Álgebra e Combinatória

Editor Convidado: Olga Azenhas

Riordan arrays from an umbral symbolic viewpoint

José Agapito Ruiz
Centro de Estruturas Lineares e Combinatórias
Departamento de Matemática, Faculdade de Ciências
Universidade de Lisboa
Campo Grande, 1749-016 Lisboa, Portugal
e-mail: jagruiz@cii.fc.ul.pt

Resumo: Esta nota salienta uma caracterização alternativa das matrizes de Riordan baseada numa renovada abordagem simbólica do cálculo umbral.

Abstract This note highlights an alternative characterization of Riordan arrays based on a symbolic renewed approach to umbral calculus.

keywords: Riordan arrays; umbrae; recurrence relations

1 Introduction

A Riordan array R is an infinite lower triangular matrix generated by a pair of formal series, $g(z) = 1 + g_1 z + g_2 z^2/2! + g_3 z^3/3! + \cdots$ and $f(z) = f_1 z + f_2 z^2/2! + f_3 z^3/3! + \cdots$, such that $R_{n,k} = [z^n/n!]\big(g(z) f(z)^k/k!\big)$ for $n \geq k \geq 0$. For example, the well-known Pascal array of binomial coefficients is a Riordan array generated by (e^z, z). If (g, f) is any Riordan array and $A = (a_0, a_1, a_2, \ldots)^T$ and $B = (b_0, b_1, b_2, \ldots)^T$ are column vectors with corresponding generating functions $A(z)$ and $B(z)$, then $(g, f)A = B$ if and only if $g(z)A\big(f(z)\big) = B(z)$. This result is known as the fundamental theorem of Riordan arrays. Furthermore, given any two Riordan arrays (g, f) and (h, l), we can obtain another Riordan array as follows,

$$\Big(g(z), f(z)\Big)\Big(h(z), l(z)\Big) = \Big(g(z)\, h\big(f(z)\big), l\big(f(z)\big)\Big). \tag{1}$$

The Riordan array $(1, z)$ is the *identity* with respect to this multiplication. Since $1 = g_0 \neq 0$, the formal series g has multiplicative inverse g^{-1}. Likewise, if $f_1 \neq 0$ the formal series f has compositional inverse $f^{\langle -1\rangle}$. Under these conditions, a Riordan array (g, f) is invertible with respect to (1) and its inverse is given by $\big(g(z), f(z)\big)^{-1} = \big(1/g(f^{\langle -1\rangle}(z))\,,\, f^{\langle -1\rangle}(z)\big)$. The *Riordan group* is the set of all invertible Riordan arrays, together with multiplication (1) as the group operation. The aim of this work is to give a brief account of a promising symbolic approach to the theory of Riordan arrays [5, 6] using a renewed umbral symbolic language [2, 4].

