Bases de Shirshov-Gröbner e módulos de Weyl

Angelo Calil Bianchi

Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

-o-

Suporte da FAPESP 2015/22040-0

Estrutura da Apresentação

- Bases de Gröbner – caso de polinômios comutativos – .
- Bases de Shirshov – caso geral – .
- Construção de bases para Módulos de Weyl.

Parte I - Bases de Gröbner

Motivação: Eliminação Gaussiana

Dadas equações

$$\begin{cases} f_i = \sum_j a_{ij}x_j + b_i = 0, \qquad a_{ij}, b_i \in \mathbb{C}, \end{cases}$$

um método comum para resolver estas equações é usar a Eliminação Gaussiana na matriz $(A|b)$ (com $A = (a_{ij})$ e $B = (b_i)$) para obter a sua forma escalonada. Pode-se, então, ler as soluções a partir desta nova matriz.

O que está acontecendo com os termos dos polinômios (que induzem as equações dadas) durante este processo?

Motivação: algoritmo Euclideano

Dados polinômios $f_1, f_2, \ldots, f_r \in \mathbb{C}[x]$, o algoritmo de Euclides é útil para determinar se o sistema

$$f_1(x) = \cdots = f_r(x) = 0$$

possui uma solução.

O que o algoritmo faz com os termos dos polinômios (que induzem estas equações)?

$\rightsquigarrow$ o que o algoritmo faz é encontrar o máximo divisor comum $g(x)$ destes polinômios. O sistema original possui solução quando $g(x)$ não é uma constante.

Próximo passo

Os objetos não são lineares e envolvem várias variáveis... E agora?

É possível estender os métodos anteriores para
equações polinomiais induzidas por polinômios não lineares?

Anéis de Polinômios

Sejam $\mathbb{C}$ um corpo e $x_1, \ldots, x_n$ um conjunto de variáveis, o conjunto

$$\mathbb{C}[x_1, \ldots, x_n] = \left\{ \sum_{i_1,\ldots,i_n \in \mathbb{Z}_+} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \; com \; a_{i_1,\ldots,i_n} \in \mathbb{C} \; e \; QSN \right\}$$

forma:

- um espaço vetorial – com as operações usuais de soma de polinômios e de multiplicação de um escalar por um polinômio;
- um anel – ao considerar a operação usual de multiplicação de polinômios.

$\Longrightarrow$ Resumidamente: uma $\mathbb{C}$-álgebra com as operações usuais.

Nomenclaturas

Sejam $c \in \mathbb{C}$ e $a_1, ..., a_n \in \mathbb{Z}_{\geq 0}$. Em $\mathbb{C}[x_1, ..., x_n]$,

- um **monômio** é um elemento da forma $x_1^{a_1} \cdots x_n^{a_n}$;
- um **termo** é um elemento da forma $cx_1^{a_1} \cdots x_n^{a_n}$;
- o **grau total** de um termo $m = cx_1^{a_1} \cdots x_n^{a_n}$ é $deg(m) = a_1 + ... + a_n$;

Primeiro ingrediente: ordens monomiais

Seja $\mathcal{M}$ o conjunto de todos os monômios em $\mathbb{C}[x_1, ..., x_n]$.
Uma **ordenação monomial em** $\mathcal{M}$ é uma relação $\prec$ em $\mathcal{M}$, satisfazendo as seguintes condições:

- Para cada par de monômios m e n vale que ou $m \prec n$ ou $n \prec m$ ou $m = n$. (tricotomia)
- Se $m \prec n$ e $n \prec p$, então $m \prec p$. (transitividade)
- Para todo monômio $m \neq 1$, vale que $1 \prec m$.
- Se $m \prec n$, então $zm \prec zn$, $\forall\, z \in \mathcal{M}$. (monotonicidade da multiplicação)

Exemplos de ordens monomiais

1. ORDEM LEXICOGRÁFICA (LEX)

$$m = x_1^{i_1} \ldots x_n^{i_n} \prec_{Lex} x_1^{j_1} \ldots x_n^{j_n} = n,$$

se $i_1 = j_1, \ldots, i_k = j_k$ e $i_{k+1} < j_{k+1}$, para algum k.

2. ORDEM LEXICOGRÁFICA REVERSA (REVLEX)

$$m = x_1^{i_1} \ldots x_n^{i_n} \prec_{Lex} x_1^{j_1} \ldots x_n^{j_n} = n,$$

se $i_n = j_n, \ldots, i_k = j_k$ e $i_{k-1} < j_{k-1}$, para algum k.

3. ORDEM LEXICOGRÁFICA DE GRAU (DEGLEX)

$$m = x_1^{i_1} \ldots x_n^{i_n} \prec_{DegLex} x_1^{j_1} \ldots x_n^{j_n} = n,$$

se $deg(m) < deg(n)$ ou se $deg(m) = deg(n)$ e $m \prec_{lex} n$.

