El problema de no entrecruzamiento

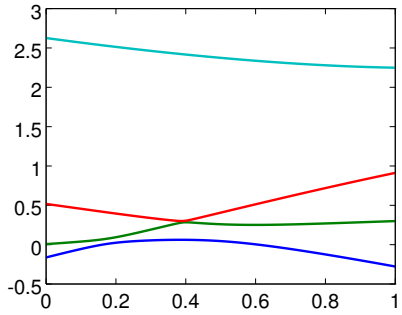
Fernando Chamizo

30 de noviembre de 2014

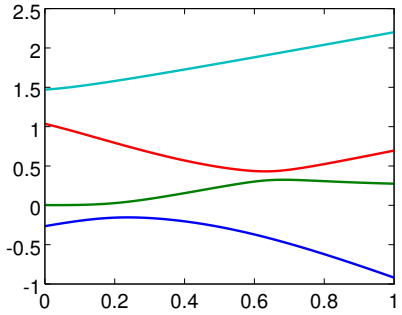
Consideremos la curva que une dos matrices $n \times n$ simétricas reales, A y B, de manera lineal. Es decir,

$$c(t) = (1-t)A + tB, \qquad t \in [0,1].$$

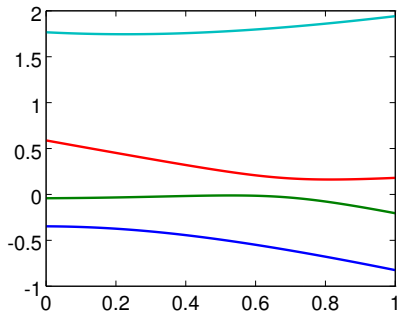
Los valores propios de $c(t)$ variarán de manera continua de los n de A a los n de B, y es fácil hacer un programa que genere matrices aleatoriamente y los pinte para $0 \le t \le 1$. El Programa 1 del Apéndice es una versión `matlab/octave`. Algunos ejemplos con $n = 4$ son:



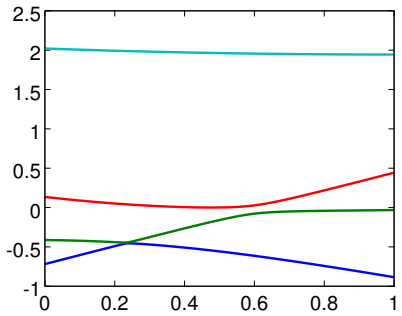
A = [0.9912 0.2037 0.8272 0.6759; 0.2037 0.4758 0.3991 0.5994; 0.8272 0.3991 0.8214 0.8411; 0.6759 0.5994 0.8411 0.7008]
B = [0.7425 0.7579 0.3891 0.4293; 0.7579 0.5730 0.8497 0.2763; 0.3891 0.8497 0.9635 0.0859; 0.4293 0.2763 0.0859 0.9047]



A = [0.4519 0.3334 0.0591 0.7409; 0.3334 0.1999 0.4272 0.1687; 0.0591 0.4272 0.9418 0.0172; 0.7409 0.1687 0.0172 0.6505]
B = [0.7266 0.0945 0.8776 0.0144; 0.0945 0.1799 0.9263 0.0682; 0.8776 0.9263 0.6513 0.8646; 0.0144 0.0682 0.8646 0.6944]



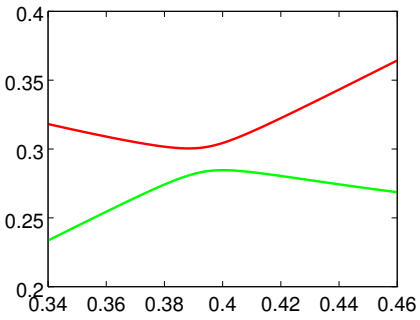
A = [0.0686 0.2994 0.5916 0.2033; 0.2994 0.7984 0.5017 0.6508; 0.5916 0.5017 0.6008 0.1125; 0.2033 0.6508 0.1125 0.4982]
B = [0.2776 0.6525 0.9173 0.5098; 0.6525 0.1973 0.1112 0.2974; 0.9173 0.1112 0.3115 0.6938; 0.5098 0.2974 0.6938 0.3065]

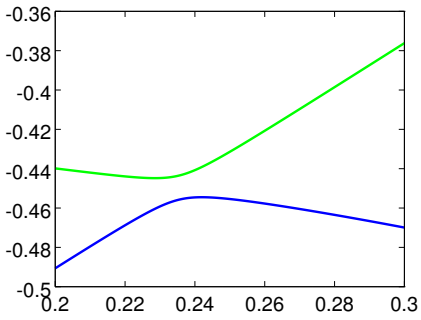


A = [0.1056 0.5938 0.2827 0.1552; 0.5938 0.2836 0.5508 0.8709; 0.2827 0.5508 0.1310 0.8337; 0.1552 0.8709 0.8337 0.5047]
B = [0.4050 0.1736 0.5752 0.6062; 0.1736 0.5199 0.9892 0.4899; 0.5752 0.9892 0.0348 0.2928; 0.6062 0.4899 0.2928 0.5111]

Olvidémonos de los colores (si es que el lector los aprecia en su copia) y pensemos que si tenemos n números que tienen que transformarse en otros n números, nadie ha decretado que lo hagan de manera ordenada. Es de esperar, por tanto que las curvas se corten con cierta probabilidad positiva. Algebraicamente, no hay nada que impida que dos valores propios coincidan al variar la t. Es más, parece razonable ensoñar algún tipo de teorema del punto fijo que asegure que esto ocurre bajo ciertas condiciones, igual que dos gráficas de funciones continuas $f : [0, 1] \longrightarrow \mathbb{R}$ se cortan siempre que $f(0) - g(0) < 0 < f(1) - g(1)$.