2 The umbral symbolism

Let A be a collection of symbols (typically Greek letters), that we call *umbrae*, together with a linear functional $E : \mathbb{C}[A] \to \mathbb{C}$ called *evaluation* such that $E[1] = 1$ and $E[\alpha^i\gamma^j \cdots \omega^k] = E[\alpha^i]E[\gamma^j] \cdots E[\omega^k]$, for $\alpha, \gamma, \ldots, \omega$ pairwise distinct. An umbra ω is said to represent a sequence $(w_n)_{n\in\mathbb{N}}$ in $\mathbb{C}$ if $E[\omega^n] = w_n$. We assume $E[\omega^0] = 1$. Two umbrae ω and γ are said to be *umbral equivalent* if $E[\omega] = E[\gamma]$, which is denoted by $\omega \simeq \gamma$, and *similar* if $E[\omega^n] = E[\gamma^n]$ for all $n \in \mathbb{N}$, which is denoted by $\omega \equiv \gamma$. The generating function (g.f. for short) of an umbra ω is the exponential formal series $e^{\omega z} := 1 + \sum_{n\geq 1} \omega^n \frac{z^n}{n!} \in \mathbb{C}[A]\,[[z]]$. By linearly extending the action of E, we shall write $f_\omega(z) = E[e^{\omega z}]$; or equivalently, $f_\omega(z) \simeq e^{\omega z}$. Some distinguished umbrae that play a crucial role in this symbolic method are: the *augmentation* umbra, denoted by ε, whose g.f. is $e^{\varepsilon z} \simeq 1$; the *unity* umbra, denoted by υ, with g.f. $e^{\upsilon z} \simeq e^z$; the *singleton* umbra, denoted by χ, having g.f. $e^{\chi z} \simeq 1 + z$ and the *Bell* umbra, denoted by β, whose g.f. is $e^{\beta z} \simeq e^{e^z-1}$. Note that $\omega \equiv \gamma$ if and only if $f_\omega(z) = f_\gamma(z)$. It is convenient to assume that each monic sequence $(w_n)_{n\in\mathbb{N}}$ in $\mathbb{C}$ ($w_0 = 1$) can be represented by infinitely many similar umbrae. This property is called *saturation*. We further enlarge A by including *auxiliary* symbols obtained from formal operations on umbrae. For instance, we define the dot product $\gamma.\alpha$ of γ and α by $f_{\gamma.\alpha}(z) := f_\gamma\big(\log f_\alpha(z)\big)$. We can readily verify that $\alpha.\varepsilon \equiv \varepsilon \equiv \varepsilon.\alpha$ and $\alpha+\varepsilon \equiv \alpha \equiv \varepsilon+\alpha$. Similarly, it follows that $\alpha+(-1).\alpha \equiv \varepsilon \equiv (-1).\alpha+\alpha$, that $\alpha.\upsilon \equiv \alpha \equiv \upsilon.\alpha$ and that $\beta.\chi \equiv \upsilon \equiv \chi.\beta$. Likewise, we call $\gamma.\beta.\alpha$ the composition umbra of γ and α, since $f_{\gamma.\beta.\alpha} = f_\gamma(f_\alpha(z) - 1)$. The compositional inverse of γ is denoted by $\gamma^{\langle -1\rangle}$ and satisfies $\gamma^{\langle -1\rangle}.\beta.\gamma \equiv \chi \equiv \gamma.\beta.\gamma^{\langle -1\rangle}$. More auxiliary umbrae can be obtained by suitable operations on umbrae. For instance, the *derivative* umbra $\alpha_{\mathcal{D}}$ of α is defined as the umbra that satisfies $\alpha^n_{\mathcal{D}} \simeq n\,\alpha^{n-1}$. Appropriate combinations of these operations and auxiliary umbrae yield useful umbral identities. For example, it can be checked that $(\alpha + \gamma.\beta.\alpha_{\mathcal{D}})_{\mathcal{D}} \equiv \gamma_{\mathcal{D}}.\beta.\alpha_{\mathcal{D}}$. In addition, setting $\mathfrak{L}_{\gamma,\alpha} \equiv -1.\gamma.\beta.\alpha^{\langle -1\rangle}_{\mathcal{D}}$, we have $(\mathfrak{L}_{\alpha,\alpha})_{\mathcal{D}} \equiv \alpha^{\langle -1\rangle}_{\mathcal{D}}$ when $\gamma \equiv \alpha$. In particular, it follows that $\mathfrak{L}_{\mathfrak{L}_{\alpha,\alpha}} \equiv \alpha$. For the sake of simplicity, we set $\mathfrak{L}_\alpha := \mathfrak{L}_{\alpha,\alpha}$.

3 Riordan arrays from an umbral point of view

Consider $g(z)$ as in Section1 and, without loss of generality, consider $f(z) = z+f_2z^2/2!+f_3z^3/3!+\cdots$. Let γ and α be any umbrae such that $g(z) \simeq e^{\gamma z}$ and $f(z) \simeq ze^{\alpha z}$. It follows that $E\big[\binom{n}{k}\,(\gamma+k.\alpha)^{n-k}\big] = \big[z^n/n!\big]g(z)\,f(z)^k/k!$. Hence,

we denote by (γ, α) the (exponential) Riordan array whose entries are given by $(\gamma, \alpha)_{n,k} \simeq \binom{n}{k} (\gamma + k.\alpha)^{n-k}$. Observe that the binomial core of any Riordan array is stressed by the umbral notation. In particular, the Pascal array is now denoted by (υ, ε). As $(\gamma, \alpha)_{n,n} = 1$ for all $n \in \mathbb{N}$, the corresponding invertible Riordan arrays are called *normalized*. Note that not all invertible Riordan arrays are normalized but any of them have a normalized version. The fundamental theorem of Riordan arrays is correspondingly encoded by $(\gamma, \alpha)\eta = \gamma + \eta.\beta.\alpha_{\mathcal{D}}$. This is equivalent, for all $n \geq 0$, to the expression

$$(\gamma + \eta.\beta.\alpha_{\mathcal{D}})^n \simeq \sum_{k=0}^{n} \binom{n}{k} (\gamma + k.\alpha)^{n-k} \eta^k \,. \tag{2}$$

Formula (2) is a restatement of a direct, though far from trivial generalization of Abel's identity for polynomials; that is,

$$(\gamma + \sigma)^n \simeq \sum_{k=0}^{n} \binom{n}{k} (\gamma + k.\alpha)^{n-k} \sigma \big(\sigma + (-k).\alpha\big)^{k-1} \quad .$$

Likewise, the multiplication of Riordan arrays is now written as

$$(\gamma, \alpha)(\sigma, \rho) = (\gamma + \sigma.\beta.\alpha_{\mathcal{D}} \,,\, \alpha + \rho.\beta.\alpha_{\mathcal{D}}) \,. \tag{3}$$