Mais nomenclaturas

Fixada uma ordem monomial em $\mathbb{C}[x_1, ..., x_n]$, dado $f \in \mathbb{C}[x_1, ..., x_n]$.
Denotaremos por:

1. $\ell m(f)$ o **Monômio líder de *f***, isto é, o maior monômio que aparece nos termos não nulos de f.
2. $\ell t(f)$ o **Termo líder de *f***, isto é, o maior termo que aparece em f.
3. **Ideal gerado pelos monômios líderes do ideal** $\mathcal{I}$:
   $\ell(\mathcal{I}) = \langle \ell m(f) \mid f \in \mathcal{I} \rangle = \langle \ell t(f) \mid f \in \mathcal{I} \rangle$

Algoritmo da Divisão em $\mathbb{C}[x]$

Teorema

Sejam $f, g \in \mathbb{C}[x]$, $f \neq 0$. Então, existem únicos polinômios $q, r \in \mathbb{C}[x]$ tais que $g = qf + r$, com $0 \leq deg(r) < deg(f)$.

Corolário

Cada ideal de $\mathbb{C}[x]$ é gerado por apenas um polinômio (ideal principal).

Um exemplo-problema

Consideremos $f_1 = xy - 1$, $f_2 = x^2 + 1$ e $f = x^2y + y$ em $\mathbb{C}[x, y]$, com a ordem LEX, $x \succ y$. Pergunta-se: $f \in \langle f_1, f_2 \rangle$?

- Dividindo f por f_1 e f_2, o resultado é a expressão

$$f = xf_1 + 0f_2 + (x + y).$$

- Dividindo f por f_2 e f_1, o resultado é a expressão

$$f = 0f_1 + yf_2 + 0,$$

Como lidar com estas situações diferentes?

Como fundamentar esta divisão por um conjunto de polinômios?

Algoritmo da Divisão em $\mathbb{C}[x_1, ..., x_n]$

Teorema

Fixada uma ordem monomial $\prec$ e uma sequência $F = (f_1, ..., f_s)$ de polinômios em $\mathbb{C}[x_1, ..., x_n]$, então cada polinômio f pode ser escrito como

$$f = q_1 f_1 + ... + q_s f_s + r,$$

onde $q_i, r \in \mathbb{C}[x_1, ..., x_n]$, $r = 0$ ou r não é divisível por nenhum dos $\ell t(f_i)$.

O resultado que se segue é um dos clássicos da teoria de ideais em anéis polinomiais, é atribuído a David Hilbert (1891).

Teorema de Hilbert

Todo ideal em $\mathbb{C}[x_1, ..., x_n]$ é finitamente gerado.

Algumas considerações...

Se $\mathcal{I} = \langle f_1, ..., f_r \rangle$. Então, por definição, $\ell m(f_i) \in \ell(\mathcal{I}), \ \forall \ i$. Em particular,

$$\langle \ell m(f_1), ..., \ell m(f_r) \rangle \subset \ell(\mathcal{I}).$$

No entanto, a inclusão contrária não é verdadeira em geral, isto é,

$$\ell(\mathcal{I}) \not\subset \langle \ell m(f_1), ..., \ell m(f_r) \rangle \, .$$

Ilustramos isto no próximo exemplo: Seja $\mathcal{I} = \left\langle x_1^2, x_1x_2 - x_2^2 \right\rangle$ e consideremos a ordem LEX. Então,

$$\left\langle \ell m(x_1^2), \ell m(x_1x_2 - x_2^2) \right\rangle = \left\langle x_1^2, x_1x_2 \right\rangle \, .$$

Além disso, $x_2^3 = x_2(x_1^2) - (x_1 + x_2)(x_1x_2 - x_2^2) \in \mathcal{I}$ e $\ell m(x_2^3) = x_2^3 \in \ell(\mathcal{I})$, porém $x_2^3 \notin \left\langle x_1^2, x_1x_2 \right\rangle$.

Motivação para a definição das bases de Gröbner

As questões que se seguem são as pedras fundamentais que conduziram o desenvolvimento do conceito de bases de Gröbner.

Seja $\mathcal{I}$ um ideal.

- Dado um polinômio $f \in \mathcal{I}$, existe um conjunto de geradores G de $\mathcal{I}$ tal que $r_G f$ seja único para qualquer ordenação dos elementos de G?
- Existe um conjunto de geradores G de $\mathcal{I}$ tal que

$$f \in \mathcal{I} \Leftrightarrow G|f?$$

- Se a resposta para as perguntas anteriores é positiva, como encontrar tal conjunto? A existência é garantida? Algoritmo?

Bases de Gröbner

Definição

Seja $\mathcal{I}$ um ideal em $\mathbb{C}[x_1, ..., x_n]$. Fixada uma ordem monomial, um conjunto $G = \{g_1, ..., g_s\} \subset \mathcal{I}$ tal que $\langle \ell m(g_1), ..., \ell m(g_s)\rangle = \ell(\mathcal{I})$ é chamado de **base de Gröbner para** $\mathcal{I}$.

