

ÁLGEBRA CONMUTATIVA Y GEOMETRÍA ALGEBRAICA

Autores: José Luis Aguado
Lugar: UNCPBA-Tandil

FÓRMULAS DE TIPO LEIBNIZ PARA DERIVACIONES INTERNAS GENERALIZADAS EN CARACTERÍSTICA POSITIVA

Dada un álgebra A y dos endomorfismos σ, τ de A , para cada $a \in A$, se define un nuevo endomorfismo $\delta_a : A \rightarrow A$ por $\delta_a(x) = a\tau(x) - \sigma(x)a$. Entonces δ_a verifica que: $\delta_a(xy) = \delta_a(x)\tau(y) + \sigma(x)\delta_a(y)$. Decimos que δ_a es una (σ, τ) -derivación (interna) de A .

Si K es un cuerpo perfecto de característica $p > 0$ y $A = K[[X]]$, se obtienen fórmulas de tipo Leibniz para $\delta_a^n(x_1x_2)$ y $\delta_a^n(x_1x_2 \cdots x_m)$ para todo $n, m \in \mathbb{N}$, donde δ_a es una (σ, τ) -derivación interna de A y σ, τ se sustituyen oportunamente por endomorfismos del tipo 1) $F_h : a \rightarrow a^{p^h}$, el morfismo de Frobenius con $h \geq 0$ y 2) $D_h = \frac{\partial}{\partial X^{p^h}}$, la derivación de Dieudonné de orden p^h .

Autores: Antonio Cafure (1,2), Guillermo Matera (2), Ariel Weissbein (3)
Lugar: (1) Universidad de Buenos Aires. (2) Universidad Nacional de General Sarmiento. (3) CoreLabs.

INVERSIÓN EFICIENTE DE MORFISMOS POLINOMIALES SOBRE CUERPOS FINITOS

Sean $F_1, \dots, F_n$ polinomios en n indeterminadas con coeficientes en $\mathbb{F}_q$, el cuerpo finito de q elementos, de grado a lo sumo d . Consideramos el morfismo $F : \mathbb{A}^n \rightarrow \mathbb{A}^n$ definido como $F(x) := (F_1(x), \dots, F_n(x))$. Asumiendo que la restricción de F a $\mathbb{F}_q^n$ es biyectiva, desarrollamos un algoritmo que, dado $y^{(0)} \in \mathbb{F}_q^n$, calcula el único punto $x^{(0)} \in \mathbb{F}_q^n$ tal que $F(x^{(0)}) = y^{(0)}$. Para eso, pensamos el gráfico de F como una subvariedad $V \subset \mathbb{A}^{2n}$ y consideramos la proyección $\pi : V \rightarrow \mathbb{A}^n$ en las variables $Y_1, \dots, Y_n$. La idea es deformar el sistema $F(X) = y^{(0)}$ en un sistema $F(X) = F(x^{(1)})$, donde $x^{(1)}$ es un punto adecuado con coordenadas en una extensión finita de $\mathbb{F}_q$. Nuestro resultado es el siguiente:

Teorema *Si los polinomios $F_1, \dots, F_n$ se evalúan con T operaciones sobre $\mathbb{F}_q$, la única solución q -racional del sistema $F(X) = y^{(0)}$ puede calcularse con $O((T + n^4 + D^2)n\delta^2)$ operaciones sobre $\mathbb{F}_q$, donde δ denota el grado de V y D , el grado del morfismo π .*

El interés por este tipo de problemas se origina en los casos en que el morfismo F codifica alguna permutación de un esquema criptográfico.

ÁLGEBRA DE NORTON DE CIERTOS GRAFOS DE DISTANCIA REGULAR

Dado un conjunto de vértices X y una distancia d definimos *grafos de distancia regular*. Consideramos $L^2(X)$ el espacio de funciones indexadas por X y en dicho espacio el operador

$$\mathcal{L} : L^2(X) \rightarrow L^2(X), \quad \mathcal{L}f(x) = \sum_{y:d(x,y)=1} f(y).$$

Se tiene una descomposición de $L^2(X)$ en autoespacios V_λ de $\mathcal{L}$, $L^2(X) = \oplus_\lambda V_\lambda$.

En cada V_λ se puede definir una estructura de álgebra $(V_\lambda, \star)$, conocida como *álgebra de Norton*, de la siguiente forma:

$$f \star g = \pi_\lambda(f \circ g) \quad f, g \in V_\lambda$$

donde π_λ es la proyección a V_λ y $\circ$ es el producto de Hadamard en $L^2(\Omega)$.