The identity is $(\varepsilon, \varepsilon)$ and the inverse of (γ, α) is $(\gamma, \alpha)^{-1} = (\mathfrak{L}_{\gamma,\alpha}, \mathfrak{L}_{\alpha})$. By way of illustration, we shall now describe three important Riordan subgroups. Arrays of type $(g(z), z)$ form the Appell subgroup and are umbrally encoded as (γ, ε). Thus, $(\gamma, \varepsilon)^{-1} = (-1.\alpha, \varepsilon)$ and $(\gamma, \varepsilon)_{n,k} = \binom{n}{k} \gamma^{n-k}$. The Associated subgroup is formed by arrays of type $(1, f(z))$, which are umbrally encoded as (ε, α), so that $(\varepsilon, \alpha)^{-1} = (\varepsilon, \mathfrak{L}_{\alpha})$ and $(\varepsilon, \alpha)_{n,k} = \binom{n}{k} \big(k.\alpha\big)^{n-k}$. Finally, arrays of type $(g(z), zg(z))$ form the Bell subgroup and are umbrally denoted by (α, α), so that $(\alpha, \alpha)^{-1} = (\mathfrak{L}_{\alpha}, \mathfrak{L}_{\alpha})$ and $(\alpha, \alpha)_{n,k} = \binom{n}{k} ((k+1).\alpha)^{n-k}$. The umbral notation simplifies the verification of many aspects of the theory of Riordan arrays. For instance, a straightforward use of (3) yields $(\gamma, \varepsilon)(\sigma, \varepsilon) = (\gamma + \sigma, \varepsilon)$ for the Appell subgroup, implying immediately that it is an Abelian subgroup. Riordan arrays are also characterized by recurrence relations. Direct nontrivial consequences of the umbral Abel identity are the following results.

Theorem 1. *For any umbra λ and any integers m and $n, k \geq 1$, it holds*

$$(\gamma, \alpha)_{n,k} \simeq \binom{n}{k} \sum_{i=0}^{n-k} \Big((-m).\mathfrak{L}_{\alpha,\lambda}\Big)^i \, (\gamma + (k-m).\alpha, \lambda)_{n-k,i} \quad .$$

Theorem 2. *For any integers $k \geq m$, $n \geq m$ such that $n, k \geq 1$, it holds*

$$(\gamma, \alpha)_{n,k} \simeq \frac{n!(k-m)!}{k!(n-m)!} \sum_{i=0}^{n-k} \binom{k-m+i}{i} \left((-m).\mathfrak{L}_\alpha\right)^i (\gamma, \alpha)_{n-m,k-m+i} \quad .$$

4 Final Remarks

Specializing the umbrae γ, α and λ in Theorems 1 and 2, we obtain, after translating the resulting formulas into the language of generating functions, exponential analogues of known recurrence relations for ordinary Riordan arrays [3]. Much more can be said and unveiled using this symbolic approach. An extended discussion of Riordan arrays and other related topics from this point of view is shown in [1].

Acknowledgements

This work was done within the activities of Centro de Estruturas Lineares e Combinatórias (Universidade de Lisboa) and was partially supported by the Portuguese Science and Technology Foundation (FCT) through the program Ciência 2008 and grant PTDC/MAT/099880/2008.

References

[1] J. Agapito, A. Mestre, P. Petrullo and M. M. Torres, *A symbolic treatment of Riordan arrays*, Submitted (2012).

[2] E. Di Nardo and D. Senato, *Umbral nature of the Poisson random variables*, Algebraic Combinatorics and computer science, Springer, Italia, 2001, pp. 245–266.

[3] A. Luzón, D. Merlini, M. A. Morón and R. Sprugnoli, *Identities induced by Riordan arrays*, Linear Algebra Appl. **436** (3), pp. 631–647 (2012).

[4] G. C. Rota and B. Taylor, *The classical umbral calculus*, SIAM J. Math. Anal., **25**, pp. 694–711 (1994).

[5] L. W. Shapiro, S. Getu, W-J. Woan and L. C. Woodson, *The Riordan group*, Discrete Appl. Math. **34** (1-3), pp. 229–239 (1991).

[6] R. Sprugnoli, *Riordan arrays and combinatorial sums*, Discrete Math. **132**: 267–290 (1994).