Las imágenes anteriores apoyan nuestra intuición pues en la primera y en la última se produce la intersección, o al menos eso parece... hasta que usamos la función de zoom del Programa 2 y observamos que están cerca pero no se llegan a tocar.





Jugando con el ordenador durante todo el tiempo que deseemos, notaremos que esta situación es general y bien misteriosa: es como si las curvas se vieran unas a otras y que en el último momento, antes de chocarse, se esquivaran.

Este fenómeno parece ser que surgió en el contexto de la mecánica cuántica (allí los *observables* son operadores autoadjuntos) y que fue explicado por J. von Neumann y E. P. Wigner en un antiguo artículo [vNW29]. Sin embargo, es muy poco conocido dentro de la comunidad matemática, salvo que está explicado sucintamente en el original libro de P. Lax de álgebra lineal [Lax07] e incluso sirve para el diseño de su portada.

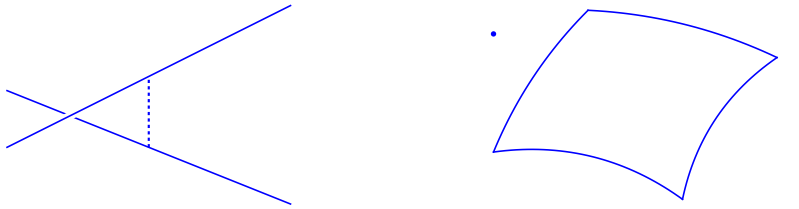
El problema matemático

Es posible construir ejemplos en los que haya entrecruzamiento. Uno de los más drásticos consiste en tomar $B = -A$, que para $t = 1/2$ da la matriz nula, coincidiendo todos los valores propios. También es frecuente que se produzcan entrecruzamientos si A y B son matrices diagonales. Lo que sucede es que estos ejemplos son comparativamente tan escasos que en la práctica es imposible que el ordenador encuentre uno al generar matrices al azar. En un intento de simular `rand(4)` en `matlab/octave`, pensemos por ejemplo que si los elementos de una matriz simétrica 4×4 siguen distribuciones independientes $U(0, 1)$, la probabilidad de que una matriz escogida aleatoriamente sea diagonal con una precisión de seis decimales es 10^{-36}.

Posiblemente es difícil hacer un teorema elegante que especifique el "azar" sobre los coeficientes y cuantifique la minúscula probabilidad de los contraejemplos (quizá eso explica que los autores matemáticos no hayan hablado del fenómeno). Por ello, con razonamientos

intuitivos, vamos a derivar el problema a otro sobre dimensiones, entendidas como el número de parámetros libres que necesitamos para describir un objeto.

Nuestra intuición del álgebra lineal y geométrica de baja dimensión, nos dice que dos objetos en $\mathbb{R}^N$ (o en otro espacio de dimensión N) no se cortan en general cuando sus dimensiones d_1 y d_2 cumplen $d_1 + d_2 < N$. Por ejemplo, es "imposible" en cierto sentido probabilista que dos rectas escogidas al azar se corten en $\mathbb{R}^3$ porque $d_1 = d_2 = 1$ y $N = 3$. Por otro lado, una recta y un plano $d_1 = 1$, $d_2 = 2$, típicamente sí tienen un punto en común.



En nuestro caso, cuando A y B se han escogido al azar, la curva $c(t)$ debería ser un objeto genérico de dimensión $d_1 = 1$. El espacio ambiente es el de matrices simétricas reales $S_n(\mathbb{R})$, que tiene dimensión (contando los elementos en la diagonal principal y por encima de ella)

$$\dim S_n(\mathbb{R}) = N \qquad \text{con} \qquad N = n + (n-1) + \cdots + 2 + 1 = \frac{n(n+1)}{2}.$$

Los contraejemplos que queremos evitar son

$$\mathcal{M}_n = \big\{ M \in S_n(\mathbb{R}) \text{ con algún valor propio repetido} \big\}.$$

Entonces el extraño fenómeno quedará explicado si probamos

$$\boxed{\dim \mathcal{M}_n < \frac{n(n+1)}{2} - 1}. \tag{1}$$

Ahora es el momento de darle la oportunidad al lector de que determine por sí mismo $\dim \mathcal{M}_n$, siempre entendida de manera un poco imprecisa como el número de parámetros libres necesarios para describir $\mathcal{M}_n$. Si no da con ella, la solución errónea que veremos a continuación, puede servir de pista.

Una solución errónea y el caso bidimensional

Para evitar que el lector que acepte el reto de calcular $\dim \mathcal{M}_n$ se tope sin querer con la solución a renglón seguido, intercalamos esta sección que, por otra parte, responde al primer impulso cuando uno se enfrenta al problema.