Teorema

Fixada uma ordem monomial em $\mathbb{C}[x_1, ..., x_n]$, todo ideal $I \subseteq \mathbb{C}[x_1, ..., x_n]$ admite uma Base de Gröbner (finita).

As bases de Gröbner respondem positivamente às perguntas anteriores.

Propriedades

1. Se $G = \{g_1, ..., g_s\}$ é uma base de Gröbner para um ideal $\mathcal{I}$, então $\langle g_1, ..., g_s \rangle = \mathcal{I}$
2. Se G é uma base de Gröbner para um ideal $\mathcal{I}$, então, para cada $f \in \mathbb{C}[x_1, ..., x_n]$, o resto $r_G(f)$ é único (i.e., independe da ordenação dos elementos de G)
3. Se G é uma base de Gröbner para um ideal $\mathcal{I}$, então $f \in I$ se, e somente se, $r_G(f) = 0$.
4. Sejam $I \subseteq \mathbb{C}[x_1, ..., x_n]$ um ideal e $G = \{g_1, ..., g_s\}$ uma base de Gröbner para I. Os monômios de $\mathbb{C}[x_1, ..., x_n]$ que não são divisíveis por $\{\ell m(g_1), ..., \ell m(g_s)\}$ formam uma $\mathbb{C}$-base para $\frac{\mathbb{C}[x_1, ..., x_n]}{I}$.

S-Polinômios: uma ferramenta para simplificar

Seja (f_1, f_2) um par fixo de elementos mônicos em $\mathbb{C}[x_1, ..., x_n]$ e $\prec$ uma ordem monomial. O S-polinômio de (f_1, f_2) em $\prec$ é

$$S_{(f_1,f_2)} = \frac{mmc(lm(f_1), lm(f_2))}{lm(f_1)} f_1 - \frac{mmc(lm(f_1), lm(f_2))}{lm(f_2)} f_2$$

Exemplo: Sejam $(f_1, f_2) = (x_1^2, x_1x_2 - x_2^2)$ e a ordem LEX. Então,
$S_{(f_1,f_2)} = x_2x_1^2 - \frac{x_1^2x_2}{x_1x_2}(x_1x_2 - x_2^2) = x_1x_2^2$

Teorema: o Critério de Buchberger

Sejam $G = \{f_1, ..., f_t\}$ o conjunto gerador do ideal $\mathcal{I} \subseteq \mathbb{C}[x_1, ..., x_n]$ e S_{f_i,f_j} o S-polinômio de f_1 e f_j. Então,

$$G \text{ é uma base de Gröbner de } \mathcal{I} \Leftrightarrow r_G(S_{f_i,f_j}) = 0, \ \forall\, i, j.$$

Algoritmo de Buchberger

Seja $\mathcal{I} = \langle f_1, ..., f_s \rangle \neq 0 \subseteq \mathbb{C}[x_1, ..., x_n]$ um ideal. Então, uma base de Gröbner para $\mathcal{I}$ pode ser construída em uma quantidade finita de passos pelo algoritmo:

```
Entrada:  F = {f_1, ..., f_s}
Saída:  uma base de Gröbner G = {g_1, ..., g_t} para o ideal I.
G := F
    REPETIR
        G' := G
        Para cada par i ≠ j em G' faça
            h := o resto da divisão de S_{f_i,f_j} por G'
            Se  h ≠ 0, então G := G ∪ {h}
    Até que G = G'
```

Bases de Gröbner Reduzidas

Uma **base de Gröbner reduzida** para um ideal polinomial $\mathcal{I}$ é uma base de Gröbner G para $\mathcal{I}$ satisfazendo:

i) os elementos de G são mônicos;

ii) $\forall\, p \in G$, nenhum monômio de p está em $\ell t(G - \{p\})$.

Proposição

Fixada uma ordem monomial em $\mathbb{C}[x_1, ..., x_n]$, todo ideal (não nulo) possui uma única base de Gröbner reduzida.

Exemplo: Seja $\mathcal{I} = \langle x_1^2, x_1x_3 - x_2^2 \rangle$. Então, $\{x_1^2, x_1x_2^2, x_1x_3 - x_2^2, x_2^4\}$ é a base de Gröbner reduzida para $\mathcal{I}$, quando se adota ou a ordem Lex ou a DegLex.

Teorema da Eliminação

Um aplicação muito útil das bases de Gröbner é a eliminação de variáveis num anel polinomial.

Teorema

Seja $\mathcal{I} \subseteq \mathbb{C}[x_1, ..., x_n]$ um ideal e seja G uma Base de Gröbner para $\mathcal{I}$, com relação à ordem reversa LEX. Então, para cada $k = 0, ..., (n-1)$, $G_k = G \cap \mathbb{C}[x_1, ..., x_k]$ é uma base de Gröbner para $\mathcal{I}_k := \mathcal{I} \cap \mathbb{C}[x_1, ..., x_k]$.