Um problema de grandes denominadores

Assis Azevedo
Departamento de Matemática e Aplicações / Centro de Matemática
Universidade do Minho
e-mail: assis@math.uminho.pt

Maria Carvalho, *António Machiavelo*
Departamento de Matemática / Centro de Matemática
Faculdade de Ciências da Universidade do Porto
e-mails: mpcarval@fc.up.pt; ajmachia@fc.up.pt

Resumo: Fixado $M \in \mathbb{N}$, escolhamos aleatoriamente $a_1 \in \mathbb{N}$ e consideremos $M_1 = \frac{M}{(M,a_1)}$. Repita-se este procedimento, seleccionando ao acaso a_2 e definindo $M_2 = \frac{M_1}{(M_1,a_2)}$, e assim sucessivamente. Dados $M, n \in \mathbb{N}$, qual é a probabilidade, digamos $\mathcal{P}(n, M)$, de ser $M_n = 1$? Tem-se $\mathcal{P}(1, M) = \frac{1}{M}$ e a relação de recorrência $\mathcal{P}(n+1, M) = \sum_{d|M} \frac{\varphi(d)}{M} \mathcal{P}(n, d)$, onde φ é a função de Euler. O que implica que, com probabilidade um, $M_n = 1$ para algum $n \in \mathbb{N}$. O sistema dinâmico discreto associado à aplicação $\chi : \mathbb{Q} \to \mathbb{Q}$ dada por $\chi(x) = x\lceil x \rceil$ simula o comportamento deste processo aleatório, tratando-se agora de saber se a órbita por χ de qualquer racional de $[1, +\infty[$ entra em $\mathbb{Z}$. Em [1], provou-se que o conjunto das fracções irredutíveis com denominador M cujas órbitas entram em $\mathbb{Z}$ no n-ésimo iterado é uma união disjunta de classes de congruência módulo M^{n+1}. Este resultado sugeriu um algoritmo eficiente para decidir se um racional está nesta união e, do número daquelas classes, deduzimos que, com probabilidade 1, a órbita de um racional de $[1, +\infty[$ entra em $\mathbb{Z}$.

Abstract: Given $M \in \mathbb{N}$, suppose one randomly chooses $a_1 \in \mathbb{N}$, sets $M_1 = \frac{M}{(M,a_1)}$, then repeats the process by randomly sorting out a_2 and letting $M_2 = \frac{M_1}{(M_1,a_2)}$, and so on. Given $M, n \in \mathbb{N}$, what is the probability, say $\mathcal{P}(n, M)$, that $M_n = 1$? Clearly $\mathcal{P}(1, M) = \frac{1}{M}$ and the numbers $P(n, M)$ satisfy the recurrence relation $\mathcal{P}(n+1, M) = \sum_{d|M} \frac{\varphi(d)}{M} \mathcal{P}(n, d)$, where φ is the Euler function. This implies that, with probability one, $M_n = 1$ for some n. The map $\chi : \mathbb{Q} \to \mathbb{Q}$ given by $\chi(x) = x\lceil x \rceil$ induces a deterministic dynamical system modeling this random behavior. The question we address now is whether the orbit by χ of any rational bigger than 1 enters $\mathbb{Z}$. In [1] we proved that the set of irreducible fractions with denominator M whose orbits by χ reach an integer in exactly n iterations is a disjoint union of congruence classes modulo M^{n+1}. The proof of this result suggested how to build an efficient algorithm to decide if an orbit fails to hit an integer before a prescribed number of iterations have elapsed. Besides, from the number of those classes, we deduced that, with probability 1, the orbit of a rational in $[1, +\infty[$ enters $\mathbb{Z}$.

palavras-chave: sistemas dinâmicos discretos; função tecto; densidade; cobertura.

keywords: discrete dynamical system; ceiling function; density; covering system.

1 Introdução

Consideremos o sistema dinâmico discreto associado à aplicação $\chi : \mathbb{Q} \to \mathbb{Q}$ dada por $\chi(x) = x\lceil x \rceil$, onde $\lceil x \rceil = \min\{z \in \mathbb{Z} : x \leq z\}$. Para $\frac{p}{q} \geq 1$, onde $p, q \in \mathbb{N}$ e $(p, q) = 1$, o j-ésimo iterado $\chi^j\left(\frac{p}{q}\right)$ é uma fracção irredutível $\frac{p_j}{q_j}$, onde q_{j+1} divide q_j. Por exemplo, os primeiros iterados de $\frac{31}{10}$ são $\frac{62}{5}$, $\frac{806}{5}$, $\frac{130572}{5}$, 681977556. O número j de iterações de χ necessárias para que se tenha $q_j = 1$ pode ser arbitrariamente grande, mas a análise numérica desta dinâmica sugere que existe sempre um tal j.

Para $x \in \mathbb{Q}$, defina-se *ordem de* x como $\mathcal{O}(x) = \min\{k \in \mathbb{N}_0 : \chi^k(x) \in \mathbb{Z}\}$, se este conjunto é não vazio, e $\mathcal{O}(x) = \infty$ caso contrário. Note-se que: $\mathcal{O}(x) = 0$ se e só se $x \in \mathbb{Z}$; $\mathcal{O}(]0, 1[) = \{\infty\}$; se $x < -1$ então $\chi(x) > 1$. Basta-nos portanto estudar a ordem dos racionais maiores do que 1.

