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.

M / n	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.