VOZES DIVERSAS
DIFERENTES SABERES

SALÃO DE INICIACAO CIENTIFICA XXX SIC

15 A 19 OUTUBRO CAMPUS DO VALE

UFRGS PROPESQ

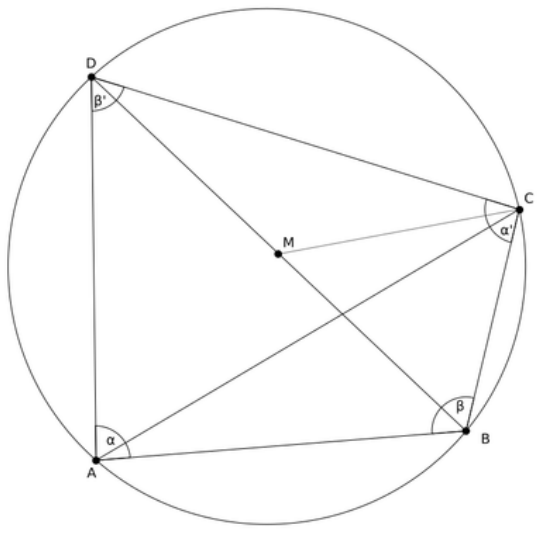
DEMONSTRAÇÃO DE TEOREMAS DE GEOMETRIA EUCLIDIANA: UM ESTUDO SOBRE BASES DE GRÖBNER

Wesley Gonçalves Lautenschlaeger
Orientadora: Thaísa Raupp Tamusiunas
Bacharelado em Matemática - Ênfase em Matemática Pura
Universidade Federal do Rio Grande do Sul - UFRGS

MOTIVAÇÃO

Com base no *método de Descartes*, queremos encontrar uma forma de provar teoremas de geometria euclidiana computacionalmente. Para isso, precisamos estabelecer um plano cartesiano em torno do teorema que queremos provar e construir polinômios em n indeterminadas associados às (finitas) hipóteses e à conclusão do teorema. Os polinômios associados às hipóteses são construídos de tal forma que se anulam sempre que as hipóteses forem verdadeiras. O método consiste em mostrar que quando as hipóteses são verdadeiras, ou seja, se anulam, a conclusão também é verdadeira, isto é, se anula. Em outras palavras, para provar a veracidade do teorema precisamos mostrar que o polinômio que representa a conclusão é uma combinação dos polinômios que representam as hipóteses.

Podemos utilizar este método para provar o *teorema de Ptolomeu*, por exemplo, que diz que em um quadrilátero inscrito em uma circunferência, o produto dos comprimentos das diagonais é igual à soma dos produtos dos comprimentos dos lados opostos. (imagem)



METODOLOGIA

Proposição: Sejam f polinômio e I ideal de $K[x_1, \ldots, x_n]$, onde K denota um corpo. São equivalentes:

1. f se anula em todos os pontos de $\mathcal{Z}(I)$;
2. $\langle 1 - zf \rangle + K[x_1, \ldots, x_n, z]I = K[x_1, \ldots, x_n, z]$;
3. $f \in \sqrt{I}$.

Utilizando este resultado, bastaria, então, dividir o polinômio c (associado à conclusão) pelos polinômios h's (referentes às hipóteses), de forma que o resto nulo representaria a pertinência do polinômio c no ideal gerado pelos polinômios h's em $K[x_1, \ldots, x_n]$.

Entretanto, o algoritmo da divisão para polinômios de mais de uma indeterminada não funciona da maneira esperada. De fato, basta mudar a ordem dos divisores que obteremos quocientes e restos diferentes.

DESENVOLVIMENTO

O ideal inicial $\text{in}(I)$ de I é o ideal de $K[x_1, \ldots, x_n]$ gerado por $\text{in}(f) \forall\ f \in I$, onde $\text{in}(f)$ representa o termo incial de f dada uma ordem monomial. Um subconjunto finito G de I é uma base de Gröbner para I se $\text{in}(I) = \langle \text{in}(G) \rangle$. Em particular, $I = \langle G \rangle$. Podemos calcular uma base de Gröbner a partir do *algoritmo de Buchberger*. Dizemos que uma base de Gröbner é *mínima* se tem coeficiente 1 para todo $g \in G$ e se $i \neq j$ então $\text{in}(g_i)$ não divide $\text{in}(g_j)$. Uma base é dita *reduzida* quando além de mínima cada g é reduzido com relação a $G \setminus \{g\}$. Todo ideal de $K[x_1, \ldots, x_n]$ possui uma, e apenas uma, base de Gröbner reduzida.

PROPRIEDADES

- O resto de um polinômio f de $K[x_1, \ldots, x_n]$ por G não depende da ordenação dos elementos de G.
- $G = \{1\}$ se, e somente se, $I = K[x_1, \ldots, x_n]$.
- Dois ideais são iguais se, e somente se, sua base de Gröbner reduzida é igual.

CONCLUSÃO

O método direto: dados $h_1, \ldots, h_s, d_1, \ldots, d_r$ e c polinômios no anel $\mathbb{C}[x_1, \ldots, x_n]$, de modo que os h's determinam as hipóteses do resultado a ser provado, os d's determinam as condições de degeneração e c sua conclusão, o algoritmo retorna uma das duas afirmações seguintes: *o resultado é verdadeiro* ou *o resultado não pode ser confirmado*.

Etapa 1: Determine uma base de Gröbner reduzida G para o ideal gerado pelos polinômios $h_1, \ldots, h_s, t_1 d_1 - 1, \ldots, t_r d_r - 1$ no anel $\mathbb{C}[x_1, \ldots, x_n, t_1, \ldots, t_r]$.

Etapa 2: Calcule o resto $R_G(c)$ da divisão de c por G. Se $R_G(c) = 0$, então *o resultado é verdadeiro*, se $R_G(c) \neq 0$, então *o resultado não pode ser confirmado*.

OUTRAS APLICAÇÕES

- Calcular o polinômio mínimo de uma extensão algébrica sobre um corpo;
- Resolver problemas de coloração de grafos e caminhos hamiltonianos;
- Calcular o MDC, o MMC e a fatoração livre de quadrados de polinômios em n indeterminadas sobre um corpo; e
- Provar se um mecanismo articulado descreve ou não uma curva dada.

REFERÊNCIAS BIBLIOGRÁFICAS

S. C. Coutinho, Polinômios e computação algébrica, Coleção Matemática e Aplicações, Primeira Edição, IMPA, (2012).

W. W. Adams, e P. Loustaunau, An introduction to Gröbner bases, American Mathematical Society, Providence (1994).