Dado um natural ímpar $a > 1$, digamos $a = 2^k b + 1$ com $k, b \in \mathbb{N}$ e b ímpar, usando indução em k concluímos que $\mathcal{O}\left(\frac{a}{2}\right) = k$. Logo a menor fracção com denominador 2 e ordem k é $\frac{2^k+1}{2}$, que cresce exponencialmente com k. A Figura 1 mostra que, pelo contrário, para denominador 3 há valores baixos de a com ordens elevadas.

ordem	menor natural a	ordem	menor natural a	ordem	menor natural a
1	7	18	2 215	35	6 335 903
2	4	19	6 151	36	1 180 939
3	13	20	8 653	37	1 751 431
4	20	21	280	38	10 970 993
5	10	22	28	39	17 545 207
6	5	23	1 783	40	66 269 497
7	29	24	81 653	41	27 952 480
8	76	25	19 310	42	60 284 614
9	50	26	114 698	43	203 071 951
10	452	27	18 716	44	191 482 466
11	244	28	196 832	45	144 756 173
12	830	29	15 214	46	45 781 445
13	49	30	7 148	47	1 343 664 136
14	91	31	273 223	48	223 084 774
15	319	32	3 399 188	49	1 494 753 473
16	2 639	33	398 314	50	20 110 862
17	5 753	34	6 553 568		

Figura 1: Menor natural a tal que $\frac{a}{3}$ tem ordem entre 1 e 50.

Apesar dos valores dos iterados de χ crescerem muito depressa (por exemplo, $\mathcal{O}\left(\frac{28}{3}\right) = 22$ e $\chi^{22}(\frac{28}{3})$ é um natural com 4 134 726 dígitos), estas experiências numéricas foram possíveis pela natureza dinâmica do problema e pela caracterização dos racionais com denominador dado e ordem fixada como os elementos de uma classe de congruência módulo uma potência do

denominador, o que tornou possível lidar apenas com numeradores até essa potência (e, por exemplo, verificar que $\mathcal{O}(a/3) \leq 56$ se $a \leq 2\,000\,000\,000$).

O problema que aqui consideramos tem alguma analogia tanto com o problema de Collatz [2] como com a conjectura de Erdös-Straus [3]: embora também correspondam a um subconjunto com densidade assimptótica total, não sabemos se as classes de congruência que descrevem os racionais com ordem finita formam uma cobertura dos inteiros.

2 Racionais com ordem finita

Por indução, deduzimos em [1] que, dados $n \in \mathbb{N}_0$ e $M \in \mathbb{N}$,

Proposição 1 *O conjunto* $\mathcal{A}_{n,M} = \{a \in \mathbb{Z} : (a, M) = 1 \text{ e } \mathcal{O}\left(\frac{a}{M}\right) = n\}$ *é uma união disjunta de* $A(n, M)$ *classes de congruência módulo* M^{n+1}.

Consequentemente,

Corolário 2 *A probabilidade,* $\mathcal{P}^*(n, M)$, *de* $\frac{a}{M}$, *com* $(a, M) = 1$, *ter ordem* n, *é igual a* $\frac{A(n,M)}{\varphi(M^{n+1})}$.

Note-se que $A(0, 1) = 1$, $A(n, 1) = 0$ se $n \in \mathbb{N}$ e, para $M > 1$, $A(0, M) = 0$, $A(1, M) = \varphi(M)$.

Teorema 3 *Se* $M > 1$ *ou* $n > 1$, *tem-se*

$$A(n, M) = \varphi(M) \sum_{d|M} A(n-1, d) \left(\frac{M}{d}\right)^{n-1}$$

ou, equivalentemente, $\mathcal{P}^*(n, M) = \sum_{d|M} \frac{\varphi(d)}{M} \mathcal{P}^*(n-1, d)$. *Em particular, se* p *é primo e* $k \in \mathbb{N}$, $A(n, p^k) = \binom{n+k-2}{n-1} \left(\varphi(p^k)\right)^n$.

Deste modo, a probabilidade de um número racional $\frac{a}{M}$, com $(a, M) = 1$ ter ordem n é igual à probabilidade de, começando com o inteiro M, o processo aleatório descrito no Resumo terminar após n passos.

3 Racionais com ordem infinita

Não conhecemos nenhum racional no complementar de $[0, 1]$ com ordem infinita. Contudo, se existirem, formam um conjunto pequeno. Usando a Proposição 1 e o Teorema 3, mostrámos em [1] que a probabilidade de um racional de $[1, +\infty[$ ter ordem finita é igual a 1.

n \ M	6	10	12	14	15	18	20
2	18	68	112	150	240	270	416
3	86	628	1 424	2 058	3 872	5 670	9 952
4	354	5 060	13 952	24 774	52 800	93 798	184 576
5	1 382	39 124	120768	287 466	668 288	1 396 278	3 048 576

Figura 2: Valor de $A(n, M)$ para $2 \leq n \leq 5$, $M \leq 20$, M não potência de primo.