Cuanto mayor sea la multiplicidad requerida de los valores propios de una matriz, más condiciones estaremos imponiendo, por tanto $\dim \mathcal{M}_n = \dim \mathcal{M}_n^*$ donde

$$\mathcal{M}_n^* = \big\{ M \in \mathcal{M}_n \ : \ M \text{ tiene un valor propio doble y los demás simples} \big\}.$$

Fijémonos en el caso en que el valor propio doble es nulo:

$$\mathcal{M}_n^{0*} = \big\{ M \in \mathcal{M}_n^* \ : \ 0 \text{ es valor propio doble de } M \big\}.$$

Cada $M \in \mathcal{M}_n^*$ se escribe de forma única como $M = \lambda I + M_0$ donde $M_0 \in \mathcal{M}_n^{0*}$ y λ representa el valor propio doble. Entonces

$$\dim \mathcal{M}_n = 1 + \dim \mathcal{M}_n^{0*}. \tag{2}$$

Ahora bien, dada $M \in S_n(\mathbb{R})$, se tiene $M \in \mathcal{M}_n^{0*}$ si y sólo si los dos últimos coeficientes del polinomio característico (y no el antepenúltimo) son nulos. Esto da lugar a dos ecuaciones polinómicas para los elementos de M y sugiere

$$\dim \mathcal{M}_n^{0*} \overset{(?)}{=} \frac{n(n+1)}{2} - 2 \qquad \text{y por tanto} \qquad \dim \mathcal{M}_n \overset{(?)}{=} \frac{n(n+1)}{2} - 1, \tag{3}$$

que contradice (1).

Veamos qué sucede en el caso $n = 2$ para explicar esta paradoja. Se tiene

$$\mathcal{M}_2^{0*} = \left\{ \begin{pmatrix} a & b \\ b & d \end{pmatrix} \ : \ a, b, d \in \mathbb{R}, \quad a + d = 0, \quad ad - b^2 = 0 \right\}.$$

Las ecuaciones que definen este conjunto se reescriben como $a = -d$, $-d^2 - b^2 = 0$ y esta última equivale a $d = 0$, $b = 0$. En definitiva, las dos ecuaciones se transforman en tres y resulta que $\mathcal{M}_2^{0*}$ sólo contiene la matriz nula. De aquí, las igualdades (3) no son correctas para $n = 2$, teniéndose que reemplazar por $\dim \mathcal{M}_2^{0*} = 0$ y $\dim \mathcal{M}_2 = 1$, que ya cae dentro de las hipótesis de (1).

Parece que la disminución en una unidad de $\dim \mathcal{M}_n$ frente a lo previsto en (3) ha sido una casualidad en el caso $n = 2$ fruto de la particular forma de las ecuaciones pero no puede ser así si confiamos en la veracidad de (1).

Una solución correcta

Vamos a calcular el número de parámetros necesarios para describir $\mathcal{M}_n^{0*}$ con $n > 2$. Fijada la base canónica se pueden identificar las matrices de $\mathcal{M}_n^{0*}$ con aplicaciones lineales autoadjuntas con un valor propio nulo doble. Damos por hecho que el lector recuerda que las aplicaciones autoadjuntas tienen autoespacios ortogonales.

Tras esta identificación, para cualquiera de las aplicaciones lineales L en $\mathcal{M}_n^{0*}$ consideramos el subespacio $W \subset \mathbb{R}^n$ generado por una base ortonormal de vectores propios

$B = \{\vec{v}_i\}_{i=1}^{n-2}$ con $L\vec{v}_i = \lambda_i \vec{v}_i$, $\lambda_i \neq 0$. Su complemento ortogonal es el autoespacio correspondiente al valor propio nulo y en este autoespacio bidimensional, L es la aplicación nula según el análisis del caso $n = 2$ en el apartado anterior.

Dada L, la base ortonormal B está determinada salvo el signo y la ordenación de sus elementos (porque los valores propios son simples) y lo mismo ocurre con $\{\lambda_i\}_{i=1}^{n-2}$ salvo su ordenación. Recíprocamente, dada una base ortonormal $B = \{\vec{v}_i\}_{i=1}^{n-2}$ y $\{\lambda_i\}_{i=1}^{n-2}$ números reales no nulos distintos, la aplicación

$$L(\vec{x}) = \sum_{i=1}^{n-2} \lambda_i \langle \vec{v}_i, \vec{x} \rangle \vec{x}$$

está en $\mathcal{M}_n^{0*}$ y tiene a $\{\vec{v}_i\}_{i=1}^{n-2}$ y $\{\lambda_i\}_{i=1}^{n-2}$ como vectores propios y valores propios correspondientes.

Podemos elegir $\vec{v}_1$ libremente en S^{n-1} (de dimensión $n-1$), tras ello, por la ortonormalidad, $\vec{v}_2$ debe estar en la intersección de S^n con el hiperplano $\langle \vec{v}_1, \vec{x} \rangle = 0$ que es como S^{n-2} (de dimensión $n-2$) y así se puede proceder inductivamente hasta $\vec{v}_2$ que debe estar en un conjunto bidimensional identificable con S^2. Si añadimos los $n-2$ grados de libertad que corresponden a la elección de los valores propios, se tiene

$$\dim \mathcal{M}_n^{0*} = (n-1) + (n-2) + \cdots + 3 + 2 + (n-2) = \frac{n(n+1)}{2} - 3$$

que tras (2) implica

$$\boxed{\dim \mathcal{M}_n = \frac{n(n+1)}{2} - 2} \tag{4}$$

y confirma (1).