Resolvendo Sistemas de Equações

Dado um sistema de equações polinomiais

$$f_1(x_1, ..., x_n) = ... = f_s(x_1, ..., x_n) = 0$$

em $\mathbb{C}[x_1, ..., x_n]$, como encontrar seu conjunto solução em $\mathbb{C}^n$?

- Adota-se a ordem LEX com $x_1 > x_2 > ... > x_n$ e calcula-se uma base de Gröbner $G = \{g_1, ..., g_t\}$ para o ideal $\mathcal{I} = \langle f_1, .., f_s \rangle$.
- Pelo Teorema da Eliminação, $G \cap \mathbb{C}[x_{k+1}, ..., x_n]$ é uma base de Gröbner para $\mathcal{I}_k = \mathcal{I} \cap \mathbb{C}[x_{k+1}, ..., x_n]$ ($\rightsquigarrow$ isso garante uma eliminação de variáveis).
- Resolve-se essas equações envolvendo "variáveis maiores" e substitui-se nas demais equações de forma semelhante ao método de Gauss para sistemas lineares triangulares.

Exemplo

Resolver em $\mathbb{C}^4$ o sistema de equações a seguir:

$$\left\{\begin{array}{rcl} xz - yw - z + 1 & = & 0 \\ yz + xw - w - 2 & = & 0 \\ y^2 + x^2 - 1 & = & 0 \\ z^2 + w^2 - 1 & = & 0 \end{array}\right. \tag{1}$$

Calculando uma base de Gröbner para o ideal

$$I = \left\langle xz - yw - z + 1, yz + xw - w - 2, y^2 + x^2 - 1, z^2 + w^2 - 1 \right\rangle,$$

adotando a ordem LEX com $x > y > z > w$, obtemos:

$$G = \left\{ \underbrace{x + z - 2w - 1}_{g_1}, \underbrace{y - 2z - w}_{g_2}, \underbrace{z - 2w - 5/2}_{g_3}, \underbrace{w^2 + 2w + 21/20}_{g_4} \right\}.$$

Exemplo - continuação

Como os elementos das bases de Gröbner têm os mesmos zeros do sistema original, segue que o conjunto solução do sistema dado em $\mathbb{C}^4$ é dado por:

$$w_2 = \frac{-10 - i\sqrt{5}}{10}, z_2 = \frac{5 - 2i\sqrt{5}}{10}, y_2 = \frac{-i\sqrt{5}}{2}, x_2 = \frac{-25 - 4i\sqrt{5}}{10}$$

$$w_1 = \frac{-10 + i\sqrt{5}}{10}, z_1 = \frac{5 + 2i\sqrt{5}}{10}, y_1 = \frac{i\sqrt{5}}{2}, x_1 = \frac{-25 + 4i\sqrt{5}}{10},$$

onde i é a unidade imaginária.

Parte II - Bases de Shirshov

Deixando os polinômios comutativos...

Rudimentos - I

Seja $X = \{x_1, \ldots, x_n, \ldots\}$ um alfabeto. Considere em X uma ordem $x_i \prec x_j \iff i < j$. Denote por X^* o semigrupo das palavras associativas sobre X.

A palavra vazia será denotada por 1 e o comprimento de uma palavra u será denotado por $l(u)$ com $l(1) = 0$. Considere em X^* duas ordens:

Ordem lexicográfica $<$

$u < 1$ para qualquer $u \in X^*$ não vazia

$u = x_i u' < x_j v' = v$ se $x_i \prec x_j$ ou $x_i = x_j$ e $u' < v'$ (indutivamente).

Ordem lexicográfica de comprimento $<<$

$u << v$ se $l(u) < l(v)$ ou $l(u) = l(v)$ e $u < v$.

Rudimentos - II

Sejam $\mathbb{F}$ um corpo e $\mathcal{A}_X$ a álgebra associativa gerada por X sobre $\mathbb{F}$.

Sejam $S, T \subseteq \mathcal{A}_X$ conjuntos de elementos mônicos.

$\diamond$ Considere o ideal bilateral J_S gerado por S em $\mathcal{A}_X$ e denote por $A = \frac{\mathcal{A}_X}{J_S}$ a álgebra associativa definida por S.

$\diamond$ Considere o ideal à esquerda I_T de $\mathcal{A}_X$ gerado pela imagem de T em A e considere o A-módulo à esquerda definido por T, denotado por $M = \frac{A}{I_T}$.

Devido ao papel específico de cada subconjunto S e T, diz-se que o A-módulo M é definido pelo par (S, T).

Uma relação de congruência

Dado $p \in \mathcal{A}_X \setminus \{0\}$, denote por $\overline{p}$ o monômio líder de p considerando a ordem $<<$, ou seja,

$$p = \alpha\overline{p} + \sum \beta_i w_i$$

com $\alpha, \beta_i \in \mathbb{F}, \alpha \neq 0, w_i \in X^*$ e $w_i << \overline{p}$.