4 O algoritmo

Consideremos $\frac{a}{M}$ e a sucessão $(a_n)_{n\in\mathbb{N}_0}$ definida por $a_0 = a$, $a_{n+1} = M\,\chi\left(\frac{a_n}{M}\right)$. Sabemos que, se $\mathcal{O}(\frac{a}{M}) \leq N$, então, dado $1 \leq s < N$, $\mathcal{O}(\frac{a_s}{M}) \leq N - s$. Além disso, pela Proposição 1, podemos substituir a_s pelo resto da divisão de a_s por M^{N+1-s}. Assim, $\mathcal{O}(\frac{a}{M})$ é o menor $s \in \mathbb{N}_0$ tal que a_s é um múltiplo de M. Note-se que, neste procedimento, só lidamos com naturais inferiores a M^{N+1} e que, em cada etapa, este limite diminui. Em resumo, o algoritmo actua do seguinte modo: dados $M \in \mathbb{N}$, $a \in \mathbb{Z}$ e $N \in \mathbb{N}$, considera $\frac{a}{M}$, o resto r_0 da divisão de a por M^{N+1} e, em geral, o resto r_{n+1} da divisão de $M\,\chi\left(\frac{a_n}{M}\right)$ por M^{N+1-s}; e conclui que

$$\mathcal{O}\left(\frac{a}{M}\right) = \begin{cases} k, & \text{se existe } k \leq N:\ M \mid r_k \text{ e } M \nmid r_s \text{ para todo o } s < k \\ > N, & \text{caso contrário.} \end{cases}$$

Trabalho parcialmente financiado pela Fundação para a Ciência e Tecnologia (FCT), através do Centro de Matemática da Universidade do Minho, do Centro de Matemática da Universidade do Porto, do Projecto FCT UT-Austin/MAT/0035/2008 e do Programa POSI.

Referências

[1] A. Azevedo, M. Carvalho, A. Machiavelo, *Dynamics of a quasi-quadratic map*, arXiv:1210.0042 [math.NT].

[2] R. Terras, *A Stopping Time Problem on the Positive Integers*, Acta Arithmetica XXX (1976), pp. 241–252.

[3] W. A. Webb, *On* $4/n = 1/x + 1/y + 1/z$, Proceedings of the American Mathematical Society 25 (1970), pp. 578–584.

Formas semidefinidas positivas e somas de quadrados

Carla Fidalgo
Instituto Superior de Engenharia de Coimbra
e-mail: cfidalgo@isec.pt

Resumo: Usando a teoria das agiformas de Reznick obtêm-se condições suficientes, fáceis de testar, para uma forma ser soma de quadrados, uma das quais é linear nos coeficientes do polinómio, tal como as de Lasserre, mas obtida de modo completamente diferente.

Abstract Using the Reznick's theory of agiformas one obtains sufficient conditions, easy to test, for a form to be sum of squares, one of which is linear in the coefficients of the polynomial, such as those of Lasserre, but made quite differently.

palavras-chave: somas de quadrados; semidefinipositividade.

keywords: sums of squares; positive semidefinitness.

1 Introdução

A questão da representação de polinómios homogéneos (formas) semidefinidos positivos (sdp)(i.e., não negativos para todas as concretizações das variáveis) como soma de quadrados (sdq) tem uma longa história, que começa com a tese de doutoramento de Minkowski, onde era afirmado ser pouco provável que toda a forma sdp positiva fosse sdq de formas. Contudo os primeiros exemplos explícitos de formas que sendo sdp não são sdq foram dados por Motzkin, em 1967, e pouco depois por Robinson. Com o virar do milénio o interesse nesta matéria aumentou consideravelmente, em boa parte devido ao importante papel da optimização. Se tivermos em consideração que Blekherman mostrou recentemente que para um dado grau a probabilidade de uma forma sdp ser sdq tende para zero à medida que o número de variáveis aumenta, percebemos o interesse de encontrar uma classe infinita de formas para as quais ser sdp é condição suficiente para ser sdq.

É bem conhecido que no que diz respeito a semidefinipositividade e a soma de quadrados é indiferente trabalhar com polinómios ou formas

Lema. Seja $P(x_1, \ldots, x_n)$ um polinómio de grau m e $P_h(x_1, \ldots, x_n, x_{n+1})$ a sua homogeneização relativamente a x_{n+1}. Então

i. P é semidefinido positivo se e só se P_h for semidefinido positivo.

ii. P é soma de quadrados se e só se P_h for soma de quadrados.

