) \end{aligned}$$

Next, let $\psi : \widetilde{R}(-n)^3 \to \widetilde{\mathfrak{i}}$ denote the zero-degree graded map characterized by mapping the three standard basis vectors to $\widetilde{a}$, $\widetilde{b}$, and $\widetilde{c}$, respectively. This gives an exact sequence

$$0 \longrightarrow \operatorname{Syz}(\widetilde{a},\widetilde{b},\widetilde{c}) \longrightarrow \widetilde{R}(-n)^3 \xrightarrow{\psi} \widetilde{R} \xrightarrow{\pi} \widetilde{R}/\widetilde{\mathfrak{i}} \longrightarrow 0,$$

which begins as a partial graded resolution of $\widetilde{R}/\widetilde{\mathfrak{i}}$ over $\widetilde{R}$ of length $1 = |\{t,s\}| - 1$. Hence the (refined) Graded Hilbert Syzygy Theorem (Theorem 6.3.15 in [CLO05]) implies that $\operatorname{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})$ is free; that is,

we have that $\mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c}) \cong \widetilde{R}(-d_1)\oplus\cdots\oplus\widetilde{R}(-d_m)$ for some $d_1,\ldots,d_m\in\mathbb{Z}$. Combining this fact with the previous result, we find for each integer $k \geq K$ that

$$\begin{aligned}
3k-3n+3 = 3\binom{k-n+1}{1} &= \dim_{\Bbbk}(\widetilde{R}(-n)^3_k) \\
&= \dim_{\Bbbk}(\ker\psi_k) + \dim_{\Bbbk}(\operatorname{im}\psi_k) \\
&= \dim_{\Bbbk}(\mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})_k) + \dim_{\Bbbk}(\widetilde{\mathfrak{i}}_k) \\
&= \dim_{\Bbbk}((\widetilde{R}(-d_1)\oplus\cdots\oplus\widetilde{R}(-d_m))_k) + \dim_{\Bbbk}(\widetilde{\mathfrak{i}}_k) \\
&= \Big(\sum_{j=1}^{m}(k-d_j+1)\Big) + k + 1 \\
&= k(m+1) + m + 1 - \sum_{j=1}^{m} d_j,
\end{aligned}$$

implying that $m=2$ and in turn that $d_1+d_2=3n$. Thus there exists some pair

$$(\widetilde{P_1},\widetilde{P_2},\widetilde{P_3}),(\widetilde{Q_1},\widetilde{Q_2},\widetilde{Q_3}) \in \mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c}) \subseteq \widetilde{R}^3,$$

with $(\widetilde{P_1},\widetilde{P_2},\widetilde{P_3}) \in \mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})_{d_1}$ and $(\widetilde{Q_1},\widetilde{Q_2},\widetilde{Q_3}) \in \mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})_{d_2}$, forming an $\widetilde{R}$-basis for $\mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})$. Thus also

$$(\widetilde{P_1},\widetilde{P_2},\widetilde{P_3}) \in \widetilde{R}(-n)^3_{d_1} = \widetilde{R}^3_{d_1-n} \qquad \text{and} \qquad (\widetilde{Q_1},\widetilde{Q_2},\widetilde{Q_3}) \in \widetilde{R}(-n)^3_{d_2} = \widetilde{R}^3_{d_2-n}.$$

Let $P_1,P_2,P_3,Q_1,Q_2,Q_3 \in R$ be the corresponding polynomials derived by evaluating at $s=1$ and set

$$\left.\begin{aligned} p = \varphi(P_1,P_2,P_3) = P_1x + P_2y + P_3 \\ q = \varphi(Q_1,Q_2,Q_3) = Q_1x + Q_2y + Q_3 \end{aligned}\right\} \in M\cap I,$$

which therefore generate $M\cap I$ as an R-module. Furthermore, assuming without loss of generality that $d_1-n \leq d_2-n$, it then follows that