Tomando como ejemplo los grafos de Johnson y los grafos de espacios polares duales, veremos una construcción de un conjunto de generadores de V_λ en los cuales el producto en el álgebra de Norton tiene una expansión sencilla.

REFERENCIAS

- [1] Brouwer, Cohen, Neumaier, *Distance-Regular Graphs*. Springer-V., 1989.
- [2] Cameron, Goethals, Seidel, The Krein condition, spherical designs, Norton algebras and permutation groups, *Proc. Kon. Nederl. Akad. Wetensch. (A)* **81** (1978).
- [3] Stanton, Orthogonal polynomials and Chevalley groups. In *Special Functions: Group Theoretical Aspects and Applications* (Eds Askey, Koornwinder, and Schempp); D. Reidel Publishing Company, (1984).

UN ALGORITMO PARA DESCRIBIR PUNTOS EN CONJUNTOS SEMIALGEBRAICOS

Dado un sistema de ecuaciones e inecuaciones polinomiales $f_1(x) = \dots = f_m(x) = 0, g_1(x) \geq 0, \dots, g_p(x) \geq 0$, con $f_i, g_j \in \mathbb{R}[X_1, \dots, X_n], i = 1, \dots, m; j = 1, \dots, p$, una de las preguntas básicas que pueden plantearse es si este sistema tiene o no una solución en $\mathbb{R}^n$. En caso de que el conjunto de las soluciones sea no vacío, la siguiente pregunta natural es cómo exhibir, de alguna manera, (algunas de) estas soluciones.

Una de las subrutinas más utilizadas en los algoritmos que resuelven este problema consiste en hallar un conjunto finito que contenga al menos un punto en cada componente conexa del conjunto de las soluciones. En el caso de sistemas de ecuaciones (sin desigualdades), la práctica más usual involucra localizar los puntos críticos sobre el conjunto en cuestión de una función polinomial (típicamente, una proyección o una distancia).

En esta charla exhibiremos un algoritmo para la resolución del problema planteado, que utiliza las *condiciones de Karush-Kuhn-Tucker* (que generalizan el teorema de los multiplicadores de Lagrange al admitir condiciones de desigualdades) para caracterizar puntos críticos. Bajo ciertas hipótesis, estas condiciones permiten reducir el problema a hallar las soluciones aisladas de un sistema de ecuaciones ampliado. Para resolver este nuevo sistema desarrollamos un método específico, basado en técnicas de deformación, que explota fuertemente su estructura. Como resultado obtenemos un nuevo algoritmo para resolver el problema original con complejidades que mejoran las de los algoritmos anteriores que lo resuelven.

VARIACIONES INFINITESIMALES DE ESTRUCTURAS DE HODGE ASOCIADAS A
HIPERSUPERFICIES EN VARIEDADES TÓRICAS SUAVES

Una manera de generar variaciones de estructuras de Hodge es a través de la cohomología de una familia de variedades proyectivas polarizadas. Estas variaciones son llamadas *variaciones geométricas*. Un problema clásico en teoría de Hodge consiste en describir las variaciones geométricas dentro del conjunto total de las variaciones. Una versión infinitesimal de este problema consiste en describir el lugar que ocupan las variaciones infinitesimales de estructura de Hodge que se originan en deformaciones infinitesimales de una variedad polarizada dada.

E. Allaud demuestra en [A] que las variaciones infinitesimales asociadas a la deformación infinitesimal de hipersuperficies genéricas del espacio proyectivo $\mathbb{CP}^n$ son no genéricas en el conjunto de las variaciones infinitesimales correspondientes. En esta comunicación discutiremos la validez de este tipo de resultado para el caso de hipersuperficies en variedades tóricas completas, simpliciales y proyectivas. En particular, si la variedad tórica es suave y su dimensión ≥ 4 , vale que la variación infinitesimal generada por la deformación infinitesimal de una hipersuperficie genérica es no genérica. Estos resultados aportan evidencia para la conjetura siguiente: *las variaciones infinitesimales de estructura de Hodge de origen geométrico no son genéricas*.

REFERENCIA

[A] Allaud, E.: *Nongenericity of variations of Hodge structure for hypersurfaces of high degree*, Duke Math. J. **129** (2005), no. 2, 201–217.