Em [1] Reznick mostra que as formas $F(\underline{a},\underline{x}) = a_1x_1^{2d} + \cdots + a_nx_n^{2d} - 2dx_1^{a_1}\cdots x_n^{a_n}$, com a_i inteiros não negativos e de soma $2d$, podem ser escritas como somas de, quando muito, $3n-4$ quadrados de polinómios.

Usamos um dos resultados de Reznick para as agiformas de Hurwitz, para mostrar que formas diagonal menos cauda (dmc) semidefinidas positivas são soma de quadrados.

2 Formas diagonal menos cauda sdp são sdq

A representação de um polinómio homogéneo como uma soma $P = P_1 + \cdots + P_k$ de formas não-nulas P_i, tais que para todos os $1 \leq i < j \leq k$, $\mathrm{var}(P_i) \cap \mathrm{var}(P_j) = \emptyset$ diz-se uma *decomposição* de P. Se uma tal decomposição obrigar a que $k = 1$, P é *indecomponível*. Uma decomposição diz-se *completa* se os P_i forem indecomponíveis.

Chamamos *diagonal menos cauda*, dmc, às formas

$$F(\underline{x}) = \textstyle\sum_{i=1}^n b_i x_i^{2d} - \sum_{\underline{i}\in I} a_{\underline{i}}\underline{x}^{\underline{i}}, \quad \text{com} \quad b_i, a_{\underline{i}} \geq 0,$$

onde I é o conjunto de $n-$uplos inteiros não negativos com soma $2d$ e pelo menos duas entradas não nulas.

O lema seguinte mostra-nos que podemos reduzir o estudo ao estudo das formas indecomponíveis.

Lema 2.1. a. Se $F = D - T$ for uma forma dmc sdp, então $\mathrm{var}(T) \subseteq \mathrm{var}(D)$.
b. Se $F = F_1 + F_2 + \cdots + F_k$ for uma decomposição de F, então

i. F é dmc sse todo o F_i for dmc;

ii. F é sdp sse todo o F_i for sdp.

Dizemos que uma forma dmc é *elementar* se a sua cauda consiste num único termo,

$$E(\underline{x}) = b_1x_1^{2d} + \cdots + b_nx_n^{2d} - \mu x_1^{a_1}\cdots x_n^{a_n}.$$

Repare-se que estas formas são generalizações das formas de Hurwitz (agiformas de Reznick) $F(\underline{a},\underline{x}) = a_1x_1^{2d} + \cdots + a_nx_n^{2d} - 2dx_1^{a_1}\cdots x_n^{a_n}$ (a_i inteiros não negativos e de soma $2d$), que são conhecidas por serem soma de quadrados. De facto os coeficientes da parte diagonal não são necessariamente os expoentes dos termos da cauda e os coeficientes da cauda não são necessariamente iguais à soma dos coeficientes diagonais.

Teorema 2.2. Sejam $b_1,\ldots,b_n \in \mathbb{R}_{\geq 0}$, $d \in \mathbb{Z}_{\geq 1}$, $\mu \in \mathbb{R}$ e $E(\underline{x}) = b_1x_1^{2d} + \cdots + b_nx_n^{2d} - \mu x_1^{a_1}\cdots x_n^{a_n}$ uma forma de grau $2d$. Definindo $\mu_0 = 2d \prod_{\substack{i=1\\ a_i\neq 0}}^{n} \left(\frac{b_i}{a_i}\right)^{a_i/2d}$, são equivalentes as seguintes condições:

i. E é sdp.

ii. $|\mu| \leq \mu_0$ ou (todos os a_i são pares e $\mu < -\mu_0$).

iii. E é sdq.

Este teorema é uma versão bastante refinada da desigualdade aritmética-geométrica, $\alpha_1 x_1 + \cdots + \alpha_n x_n - x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq 0$, para todos os $\alpha_i, x_i \geq 0$ com $\sum_{i=1}^n \alpha_i = 1$. Repare-se que os coeficientes da parte diagonal não são iguais à potências da cauda e o seu coeficiente não é necessariamente igual à soma dos coeficientes da parte diagonal.

A ideia para provar o resultado principal, relativo à representabilidade de formas dmc sdp $F(\underline{x})$, consiste em determinar o respectivo mínimo e escrever a forma como soma de uma forma diagonal com formas $E(\underline{x})$ que têm o mesmo mínimo. Para o conseguirmos usamos os dois resultados seguintes, dos quais o segundo nos mostra como construir formas dmc elementares sdp com uma cauda e um zero desejados.

Recorde-se que o $(n-1)$-simplex é $\Delta_{n-1} = \{\underline{x} \in \mathbb{R}^n_{\geq 0} : \sum_i x_i = 1\}$ e o seu interior (relativo) é $\text{int}(\Delta_{n-1}) = \{\underline{x} \in \Delta_{n-1} : \forall i\, x_i > 0\}$.