Sejam $p, q \in \mathcal{A}_X$ e $w \in X^*$. Diz-se que p é congruente a q com respeito ao par (S, T) e a w, e denota-se $p \equiv q \mod (S, T; w)$, se

$$p - q = \sum \alpha_i a_i s_i b_i + \sum \beta_j c_j t_j,$$

onde $\alpha_i, \beta_j \in \mathbb{F}, a_i, b_i, c_j \in X^*, s_i \in S, t_j \in T$ com $a_i\overline{s_i}b_i << w$ e $c_j\overline{t_j} << w$ para cada i e j.

Composições de elementos em $\mathcal{A}_X$

Sejam $p, q \in \mathcal{A}_X$. Define-se a composição de p e q como:

- Se existem a e b em X^* tais que $\overline{p}a = b\overline{q} = w$ com $l(\overline{p}) > l(b)$, então a composição de interseção é definida como $(p, q)_w = pa - bq$.
- Se existem a e b em X^* tais que $a\overline{p}b = \overline{q} = w$, então a composição de inclusão é definida como $(p, q)_w = apb - q$.
- Se existe a em X^* tal que $\overline{p} = a\overline{q} = w$, então a composição justificada à direita é definida compo $(p, q)_w = p - aq$.

Conjuntos fechados por composições

- Um conjunto S de elementos mônicos em $\mathcal{A}_X$ é dito fechado sob composições se para quaisquer $p, q \in S$ e $w \in X^*$ tais que $(p,q)_w$ está definido tem-se $(p,q)_w \equiv 0 \mod (S;w)$.

- Um conjunto T de elementos mônicos em $\mathcal{A}_X$ é dito fechado sob composições justificadas à direita com respeito a S se para quaisquer $p, q \in T$ e $w \in X^*$ tais que $(p,q)_w$ está definido tem-se $(p,q)_w \equiv 0 \mod (S,T;w)$.

Definição

Um par (S, T) de subconjuntos de elementos mônicos de $\mathcal{A}_X$ é chamado de um par de Shirshov-Gröbner para o A-módulo M definido por (S, T) se

$\diamond$ S é fechado sob composição

$\diamond$ T é fechado sob composições justificadas à direita relativamente a S

$\diamond$ para todos $p \in S$, $q \in T$ e $w \in X^*$ tais que $(p, q)_w$ está definido tem-se $(p, q)_w \equiv 0 \mod (S, T; w)$

Definição

Uma palavra $u \in X^*$ é dita (S, T)-reduzida se $u \neq a\bar{s}b$ e $u \neq c\bar{t}$ para qualquer $s \in S$, $t \in T$ e $a, b, c \in X^*$. Caso contrário, $u \in X^*$ é dita (S, T)-redutível.

Resultados Fundamentais

Lema da Composição de Shirshov

Se (S, T) é um par de Shirshov-Gröbner par para o A-módulo M e $p \in \mathcal{A}_X$ é trivial em M, então $\overline{p}$ é (S, T)-redutível.

Teorema da Base

Se (S, T) é um par de Shirshov-Gröbner para o A-módulo M, então o conjunto das palavras $(S, T)-$reduzidas forma uma base para M.

Teorema (Completamento)

Um par $(\mathcal{S}, \mathcal{T})$ pode ser completado a um par de Shirshov-Gröbner (S, T) para o A-módulo M.

Parte III - Módulos de Weyl

Uma aplicação em módulos de peso máximo

Historical overview

1. **Local Weyl modules** were first considered in '2001 by Chari and Pressley, in the classical and quantum affine contexts, motivated by representations of quantum affine algebras. All the results of that paper go over with no difficulty to the case of the **current algebras** $\mathfrak{g} \otimes \mathbb{C}[t]$.
2. A more general case was considered in '2004 by Feigin and Loktev by replacing the polynomial ring with the coordinate ring of an algebraic variety and partial results analogous to those of Chari and Pressley.

Historical overview

3. Chari, Fourier and Khendai in '2010 considered a categorical (i.e, functorial) approach to the algebra $\mathfrak{g} \otimes A$, where A is a commutative associative algebra (with unit) over the complex numbers. $\rightsquigarrow \mathfrak{g} \otimes \mathbb{C}, \ \mathfrak{g} \otimes \mathbb{C}[t], \ \mathfrak{g} \otimes \mathbb{C}[t, t^{-1}], \ \mathfrak{g} \otimes \frac{\mathbb{C}[t]}{<t^k>}$.
4. Moura and Jakelic started in '2007 the study of the positive characteristic analogous of local Weyl modules for loop algebras (in the context of **hyperalgebras**). Followed by a joint work of B., Macedo and Moura in '2015 involving loop and current algebras.

Historical overview

5. Different perspectives on Weyl modules include many works in the last 15 years... and a long list of authors: Batra, Bennett, Futorny, Feigin, Kus, Lau, Littelmann, Loktev, Naoi, Neher, Manning, Savage, Venkatesh, Zhao and so on.
6. Even with a large number of papers dedicated to the study of structure, character, dimension, decomposition, tensor product, fusion product, and reducibility of Weyl modules, only three of them focuses in the construction of bases for local Weyl modules and one of them about basis for truncated local Weyl modules.