Un poco de geometría algebraica computacional

Habíamos considerado $\mathcal{M}_n^*$ en lugar de $\mathcal{M}_n$ para evitar singularidades correspondientes a más coincidencias entre valores propios. Volvamos ahora al conjunto original para hacernos preguntas sobre las ecuaciones que lo definen y la naturaleza de las singularidades, además nos servirán como excusa para dar introducir unas someras pinceladas de geometría algebraica en su vertiente más computacional. Una vez resuelto el problema, esta larga sección es un lujo que nos aleja un poco del enunciado original pero que puede resultar instructivo aunque sólo sea por mostrar el tipo de cálculos computacionales, hoy en día triviales, q ue asombrarían a nuestros inmediatos predecesores. Aquí nos centramos en `Sage` que tiene la ventaja de ser sencillo y de ámbito general. Otros paquetes más específicos son más eficientes en los cálculos de geometría algebraica.

Identificando las matrices simétricas reales con $\mathbb{R}^{n(n+1)/2}$, se tiene

$$\mathcal{M}_n = \left\{ (a_{ij})_{1=i\leq j\leq n} \in \mathbb{R}^{n(n+1)/2} \ : \ \operatorname{rang}(a_{ij} - \lambda \delta_{ij}) \leq n-2 \text{ para algún } \lambda \right\}$$

donde δ_{ij} es la *delta de Kronecker* (los elementos de la matriz identidad) y en el cálculo del rango se supone $a_{ij} = a_{ji}$.

En geometría algebraica, fijado un cuerpo K, un *conjunto algebraico* en $\mathbb{A}^n_K$ es simplemente un subconjunto de K^n definido por ecuaciones polinómicas. La notación habitual en este contexto es referirse a K^n como $\mathbb{A}^n_K$ para intentar distinguir el espacio vectorial K^n de su estructura de espacio afín representado por $\mathbb{A}^n_K$, pero como conjuntos son exactamente lo mismo.

Siguiendo con la terminología, el *ideal de un conjunto algebraico* C en $\mathbb{A}^n_K$ es el ideal en $K[x_1, x_2, \ldots, x_n]$ formado por los polinomios que se anulan en C, esto es,

$$\mathbf{I}(C) = \big\{P \in K[x_1, x_2, \ldots, x_n] \ : \ P(a_1, a_2, \ldots, a_n) = 0, \quad \forall (a_1, a_2, \ldots, a_n) \in C\big\}.$$

Recíprocamente, se define el *conjunto de ceros de un ideal* $I \subset K[x_1, x_2, \ldots, x_n]$ como el conjunto algebraico

$$\mathbf{V}(I) = \big\{(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n_K \ : \ P(a_1, a_2, \ldots, a_n) = 0, \quad \forall P \in I\big\}.$$

Ideal de eliminación y resultante

Nos preguntamos si $\mathcal{M}_n$ viene dado por ecuaciones polinómicas. Es decir, con la notación recién introducida, si es un conjunto algebraico en $\mathbb{A}^{n(n+1)/2}_{\mathbb{R}}$. La condición $\operatorname{rang}(a_{ij} - \lambda\delta_{ij}) \leq n-2$ se traduce en que todos los menores de orden $n-1$ se anulen, lo que lleva a una serie de ecuaciones polinómicas en los a_{ij} pero también en λ. El problema que surge es si es posible eliminar esta última variable sin perder ninguna información. En términos algebraicos esto es lo que se llama el (primer) *ideal de eliminación* [CLO07]. Dado un ideal de polinomios, es el subideal formado por los polinomios que no contienen cierta variable seleccionada.

La manera de construir este ideal de eliminación está estrechamente ligada al concepto clásico de *resultante* que aparece y reaparece en multitud de contextos. El tema está muy bien tratado en [CLO07, Ch.3]. Aquí sólo veremos la idea a través de un ejemplo concreto. Supongamos que tenemos que resolver el sistema no lineal de ecuaciones:

$$\begin{cases} 21x^3 - 49x^2y + 13y^3 + 15 = 0 \\ x^2 - 3xy - 3y^2 + 5 = 0 \end{cases} \tag{5}$$

El procedimiento ingenuo de despejar y sustituir choca con que la solución de la ecuación de segundo grado, y mucho más la de tercer grado, llevaría a complejos cálculos sin atisbos de acercarnos a la solución. Llamemos F y G a los polinomios que definen las ecuaciones de (5), respectivamente, y consideremos la expresión

$$(a_0x + a_1)F + (b_0x^2 + b_1x + b_2)G.$$

Al operar, los coeficientes de $1, x, x^2, x^3, x^4$ son expresiones lineales en a_0, a_1, b_0, b_1, b_2 con coeficientes que son polinomios en y. El determinante de dicho sistema es la *resultante*. En nuestro caso, el Programa 3 en `Sage` nos da al instante

$$R = -12725y^6 + 74200y^4 + 6375y^3 - 116375y^2 - 6825y + 55350.$$

La identidad de Bezout para polinomios coprimos corresponde a resolver el sistema con coeficientes $1, 0, 0, 0, 0$ para $1, x, x^2, x^3, x^4$ y la anulación de R se revela como la obstrucción a que se pueda llevar a cabo esto con éxito. Resolviendo por la regla de Cramer y multiplicando por R se encuentran dos polinomios explícitos $A = A(x, y)$ y $B = B(x, y)$ tales que

