

Encontro Nacional da Sociedade Portuguesa de Matemática

25 a 28 de Junho de 2008

ISEC

Lógica e Computação

Org. Fernando Ferreira

26 de Junho, 5^a feira, 11h-12h30

- Mário Edmundo e Giuseppina Terzo: *Lógica e sub-anéis exponenciais livres*
- João Rasga, Luís Cruz-Filipe, Cristina Sernadas e Amílcar Sernadas: *Discrete-measure almost-everywhere quantification*
- Jaime Gaspar: *Interpretações funcionais e suas factorizações*

27 de Junho, 6^a feira, 11h-12h30m

- Andreia Teixeira: *Os maiores rectângulos monocromáticos: aplicações à complexidade de comunicação*
- Luís Antunes e Lance Fortnow: *Sophistication revisited*
- André Souto e Luís Antunes: *Sequências infinitas sofisticadas*

27 de Junho, 6^a feira, 14h-15h30m

- Reinhard Kahle: *Reverse Proofs-as-Programs*
- Manuel Campagnolo: *Sistemas dinâmicos contínuos e computação*
- Isabel Oitavem: *Árvores e esquemas de recursão*

SOPHISTICATION REVISITED

Luís Antunes^(a), Lance Fortnow^(b)

^(a)Universidade do Porto and LIACC-UP

^(b)Northwestern University

Abstract

Kolmogorov complexity measures the amount of information in a string as the size of the shortest program that computes the string. The Kolmogorov structure function divides the smallest program producing a string in two parts: the useful information present in the string, called sophistication if based on total functions, and the remaining accidental information. We formalize a connection between sophistication (due to Koppel) and a variation of computational depth (intuitively the useful or nonrandom information in a string), prove the existence of strings with maximum sophistication and show that they are the deepest of all strings.

SISTEMAS DINÂMICOS CONTÍNUOS E COMPUTAÇÃO

Manuel Campagnolo

Instituto Superior de Agronomia e SQIG - Instituto de Telecomunicações

Resumo

Muitos modelos computacionais discretos são equivalentes, dada uma codificação simples, a sistemas dinâmicos discretos. Nesta apresentação será feita uma revisão de resultados que estabelecem uma equivalência entre modelos de computação e sistemas dinâmicos contínuos e será discutida a relevância desses resultados no estudo das propriedades computacionais de equações diferenciais ordinárias.

LÓGICA E SUB-ANÉIS EXPONENCIAIS LIVRES

Mário Jorge Edmundo^(a) e Giuseppina Terzo^(b)

^(a)Universidade Aberta e CMAF - Universidade de Lisboa

^(b)CMAF - Universidade de Lisboa

Resumo

Nesta comunicação apresentamos um trabalho conjunto com G.Terzo onde mostramos como construir sub-anéis exponenciais livres do anel exponencial dos reais, respectivamente dos complexos, usando Lógica.

INTERPRETAÇÕES FUNCIONAIS E SUAS FACTORIZAÇÕES

Jaime Gaspar

Technische Universität Darmstadt e FCT

Resumo

Numa primeira parte fazemos uma muito breve introdução às interpretações funcionais e suas aplicação em Matemática. De seguida, relacionamos algumas interpretações funcionais por meio de factorizações.

TOWARDS ‘REVERSE PROOFS-AS-PROGRAMS’

Reinhard Kahle

CENTRIA e Departamento de Matemática, Universidade Nova de Lisboa

Resumo

O paradigma de *Proofs-as-Programs* permite considerar demonstrações (constructivas de sentenças Π_2^0) directamente como programas executáveis (por exemplo numa linguagem de programação funcional). Baseado numa teoria para algoritmos de MOSCHOVAKIS propomos investigar a “imagem inversa” desta teoria em relação a uma função de extracção de programas. A relação de igualdade dada na teoria de algoritmos deve fundamentar uma relação correspondente entre demonstrações. Trata-se de trabalho em progresso.

ÁRVORES E ESQUEMAS DE RECURSÃO

Isabel Oitavem

Universidade Nova de Lisboa e CMAF - Universidade de Lisboa

Resumo

Exploramos o uso de ponteiros em esquemas de recursão, com vista a dotar os esquemas de recursão de uma estrutura de árvore e assim obter caracterizações implícitas de classes de complexidade não deterministas.