Origin of this work

The present work was originally intended to present a different approach to obtain some “different types” of bases for local Weyl modules for the $\mathfrak{sl}_2$-current algebra with a good “computational” and “combinatorial” behavior.

In a joint work with Evan Wilson we obtained:

- an uniform approach to construct few different bases for $\mathfrak{sl}_2$-current algebras.
  $\rightsquigarrow$ indeed, a characteristic-free construction of a basis for local Weyl modules for the hyper current algebra associated to $\mathfrak{sl}_2$.
- a basis that agree with truncations to give a basis for truncated local Weyl modules.

Preliminaries: the base simple Lie algebra – notation.

$\mathfrak{g}$: a finite-dimensional complex simple Lie algebra with a fixed Cartan subalgebra $\mathfrak{h}$.

- R the associated root system with a fixed choice of positive roots $R^+ \subseteq R$ and corresponding triangular decomposition $\mathfrak{g} = \mathfrak{n}^- \oplus \mathfrak{h} \oplus \mathfrak{n}^+$.
- I : indexing set for the nodes of the Dynkin diagram of $\mathfrak{g}$.
- $\{\alpha_i \mid i \in I\}$: the associated simple roots.
- $\{\omega_i \mid i \in I\}$: the fundamental weights.
- P^+ : the $\mathbb{Z}_+$-span of the fundamental weights of $\mathfrak{g}$.
- Q^+ : the $\mathbb{Z}_+$-span of the simple roots of $\mathfrak{g}$.
- $\{x_\alpha^\pm, h_i : \alpha \in R^+, i \in I\}$ a Chevalley basis of $\mathfrak{g}$.

Preliminaries: the current algebra

The *current algebra* of $\mathfrak{g}$ is the vector space

$$\mathfrak{g}[t] = \mathfrak{g} \otimes \mathbb{C}[t]$$

with a Lie algebra structure given by

$$[x \otimes f, y \otimes g] = [x, y] \otimes fg$$

for $x, y \in \mathfrak{g}$ and $f, g \in \mathbb{C}[t]$.

1. $\mathfrak{g} \otimes 1 \cong \mathfrak{g}$ is a subalgebra of $\mathfrak{g}[t]$
2. If $\mathfrak{b}$ is a subalgebra of $\mathfrak{g}$, then $\mathfrak{b}[t] = \mathfrak{b} \otimes \mathbb{C}[t]$ is naturally a subalgebra of $\mathfrak{g}[t]$. In particular,

$$\mathfrak{g}[t] = \mathfrak{n}^{-}[t] \oplus \mathfrak{h}[t] \oplus \mathfrak{n}^{+}[t].$$

3. The PBW theorem implies that the multiplication establishes isomorphisms

Local Weyl module

Definition of local Weyl module

Given $\lambda = \sum_{i=1}^{r} m_i\omega_i \in P^+$, the local Weyl module $W(\lambda)$ is the $U(\mathfrak{g}[t])$-module generated by an element v_λ with defining relations (for all $h \in U(\mathfrak{h}),\ \alpha \in R^+,\ k > \lambda(h_\alpha)$)

$$\mathfrak{n}^+[t]v_\lambda = \mathfrak{h} \otimes t\mathbb{C}[t]v_\lambda = (h - \lambda(h))v_\lambda = (x_\alpha^-)^{(k)}v_\lambda = 0.$$

1. Local Weyl modules are universal finite-dimensional highest weight modules.

Some commuting relations

Garland's formula (Garland '1978)

Let $\alpha \in R^+$, $a, b \in \mathbb{C}[t]$ and $\ell, k, m, n \in \mathbb{Z}_+$, $\ell \leq k$. We have

$$(x_\alpha^+ \otimes a)^{(\ell)}(x_\alpha^- \otimes b)^{(k)} = \left(\sum_{j=0}^{\infty} x_\alpha^- \otimes a^j b^{j+1}\ u^{j+1}\right)_k^{(k-\ell)}$$

$$\mod U(\mathfrak{g}[t])U(\mathfrak{h} \otimes t\mathbb{C}[t])^0 \oplus U(\mathfrak{g}[t])U(\mathfrak{n}^+[t])^0,$$

where the subindex k means the coefficient of u^k in the respective series and the n^{th}-power with parenthesis is the n^{th}-divided power of x by $x^{(n)} = \frac{x^n}{n!}$.

...using these commuting relations

“Garland’s formula” applied to a generator of $W(\lambda)$

Let $\alpha \in R^+$ and $\ell, k \in \mathbb{Z}_+$ with $0 \leq \ell \leq k, k > \lambda(h_\alpha)$. We have

$$(x_\alpha^+ \otimes t)^{(\ell)}(x_\alpha^- \otimes 1)^{(k)} v_\lambda = \left(\sum_{j=0}^{\infty} x_\alpha^- \otimes t^j \, u^{j+1} \right)_k^{(k-\ell)} v_\lambda + T v_\lambda$$

for some $T \in U(\mathfrak{g}[t])U(\mathfrak{h} \otimes t\mathbb{C}[t])^0 \oplus U(\mathfrak{g}[t])U(\mathfrak{n}^+[t])^0$.