$$AF + BG = R \qquad \text{con } \deg_x A = 1,\ \deg_x B = 2.$$

Si F y G se anulan en (x_0, y_0), entonces R se anula. Recíprocamente, si R se anula para cierto y_0 entonces $F(x, y_0)$ y $G(x, y_0)$ tienen factores en común como polinomios en x porque la identidad de Bezout para coprimos es imposible. De esta forma, $\langle R\rangle$ es el ideal de eliminación de $\langle F, G\rangle$. De cara a resolver (5), el problema se vuelve tan fácil o difícil como resolver polinomios de una variable. Factorizando R (lo cual ya lo hace Programa 3) se tiene

$$R = -25(y-2)(y-1)^2(509y^3 + 2036y^2 + 2631y + 1107).$$

Sustituyendo $y = 2$, $y = 1$ en (5) se obtienen las soluciones $(-1, 2)$, $(2, 1)$ y $(1, 1)$. El factor de tercer grado se puede tratar con métodos numéricos y obtener (ver el Programa 4) las soluciones aproximadas $(0.76232410, -1.7973767)$, $(-0.31726294, -1.1549067)$, $(-2.4450612, -1.0477166)$.

En `Sage` calcular el ideal de eliminación se reduce a una instrucción aunque puede ser muy poco eficiente cuando aumenta el número de variables. Utilizando el Programa 5 (seguido del Programa 6 para imprimir el resultado) se calculan generadores de $\mathbf{I}(\mathcal{M}_3)$ llegándose a que $\mathcal{M}_3$ es el conjunto algebraico

$$\mathcal{M}_3 = \Big\{(y_1, y_2, \ldots, y_6) \in \mathbb{R}^6 \ :\ P_1 = P_2 = P_3 = P_4 = P_5 = P_6 = P_7 = 0\Big\}$$

donde escribimos $y_1 = a_{11}$, $y_2 = a_{12}$, $y_3 = a_{13}$, $y_4 = a_{22}$, $y_5 = a_{23}$, $y_6 = a_{33}$ y

$$\begin{aligned}
P_1 &= y_2y_3y_4 - y_2^2y_5 + y_3^2y_5 - y_2y_3y_6\\
P_2 &= y_3^3 + y_1y_3y_4 - y_3y_4^2 - y_1y_2y_5 + y_2y_4y_5 - y_3y_5^2 - y_1y_3y_6 + y_3y_4y_6\\
P_3 &= y_2y_3^2 - y_1y_3y_5 + y_3y_4y_5 - y_2y_5^2\\
P_4 &= y_2^2y_3 - y_1y_2y_5 - y_3y_5^2 + y_2y_5y_6\\
P_5 &= y_1y_2y_3 - y_1^2y_5 - y_2^2y_5 + y_1y_4y_5 + y_5^3 - y_2y_3y_6 + y_1y_5y_6 - y_4y_5y_6\\
P_6 &= y_2^3 - y_1y_2y_4 - y_1y_3y_5 - y_2y_5^2 + y_1y_2y_6 + y_2y_4y_6 + y_3y_5y_6 - y_2y_6^2\\
P_7 &= y_1y_2^2 - y_1y_3^2 - y_1^2y_4 - y_2^2y_4 + y_1y_4^2 + y_4y_5^2 + y_1^2y_6 + y_3^2y_6 - y_4^2y_6 - y_5^2y_6 - y_1y_6^2 + y_4y_6^2
\end{aligned}$$

No es casual que los polinomios P_i muestren ciertas simetrías, porque $\mathcal{M}_3$ también las tiene. Por ejemplo, $(y_1, y_2, y_3, y_4, y_5, y_6) \in \mathcal{M}_3$ implica $(y_1, y_3, y_2, y_6, y_5, y_4) \in \mathcal{M}_3$ pensando un cambio de base que consiste en intercambiar los ejes Y y Z, lo que no modifica el rango ni la simetría.

El diccionario de la geometría algebraica

La motivación para introducir el ideal de un conjunto algebraico y el conjunto de ceros de un ideal es abordar algebraicamente problemas geométricos: el propósito fundamental de la geometría algebraica.

A pesar de que los dos conceptos tienen una formulación simétrica, basta pensar un poco para encontrar ejemplos en los que $\mathbf{I}$ no invierte a $\mathbf{V}$. Por ejemplo, $I = \langle x^2 + y^2 \rangle$ cumple $\mathbf{V}(I) = \{(0,0)\}$ en $\mathbb{A}^2_{\mathbb{R}}$, sin embargo $\mathbf{I}\big(\{(0,0)\}\big)$ no es I sino un ideal más grande en $\mathbb{R}[x,y]$, el de todos los polinomios sin término independiente. Esto sucede porque $\mathbb{R}$ no es algebraicamente cerrado, en $\mathbb{R}$ no se pueden resolver todas las ecuaciones algebraicas y se pierde información. Si estuviéramos en $\mathbb{C}$, se factorizaría $x^2 + y^2 = (x - iy)(x + iy)$ y el conjunto de ceros en $\mathbb{A}^2_{\mathbb{C}}$ sería la unión de dos rectas, $\mathbf{V}(I) = \{(iy, y)\} \cup \{(-iy, y)\}$, cumpliéndose $\mathbf{I}\big(\mathbf{V}(I)\big) = I$.