DISCRETE-MEASURE ALMOST-EVERYWHERE QUANTIFICATION

João Rasga^(a), Luís Cruz-Filipe^(b), Cristina Sernadas^(a), Amílcar Sernadas^(a)

^(a)Instituto Superior Técnico and SQIG - Instituto de Telecomunicações

^(b)Universidade de Lisboa and LASIGE-FCUL

Abstract

Recent developments in the area of generalized quantifiers are briefly described, and an axiomatization for a conservative enrichment of (two-sorted) first-order logic with almost-everywhere quantification is proposed. The completeness of the axiomatization against the measure-theoretic semantics is carried out using a variant of the Lindenbaum-Henkin technique. The independence of the axioms is analyzed. A suitable fragment of the logic is translated to first-order logic and validity is shown to be preserved.

SEQUÊNCIAS INFINITAS SOFISTICADAS

André Souto¹

Universidade do Porto

Abstract

De forma independente, Solomonoff, Kolmogorov e Chaitin definiram a complexidade de um objecto x como sendo o comprimento do programa mínimo que numa máquina de Turing produz x . A função *estrutura* de Kolmogorov divide o programa mínimo de x em duas partes: a primeira parte tem em conta a regularidade *útil* intrínseca ao objecto e a outra parte descreve a restante informação *acidental* de x . Kolmogorov sugeriu que a informação útil é representada por um conjunto finito no qual x é um elemento típico, donde resulta que a a descrição em duas partes do conjunto finito juntamente com o índice de x nesse conjunto deve ser tão curta como a descrição mais simples de x . A medida resultante foi designada no trabalho de Koppel por *sofisticação* de um objecto. Formalmente, a sofisticação de um objecto é o comprimento do programa (total) mínimo (p) que com algum tipo de dado (d) (finito ou infinito) produz esse objecto e tal que $|p| + |d|$ é, a menos de uma constante fixa, tão pequeno quanto a descrição mínima do objecto. Mais tarde, Antunes e Fortnow [1] revisitaram a noção de sofisticação para *strings* finitas e formalizaram uma relação entre esta medida e uma variante da profundidade computacional (que intuitivamente mede a quantidade de informação útil ou não aleatória numa *strings*), provando a existência de objectos de sofisticação máxima que correspondem a objectos de elevada profundidade computacional.

No presente trabalho propomos uma nova abordagem à sofisticação para sequências infinitas. A principal motivação deste trabalho prende-se com o facto de a medida de sofisticação para sequências infinitas não estar devidamente definida no trabalho de Koppel, uma vez que a noção proposta de “descrição de uma sequência infinita” proposta em [2] não é aplicável a todas as sequências. Começamos por redefinir a noção de sofisticação para sequências infinitas, introduzindo a inferior e superior sofisticação como sendo o \liminf e \limsup , respectivamente, da razão entre a sofisticação dos segmentos iniciais da sequência pelo tamanho desses segmentos. Em seguida provamos, que existem sequências altamente estocásticas se usarmos a sofisticação superior e provavelmente estes objectos não existem se usarmos a sofisticação inferior.

Koppel provou a equivalência entre a sofisticação e a profundidade lógica. Contudo a definição de profundidade lógica usada é diferente da proposta por Bennett, uma vez que impõe que as funções usadas na definição sejam totais. No artigo [1], Antunes e Fortnow, deram um exemplo de objectos finitos onde a equivalência não é válida se considerarmos a complexidade de Kolmogorov na definição de sofisticação e substituímos a profundidade lógica pela profundidade computacional. Neste trabalho aprofundamos esta ideia e mostramos um exemplo de uma sequência, a diagonal do problema de paragem, para a qual a sofisticação é zero mas a profundidade computacional é alta.

Referências

- [1] L. Antunes and L. Fortnow, *Sophistication Revisited*, Proceedings of the 30th ICA-Languages and Programming, Lecture Notes in Computer Science, 2719:267-277, Springer,

¹Trabalho conjunto com Luís Antunes

2003.