...using these commuting relations

“Garland’s formula applied"to a generator of $W(\lambda)$

Let $\alpha \in R^+$ and $\ell, k \in \mathbb{Z}_+$ with $0 \leq \ell \leq k, k > k > \lambda(h_\alpha)$. We have

$$(x_\alpha^+ \otimes t)^{(\ell)} \underbrace{(x_\alpha^- \otimes 1)^{(k)} v_\lambda}_{=0} = \underbrace{T v_\lambda}_{=0} + \left(\sum_{j=0}^{\infty} x_\alpha^- \otimes t^j \; u^{j+1} \right)_k^{(k-\ell)} v_\lambda = 0$$

since we have $U(\mathfrak{g}[t])U(\mathfrak{h} \otimes t\mathbb{C}[t])^0 v_\lambda = 0$ and $U(\mathfrak{g}[t])U(\mathfrak{n}^+[t])^0 v_\lambda = 0$ due to the defining relations of $W(\lambda)$.

Conclusion:

$$\left(\sum_{j=0}^{\infty} x_\alpha^- \otimes t^j \; u^{j+1} \right)_k^{(k-\ell)} v_\lambda = 0$$

How to get a monomial basis for $W(\lambda)$?

Let $\mathcal{J}_\lambda$ be the ideal of $U(\mathfrak{n}^-[t])$ generated by the set

$$\{X_\alpha(u)_k^{(k-\ell)} | 0 \leq \ell \leq k,\ \lambda(h_\alpha) < k\},$$

where

$$X_\alpha(u) = \sum_{j=0}^{\infty} x_\alpha^- \otimes t^j\ u^{j+1}$$

The map $U(\mathfrak{n}^-[t]) \to W(\lambda)$ sending g to $g\omega_\lambda$ induces an isomorphism of vector spaces

$$U(\mathfrak{g}[t])/\mathcal{R} \equiv U(\mathfrak{n}^-[t])/\mathcal{J}_\lambda \equiv W(\lambda).$$

The case $\mathfrak{g} = \mathfrak{sl}_2$

1. I is singleton for $\mathfrak{sl}_2$.

   We simplify notation

$$\omega := \omega_1, \quad x^{\pm} := x^{\pm}_{\alpha_1}, \quad h := h_1, \quad \alpha := \alpha_1, \quad X(u) := X_\alpha(u).$$

2. P^+ is in a bijective correspondence with $\mathbb{Z}_+$

   We denote by m the weigth $m\omega$ and $v_m = v_{m\omega}$.

Passing to a polynomial setting

$\mathbb{C}_\infty$: polynomial ring in infinite many variables.

$\mathbb{C}_m$: polynomial ring in finitely many variables.

1. $\phi : U(\mathfrak{n}^-[t]) \to \mathbb{C}_\infty$ defined by $(x^- \otimes t^r)^k \mapsto x_r^k$ for all $r, k \in \mathbb{Z}_+$ is an isomorphism.
2. Let J_m the ideal in $\mathbb{C}_m$ corresponding to $\mathcal{J}_m$.
3. ϕ and the inclusion $\mathbb{C}_m \hookrightarrow \mathbb{C}_\infty$ provide us the isomorphism

$$\mathbb{C}_m/J_m \cong U(\mathfrak{n}^-[t])/\mathcal{J}_m \cong W(m)$$

CONCLUSION:

$$\dim W(m) = \dim \mathbb{C}_m/J_m.$$

The main theorem.

Theorem - B., Wilson '2016

The set of leading monomials with respect to lexicographic order of a reduced Gröbner basis G_m of J_m is $\{x_0^{(a_0)} \cdots x_{m-r+1}^{(a_{m-r+1})} | r \in \mathbb{Z}_{\geq 2}, a_0 + a_1 + \cdots + a_{m-r+1} = r, a_{m-r+1} \neq 0\}$.

The proof is very combinatorial and use "some group action" with:

- Kostka numbers
- Jacobi-Trudi determinant formula
- Complete (homogeneous) symmetric polynomial

Corollary - (Lexicographic basis) – B., Wilson '2016

$\{x_0^{(a_0)} \cdots x_{m-r}^{(a_{m-r})} | r \in \mathbb{Z}_{\geq 0}, a_0 + a_1 + \cdots + a_{m-r} = r\}$ is a monomial $\mathbb{C}$-linear basis of $\frac{\mathbb{C}_m}{J_m}$. In particular, $\dim\left(\frac{\mathbb{C}_m}{J_m}\right) = 2^m = \dim W(m)$.

The main theorem

Remarks

- Chari-Pressley's construction produces this same basis over $\mathbb{C}$.
- B.-Wilson's construction is valid for an arbitrary characteristic base field in the context of hyperalgebras.