Lema 2.3. Seja F uma forma sdp dmc indecomponível de dimensão $n \geq 2$. Então existe um mínimo local de $F|\Delta_{n-1}$ em $\text{int}(\Delta_{n-1})$.

Proposição 2.4. Seja $\underline{u} \in \text{int}(\Delta_{n-1})$, $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0}$, $\sum_{i=1}^n a_i = 2d \geq 2$, e $\mu > 0$. Definam-se b_i, $i = 1, \ldots, n$ e a forma E por

$b_i = \frac{\mu}{2d} a_i \frac{u_1^{a_1} \cdots u_n^{a_n}}{u_i^{2d}}$ e $E(\underline{x}) = \sum_{i=1}^n b_i x_i^{2d} - \mu x_1^{a_1} \cdots x_n^{a_n}$. Então os b_i estão bem definidos. Se $E \neq 0$ então E é uma forma dmc sdp indecomponível e tem um zero em $\underline{u}$. Se $\dim(E) = n$, $\underline{u}$ é o único zero em Δ_{n-1}.

O teorema seguinte constitui um dos dois resultados mais importantes deste trabalho

Teorema 2.5 Para toda a forma dmc indecomponível F, de dimensão n, são equivalentes as seguintes condições:

i. F é sdp.

ii. F tem um mínimo local $\underline{u}$ no $\text{int}(\Delta_{n-1})$ tal que $F(\underline{u}) \geq 0$.

iii. F tem um único mínimo local $\underline{u}$ no $\text{int}(\Delta_{n-1})$ tal que $F(\underline{u}) \geq 0$.

iv. F é soma de formas dmc sdp elementares indecomponíveis
mais uma forma diagonal sdp.

v. F é uma soma de quadrados.

Em particular toda a forma dmc sdp é uma soma de quadrados.

Repare-se que este resultado permite-nos estudar a semidefinipositividade de uma forma dmc usando processos de minimização clássicos. As provas dos resultados apresentados são construtivas, pelo que para decidir se uma dada forma dmc $F(\underline{x})$ pode ser escrita como sdq, e em caso afirmativo, encontrar uma representação explícita pode ser feito através do algoritmo:

1. Escreva a decomposição completa de F, $F = F_1 + \cdots + F_k$ em formas dmc indecomponíveis F_i;

2. Determine para cada uma das formas indecomponíveis F_i, o único mínimo local $\underline{u}_i$ no interior do simplex;

3. Se existir um i tal que $F_i(\underline{u}_i) < 0$, então pare: F_i, e consequentemente F, não pode ser sdq;

4. Caso contrário, para cada termo da cauda de F_i use a proposição 2.4 para encontrar uma forma dmc sdp elementar indecomponível que tenha este termo na cauda e que se anule em $\underline{u}_i$;

5. Escreva cada um dos F_i como soma de formas dmc não-diagonais elementares mais uma forma diagonal.

6. Escreva cada uma das formas dmc não-diagonais elementares obtidas no passo 5 como soma de quadrados de binómios.

7. Somando as representações como sdq de todos os F_i no passo 6 e as respectivas formas diagonais do passo 5 obtemos uma representação de F como soma de quadrados de binómios.

Agradecimentos. Os meus sinceros agradecimentos ao Professor Alexander Kovačec pelas numerosas e valiosas conversas que tivemos, os seus conselhos sempre sensatos, a sua total disponibilidade e o ter partilhado comigo a sua enorme cultura matemática. Agradeço ainda ao M. Marshall e ao M. Ghasemi, o interesse manifestado por [2], do qual resultaram dois artigos [4, 5].

Referências

[1] B. Reznick, A quantitative version of Hurwitz' theorem on the arithmetic-geometric inequality, *J. reine angew. Math.* 377, (1987), pp. 108–112.

[2] C. Fidalgo e A. Kovačec, Positive semidefinite diagonal minus tail forms are sums of squares, *Math. Zeit.*, Springer, Vol 269, Issue 3, (2011), pp. 629–645.

[3] G. Blekherman, There are significantly more nonnegative polynomials than sums of squares, *Israel J. Math.* 153, (2006), pp. 355–380.

[4] M. Ghasemi e M. Marshall, Lower bounds for a polynomial in terms of its coefficients. *Arch. Math.* 95, No. 4, (2010), pp. 343–353.

[5] M. Ghasemi e M. Marshall, Lower bounds for polynomials using geometric programming, *SIAM J. Optim.* 22, No. 2, (2012), pp. 460–473.

[6] J. B. Lasserre, Sufficient conditions for a polynomial to be a sum of squares, *Arch. Math.* 89, (2007), pp. 390–398.

[7] T. S. Motzkin,The arithmetic-geometric inequality, (*Inequalities Oved Shisha, Ed.*), Proc. of Sympos. at Wright-Patterson AFB, August 19-27, (1965), pp. 205–224.