- [2] L. Antunes, L. Fortnow, D. van Melkebeek and N. V. Vinodchandran, *Computational depth: concept and applications*, TCS, 354(3): 391-404, 2006.
- [3] M. Koppel, *Structure*, in “The universal Turing machine: a half-century survey”, pages = 403–419, Springer-Verlag New York, Inc., 1988

OS MAIORES RECTÂNGULOS MONOCROMÁTICOS: APLICAÇÕES À COMPLEXIDADE DE COMUNICAÇÃO

Andreia Teixeira

Universidade do Porto

Abstract

O conceito de complexidade de comunicação foi introduzido por Yao em 1979, ver [2, 3]; desde aí tem sido aplicado a inúmeros problemas como, por exemplo, à optimização do projecto de circuitos VLSI e à minimização da comunicação em diversos tipos de redes.

Suponhamos que a Alice e o Bob pretendem determinar o valor de uma dada função $f(x, y)$, onde x e y são palavras de n bits. A Alice conhece apenas x e o Bob conhece apenas y . Um método óbvio de ficarem ambos a conhecer $f(x, y)$ é o seguinte: (i) a Alice envia x ao Bob, (ii) o Bob calcula $f(x, y)$ e envia este valor à Alice. Este método requer a troca de $n + 1$ bits. Contudo para muitas funções é possível atingir o objectivo pretendido com muito menos bits trocados entre a Alice e o Bob.

A complexidade de comunicação da função f associada a um determinado protocolo é o número de bits que a Alice e o Bob, seguindo esse protocolo, têm que trocar no pior caso; um protocolo diz-se óptimo quando minimiza esse número de bits. A complexidade de comunicação da função f é o número de bits trocados (no pior caso) quando se utiliza um protocolo óptimo. O livro [1] é uma boa referência genérica sobre complexidade de comunicação.

O conceito de rectângulo combinatório é fundamental na Complexidade de Comunicação. Dado um conjunto R , um rectângulo combinatório é um conjunto $A \times B$ onde A e B são subconjuntos de R . Um quadrado $R \times R$ juntamente com uma função $c : R \times R \rightarrow \{0, 1\}$ é denominado de rectângulo colorido. Diz-se que um quadrado colorido é aleatório se cada $c(x, y)$ é uma variável aleatória independente (neste caso, diz-se que c é uma função aleatória). Um rectângulo combinatório colorido $A \times B$ é dito monocromático se $c(x, y)$ tem sempre o mesmo valor (0 ou 1) para todo $x \in A$ e $y \in B$.

É de particular interesse o conhecimento da área a do maior rectângulo monocromático em $R \times R$, uma vez que a partir do valor de a é possível estabelecer facilmente um minorante para a complexidade de comunicação de f . Com efeito, tem que haver pelo menos n^2/a rectângulos monocromáticos, pelo que a altura de qualquer árvore associada a um protocolo é, pelo menos, $\lceil \log(n^2/a) \rceil$; essa altura é essencialmente a complexidade de comunicação de f .

Estudamos a área máxima assintótica de rectângulos combinatórios monocromáticos (mcr) num quadrado aleatório, estabelecendo generalizações e aperfeiçoamentos relativamente aos resultados já conhecidos. Concluimos que num quadrado colorido aleatório, o maior rectângulo combinatório monocromático tem área $(1+o(n))n/2$ e forma $2 \times (n/4)$ ou $(n/4) \times 2$. Aplicamos estes resultados à complexidade de comunicação obtendo um minorante da chamada função aleatória: Seja $f_p(x, y)$ a função aleatória que vale 1 com probabilidade $p > 0$ e vale 0 com probabilidade $1 - p > 0$. A complexidade de comunicação determinística de uma função aleatória $f_p(x, y)$ satisfaz assintoticamente

$$D(f) \geq \lceil \log n + \log(p \ln(1/p) + (1 - p) \ln(1/(1 - p))) + \log e \rceil$$

Referências

- [1] Eyal Kushilevitz, Noam Nisan, *Communication Complexity*, Cambridge University Press, New York, Springer-Verlag, 1996.
- [2] Andrew Chi-Chih Yao, *Some complexity questions related to distributive computing*, Proceedings of the 11th Annual ACM Symposium on Theory of Computing, Atlanta, pp 209-213, 1979.
- [3] Andrew Chi-Chih Yao, *The entropic limitations on VLSI computations*, Proceedings of the 13th Annual ACM Symposium on Theory of Computing, Milwaukee, pp 308-311, 1981.