Corollary - (Reverse Lexicographic basis) – B., Wilson '2016

Let

$$\mathcal{R}_1 = \{x_0^{f_0} x_1^{f_1} \cdots x_{m-1}^{f_{m-1}} v_m \mid \sum_{i=0}^{m-1} f_i \leq \frac{m}{2}, (i-1)f_i + if_{i+1} \leq m - 2\sum_{j=i}^{m-1} f_j, \text{ for } 1 \leq i \leq m-2$$

and

$$\mathcal{R}_2 = \{x_0^{f_0} x_1^{f_1} \cdots x_{m-1}^{f_{m-1}} v_m \mid \sum_{i=0}^{m-1} f_i = k > \frac{m}{2} \text{ and } x_0^{m-2k+f_0} x_1^{f_1} \cdots x_{m-1}^{f_{m-1}} \in \mathcal{R}_1\}.$$

The set $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$ is a basis for $W(m)$ over $\mathbb{C}$.

The truncated local Weyl module

If we consider *mutatis mutandis* the definition of local Weyl modules $W(m)$ for $U(\mathfrak{sl}_2 \otimes \mathbb{C}[t])$ replacing $\mathbb{C}[t]$ by $\frac{\mathbb{C}[t]}{\langle t^k \rangle}$, we construct the so called *k-truncated local Weyl module* $W^k(m)$.

Theorem – B., Wilson '2016

Let $m, k \in \mathbb{Z}_+$.

1. The main theorem of this work with the **reverse** lexicographical order produces a monomial basis for $W(m)$ which "contains" (in the sense of the monomials) a basis for $W^k(m)$.
2. Write $m = nk + j$ with $0 \leq j < k$. Then,

$$\dim W^k(m) = (n+1)^{k-j}.(n+2)^j.$$

Explicit example $\mathfrak{g} = \mathfrak{sl}_2$ and $m = 3$.

$\diamond$ Lexicographic order:

$$W(3) = span_{\mathbb{C}}\{v_3, x^- v_3, x^- \otimes t v_3, (x^- \otimes t^2)v_3, (x^-)^2 v_3, x^-(x^- \otimes t)v_3, (x^-)^3 v_3, (x^- \otimes t)^2 v_3\}$$

$\diamond$ Reverse Lexicographic order:

$$W(3) =$$

$$= span_{\mathbb{C}}\{v_3, x^- v_3, x^- \otimes t v_3, (x^- \otimes t^2)v_3, (x^-)^2 v_3, x^-(x^- \otimes t)v_3, (x^-)^3 v_3, x^-(x^- \otimes t^2)v_3\}$$

$\diamond$ A truncated basis for $k = 2$ with the reverse lexicographic order:

$$W^2(3) = span_{\mathbb{C}}\{\dot{v}_3, x^- \dot{v}_3, x^- \otimes t \dot{v}_3, (x^-)^2 \dot{v}_3, x^-(x^- \otimes t)\dot{v}_3, (x^-)^3 \dot{v}_3\}$$

$\diamond$ A “wrong construction of a truncated basis” for $k = 2$ would be:

$$W^2(3) = span_{\mathbb{C}}\{\dot{v}_3, x^- \dot{v}_3, x^- \otimes t \dot{v}_3, (x^-)^2 \dot{v}_3, x^-(x^- \otimes t)\dot{v}_3, (x^-)^3 \dot{v}_3, (x^- \otimes t)^2 \dot{v}_3\}$$

Beyond the $\mathfrak{sl}_2$-case.

$U(\mathfrak{n}^-[t])$ is not commutative !!!

We can work on an (almost) polynomial quocient rings by using Shirshov–Gröbner bases in $U(\mathfrak{n}^-[t])/\mathcal{J}_\lambda$

The advantage of the ***"methods a la Shirshov-Gröbner"*** is the uniformity and validity for Universal Enveloping algebra and the Basis Theorem.

Obrigado!!!

Referências Bibliográficas

A. Bianchi, T. Macedo, and A. Moura *On Demazure and local Weyl modules for affine hyperalgebras*, Pacific J. Math. **274** (2015), p. 257–303.

V. Chari, G. Fourier, and T. Khandai, *A categorical approach to Weyl modules*, Transf. Groups **15** (2010), 517–549.

V. Chari and A. Pressley, *Weyl modules for classical and quantum affine algebras*, Represent. Theory **5** (2001), 191–223.

Cox, D., Litlle, J., and O'Shea, D., *Ideals, Varieties and Algorithms - An Introduction to Computational Geometry and Commutative Algebra*, Springer-Verlag, New York-Berlin-Heidelberg, 1996.

B. Feigin and S. Loktev,*Multi-dimensional Weyl modules and symmetric functions*, Comm. Math. Phys. **251** (2004), 427-?445.

H. Garland, *The arithmetic theory of loop algebras*, J. Algebra **53** (1978), 480–551.

D. Jakelic and A. Moura, *Finite-dimensional representations of hyper loop algebras*, Pacific J. Math. **233** (2007), no. 2, 371–402.