En $\mathbb{A}^2_{\mathbb{C}}$ todavía encontramos contraejemplos como $I = \langle (x - y)^2 \rangle$ pues en este caso $\mathbf{V}(I) = \{(x, x)\}$ y por tanto $\mathbf{I}\big(\mathbf{V}(I)\big) = \langle x - y \rangle \neq I$. La explicación aquí es que $(x-y)^2 = 0$ no añade nada nuevo a $x-y = 0$ porque simplemente estamos elevando cero a una potencia. Con el propósito de eliminar este caso, dado un ideal I en un anillo R se define su *radical* como

$$\operatorname{rad}(I) = \big\{ r \in R \ : \ r^n \in I \text{ para algún } n \in \mathbb{Z}^+ \big\}.$$

Como en la aritmética usual, el radical quita las potencias, por ejemplo $\operatorname{rad}\big(\langle (x-y)^2 \rangle\big) = \langle x - y \rangle$. Se dice que I es *radical* si $\operatorname{rad}(I) = I$.

El *teorema de los ceros de Hilbert* (véase una prueba en [Hul03]), muy conocido también como *Nullstellensatz*, afirma que en cuerpos algebraicamente cerrados $\mathbf{I}\big(\mathbf{V}(I)\big) = \operatorname{rad}(I)$, es decir, que para ideales radicales, $\mathbf{I}$ invierte a $\mathbf{V}$. Por otro lado, $\mathbf{V}\big(\mathbf{I}(C)\big) = C$ es trivial. Esto permite establecer las siguientes biyecciones que conforman un reflejo algebraico en $K[x_1, x_2, \ldots, x_n]$ de la geometría en $\mathbb{A}^n_K$:

$$\begin{aligned} \{\text{ideales radicales}\} &\longleftrightarrow \{\text{conjuntos algebraicos}\} \\ \{\text{ideales primos}\} &\longleftrightarrow \{\text{variedades algebraicas}\} \\ \{\text{ideales maximales}\} &\longleftrightarrow \{\text{puntos}\} \end{aligned}$$

Aquí las *variedades algebraicas* (afines) son los conjuntos algebraicos que no son unión de otros conjuntos algebraicos propios. Por ejemplo, $x - y = 0$ define una variedad algebraica mientras que $x^2 - y^2 = 0$ sólo un conjunto algebraico, porque es unión de las rectas $x - y = 0$ y $x + y = 0$. Algunos autores llaman variedades algebraicas a todos los conjuntos algebraicos, especificando, si es necesario, si son *irreducibles*, es decir que no son uniones de otros.

El Programa 5 al mostrar como salida `True` en la última línea, muestra algebraicamente que $\mathcal{M}_3$ es de una pieza como conjunto algebraico complejo, no proviene de pegar distintas variedades.

Singularidades

En las variedades algebraicas se permiten singularidades (a diferencia de lo que ocurre en el contexto de la geometría diferencial) porque sólo imponemos que vengan definidas por ecuaciones polinómicas y la regularidad de las ecuaciones no garantiza la del conjunto algebraico correspondiente. En el caso de curvas en $\mathbb{A}^2_{\mathbb{R}}$, pensamos por ejemplo en $y^2 - x^3 = 0$ que tiene una cúspide en el origen a pesar de que $y^2 - x^3$ es todo lo derivable que queramos en ambas variables.

En geometría algebraica, la no singularidad en un punto p de una variedad algebraica de dimensión n se define habitualmente como $\dim \mathfrak{m}_p/\mathfrak{m}_p^2 = n$ donde $\mathfrak{m}_p$ es el ideal maximal formado por todos los polinomios (en realidad funciones racionales) que se anulan en p. Esta manera de caracterizar las singularidades es más adecuada para tratar con ellas algebraicamente. A pesar del lenguaje alambicado, lo que indica $\mathfrak{m}_p/\mathfrak{m}_p^2$ en última instancia es que quitemos los términos de orden mayor que dos en el desarrollo de Taylor (se anulan al tomar el cociente por $\mathfrak{m}_p^2$) y entonces vemos las derivadas. Por ello en $\mathbb{A}^n_{\mathbb{R}}$ o en $\mathbb{A}^n_{\mathbb{C}}$ recuperamos nociones similares a las conocidas.

Digamos que el ideal de una variedad algebraica de dimensión n definida en $\mathbb{A}^N_{\mathbb{C}}$ está generado por las coordenadas de $F = (f_1, f_2, \ldots, f_m)$. Para que un punto no sea singular debemos tener suficientes vectores independientes como para generar el espacio tangente. Es decir, tantos como la dimensión de la variedad, y la variedad es no singular en un punto p cuando

$$n = \dim \ker DF(p) = N - \text{rang}DF(p)$$

donde DF es la matriz jacobiana. En el ejemplo inicial de la curva, $DF = (-3x^2, 2y)$ que tiene rango 1 excepto en el origen. El lector atento habrá observado que hay un cabo suelto y es que lo anterior apela a la dimensión de la variedad que no hemos definido. Hacerlo en términos algebraicos a partir de las propiedades del ideal no es sencillo [CLO07, Ch.9] pero de nuevo en $\mathbb{C}$ podemos tomar un atajo [Hul03, Ch.3] y, con la notación anterior, definir la dimensión como el mínimo valor de $\dim \ker DF(p)$. Es decir, pensamos que en los puntos singulares (que son excepcionales) hay más "tangentes" que las habituales.