$$\deg_t p = \max\{\deg_t P_1, \deg_t P_2, \deg_t P_3\} = d_1-n$$

as otherwise we would have a syzygy of homogeneous degree strictly smaller than that of the generators. This then implies that $\deg_t q = d_2-n$ so that

$$\deg_t p + \deg_t q = (d_1-n)+(d_2-n) = 3n-2n = n.$$

Finally, since $p,q\in M\cap I\subseteq I$, it follows that $\langle p,q\rangle \subseteq I$ and, since $cx-a, cy-b \in M\cap I \subseteq \langle p,q\rangle$, it follows that $I\subseteq\langle p,q\rangle$. □

In proving the previous result, we established that $\mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})$ is a free $\widetilde{R}$-module of rank 2 and that dehomogenizing any basis pair for this module derives such a moving line basis for I. Thus, as long as we can compute a basis pair for $\mathrm{Syz}(\widetilde{a},\widetilde{b},\widetilde{c})$, we essentially have a procedure for computing such a moving line basis.

Fortunately, software like *Macaulay2* is indeed capable of performing such a computation (although we will not investigate its algorithm for doing so here). For example, we can compute such a moving line basis corresponding (yet again) to the earlier example parametrization for $V=S^1$ in *Macaulay2* as follows.

```
i1 : S = QQ[t, s];

i2 : {a, b, c} = (2*t, t^2 - 1, t^2 + 1);

i3 : n = max apply({a, b, c}, f -> first degree f);

i4 : degreeNHomogenize = (f, s, n) -> s^(n - first degree f) * homogenize(f, s);

i5 : homogenizedPolys = apply({a, b, c}, f -> degreeNHomogenize(f, s, n));

i6 : L = syz matrix {homogenizedPolys}

o6 = {2} | t  -s |
     {2} | -s -t |
     {2} | -s t  |

             3       2
o6 : Matrix S  <--- S

i7 : T = S[x, y];

i8 : homogeneousMLBasis = matrix{{x, y, 1}} * substitute(L, T);

             1       2
o8 : Matrix T  <--- T

i9 : MLBasis = substitute(homogeneousMLBasis, {s => 1})

o9 = | tx-y-1 -x-ty+t |

             1       2
o9 : Matrix T  <--- T
```

Here we see that one moving line basis for I corresponding to theorem 9 is $(tx - y - 1, -x - ty + t)$. Surprisingly, these two elements of $\mathbb{k}[t, x, y]$ are in fact the other two elements of the Gröbner basis computed in section 1.

From here, given that our primary objective is to find an implicit description for V, we can simply compute the resultant of our new basis for I just like in section 2. Of course, the fact that we are relying on a previous method is why it is not entirely accurate to refer to moving line bases as a true third method for implicitization. To illustrate, we continue our previous *Macaulay2* session.

```
i10 : M = sylvesterMatrix(MLBasis_(0, 0), MLBasis_(0, 1), t)

o10 = {-1, -1} | x    -y-1 |
      {-1, -1} | -y+1 -x   |

               2       2
o10 : Matrix T  <--- T

i11 : det M

         2    2
o11 = - x  - y  + 1

o11 : T
```

Here we arrive at the equivalent implicit description $-x^2 - y^2 + 1 \in \Bbbk[x, y]$ for V. What is worth noting, however, is that the Sylvester matrix used to compute this resultant was significantly smaller, coming from the fact that the degrees in t of the new moving line basis are smaller than those of the original. At first glance, this is the reason why computing such a new basis could be desirable, and why one might consider this to be a "third" method for implicitization. That being said, such a distinction raises the obvious question of whether we are just offloading the computational load to the computation of the moving line basis itself (which in turn is presumably implemented using Gröbner bases) and therefore not actually yielding any computational improvement over the previous two methods. Further exploration of these reasonable questions is reserved for future study.

References

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015.

[Sot26] Frank Sottile. Algebraic geometry for applications. Available at https://franksottile.github.io/tmp/aga.pdf, March 3 2026.