Hay cierta necesidad de trabajar con el ideal más que con las ecuaciones para evitar problemas con los ideales no radicales. Por ejemplo, si definimos la recta $y = x$ con la ecuación $(x-y)^2 = 0$ la jacobiana nula en el origen. Respecto a la dimensión, es importante trabajar en el contexto de variedades porque un conjunto algebraico puede ser unión de variedades de diferente dimensión. Por ejemplo $\{zx = 0, zy = 0\}$ es la unión del plano XY (dimensión 2) con el eje Z (dimensión 1).

Las únicas matrices simétricas reales 3×3 con tres valores propios iguales son múltiplos de la identidad. Estos son los "puntos" de $\mathcal{M}_3$ que completan $\mathcal{M}_3^*$. Estudiemos si son singulares. Según lo anterior, tenemos que calcular el rango de DF con $F = (P_1, P_2, \ldots, P_7)$ en el punto $(a, 0, 0, a, 0, a)$. El Programa 7 hace este cálculo y devuelve 0, por tanto la jacobiana es nula en estos puntos que por consiguiente son muy singulares. Posiblemente lo mismo se aplica en $\mathcal{M}_n$ para cualquier n.

Acerca del número de ecuaciones y de generadores

Si calculamos la resultante de P y P' con P un polinomio de una variable o pensando que el resto están congeladas (y la derivada es parcial), obtendremos una expresión que se anula cuando P tiene una raíz doble. Salvo por un factor constante, esto es lo que se llama el *discriminante* [Hul03, §4.3].

Podríamos caracterizar entonces $\mathcal{M}_n$ imponiendo que el discriminante de su polinomio característico sea nulo. Esto da lugar a una sola ecuación polinómica en los (a_{ij}) y vuelve a sugerir, como en la solución errónea, que $\dim \mathcal{M}_n = n(n+1)/2 - 1$, lo cual es falso. La

explicación a esta paradoja es que este discriminante es suma de cuadrados y al trabajar en $\mathbb{R}$ esa única ecuación se desdobla en otras, una por cada cuadrado. En [Lax98] se trata el problema, aunque ya en [Ily92] se había probado que es posible obtener de esta forma $n!$ ecuaciones. Para $n = 3$ esto son 6 ecuaciones que reducen las 7 que hemos dado nosotros escogiendo generadores del ideal $\mathbf{I}(\mathcal{M}_3)$.

En cualquier caso, como $\dim \mathcal{M}_3 = 4$ y $\mathcal{M}_3 \subset \mathbb{A}^6_{\mathbb{R}}$, sería de sospechar que dos ecuaciones son suficientes porque cada una impone una ecuación. Este tipo de argumentos son incorrectos en geometría algebraica, y las siguientes líneas tratan de ilustrar mínimamente la complejidad de la situación.

El ideal de un conjunto algebraico C nos da todas las posibles ecuaciones de conjuntos algebraicos que contiene a C, por tanto es natural pensar que un sistema de ecuaciones que defina C sin "redundancias", genera el ideal. Por ejemplo, $C_1 = \{(0,0)\}$ y $C_2 = \{(t,t^2)$, en $\mathbb{A}^2_{\mathbb{C}}$ están determinados por los conjuntos de ecuaciones $\{x = 0,\ y = 0\}$ y $\{y - x^2 = 0\}$. Se tiene $\mathbf{I}(C_1) = \langle x, y\rangle$, como ya habíamos indicado. Por otro lado, el algoritmo de la división da $P(x,y) = (y-x^2)C(x,y)+R(x)$ y $P \in \mathbf{I}(C_2)$ si y sólo si $R = 0$, es decir, $\mathbf{I}(C_2) = \langle y - x^2\rangle$.

Sin embargo, esta primera idea de que el número de generadores del ideal sea el número de ecuaciones y que las propias ecuaciones pueden servir de generadores, es falsa. Por ello, $\mathcal{M}_3$ admite 6 ecuaciones aunque su ideal posiblemente no admita menos de 7 generadores.

Para comprobar que el número de generadores del ideal puede ser mayor que el de ecuaciones, es decir, que hay polinomios que se anulan en un conjunto algebraico (o variedad) no contemplados en las ecuaciones, consideremos la curva parametrizada $C = \left\{(t^3, t^4, t^5)\right\}$ en $\mathbb{A}^3_{\mathbb{C}}$. No es difícil probar que $C = \left\{x^2y - z^2 = 0,\ x^4 + y^3 - 2xyz = 0\right\}$ Veamos que, sin embargo, $\mathbf{I}(C) \neq \langle x^2y - z^2,\ x^4 + y^3 - 2xyz\rangle$. Todavía más drástico, $\mathbf{I}(C)$ no puede estar generado por ningún par de polinomios. Es obvio que $y^2 - xz,\ x^3 - yz,\ z^2 - x^2y \in \mathbf{I}(C)$. Dados $g_1, g_2 \in \mathbf{I}(C)$, la parametrización obliga a que g_1 y g_2 no tengan términos lineales ni constantes. Si s_1 y s_2 son sus términos de segundo grado, $\mathbf{I}(C) = \langle g_1, g_2\rangle$, implicaría que $y^2 - xz$, $-yz$ y z^2 son combinaciones lineales (con coeficientes en $\mathbb{C}$) de s_1 y s_2, lo cual es una contradicción.

Tampoco es cierto que una variedad algebraica de codimensión k pueda ser definida con k ecuaciones. Por ejemplo, en [Har62] se menciona la superficie parametrizada $\left\{\left(t, tu, u(u-1), u^2(u-1)\right)\right\}$ en $\mathbb{A}^4_{\mathbb{C}}$ que no puede ser definida con dos ecuaciones. La terminología al uso es llamar *intersección completa* a la situación en la que el número de ecuaciones o de generadores del ideal coincide con la codimensión. En el primer caso se aclara que es *set-theoretic* y en el segundo, *ideal-theoretic*.

Para dar un indicio de la complejidad del tema, todavía es un problema abierto saber si en $\mathbf{A}^3_K$ una curva algebraica siempre se puede definir con dos ecuaciones [Lam06]. Sería instructivo que algo tan básico se mencionase en los textos de introducción a la geometría algebraica. En el lado positivo, se sabe que tres ecuaciones son suficientes [Kne60].

Agradecimientos. Agradezco a los asistentes al curso de máster 2014/2015 "Geometría Diferencial" de la UAM por su interés en el problema. Especialmente a R. González que me señaló [Ily92] y a S. Ranz que me preguntó acerca de las singularidades.

Apéndice de programas

Programa 1: Dibuja curvas de autovalores

```
% dimension
N = 4;
% random matrices
A = rand(N,N);
B = rand(N,N);
%force symmetry
A = A+A';
B = B+B';
% number of points in plot
P = 400;
% with the standard output this gives almost 1pixel precision
R = zeros(N,P);
P = P-1;
for n=0:P;
        R(:,n+1) = eig((1-n/P)*A+n/P*B);
end
t = [0:1/P:1];
% plot graphs.
figure(1)
plot(t,R,'-','linewidth',3)
```

Nota: Para imprimir el resultado, usar `print('-depsc','fichero.eps')`

Programa 2: Zoom del dibujo

```
% ii = number of the low graph, [a,b] =interval
function zoomm( A,B, N, ii, a, b )
        %number of points in plot
        P = 400;
        % with the standard output this gives almost 1pixel precision
        R = zeros(N,P);
        P = P-1;
        for n=0:P;
                t = a + n*(b-a)/P;
                R(:,n+1) = eig((1-t)*A+t*B);
        end
        t = linspace(a,b,P+1);
        figure(2)
        plot(t,R(ii,:),'-', t,R(ii+1,:),'-','linewidth',3)
```

Programa 3: Resultante

```
P.<x,y> = PolynomialRing(QQ, 2)
F = 21*x^3-49*x^2*y+13*y^3+15
G = x^2-3*x*y-3*y^2+5
print F.resultant(G)
print factor( F.resultant(G) )
```

Programa 4: Soluciones aproximadas de (5)

```
var('x y')
R = 509*x^3 + 2036*x^2 + 2631*x + 1107
vy = [find_root(R, -2,-1.6), find_root(R, -1.6, -1.1), find_root(R, -1.1, 0)]

F = 21*x^3-49*x^2*y+13*y^3+15
G = x^2-3*x*y-3*y^2+5
H = (F-G*(21*x+14*y)).expand()

for k in range(3):
        s = solve([H, y-vy[k]],x,y, solution_dict=True)
        print [[v[x].n(30), v[y].n(30)] for v in s]
```

Programa 5: Definición de la variedad

```
y1,y2,y3,y4,y5,y6,la = QQ['y1,y2,y3,y4,y5,y6,la'].gens()
M = matrix([[y1-la,y2,y3],[y2,y4-la,y5],[y3,y5,y6-la]])
P = []
for si in [[0,1],[0,2],[1,2]]:
        for sj in [[0,1],[0,2],[1,2]]:
                P.append( det(M[si, sj]) )
I = ideal(P).radical()
print 'dimension = ',I.dimension()
I = I.elimination_ideal([la])
print I.is_prime()
```

Programa 6: Muestra los polinomios en LaTeX

```
for pol in I.gens():
        print r'\['
        print latex(pol)
        print r'\]'
```

Programa 7: Los múltiplos de la identidad son singulares

```
list_P = []
for pol in I.gens():
        list_P.append( pol )
jac = jacobian(list_P,(y1,y2,y3,y4,y5,y6))
print ( jac(y2=0,y3=0,y4=y1,y5=0,y6=y1) ).rank()
```

Referencias

[CLO07] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[Har62] R. Hartshorne. Complete intersections and connectedness. *Amer. J. Math.*, 84:497–508, 1962.

[Hul03] K. Hulek. *Elementary algebraic geometry*, volume 20 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2003. Translated from the 2000 German original by Helena Verrill.

[Ily92] N. V. Ilyushechkin. The discriminant of the characteristic polynomial of a normal matrix. *Mat. Zametki*, 51(3):16–23, 143, 1992.

[Kne60] M. Kneser. Über die Darstellung algebraischer Raumkurven als Durchschnitte von Flächen. *Arch. Math.*, 11:157–158, 1960.

[Lam06] T. Y. Lam. *Serre's problem on projective modules*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Lax98] P. D. Lax. On the discriminant of real symmetric matrices. *Comm. Pure Appl. Math.*, 51(11-12):1387–1396, 1998.

[Lax07] P. D. Lax. *Linear algebra and its applications*. Pure and Applied Mathematics (Hoboken). Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2007.

[vNW29] J. von Neumann and E. P. Wigner. Über das verhalten von eigenwerten bei adiabatisdren prozessen. *Phys. Zschr.*, 60:467–470, 1929.