Conhecimento Zero Estatístico e Reduções Eficientes para o Problema MKTP

Nicollas M. Sdroievski[1], **Murilo V. G. da Silva (orientador)**[1], **André L. Vignatti (co-orientador)**[1]

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)
Curitiba – PR – Brasil

Abstract. *This paper is a summary of the dissertation with the same title. In the dissertation we study the complexity of computational problems that are candidates for **NP**-intermediate status. In this process, we connect the complexity class **SZK**, related to zero-knowledge proofs, to the computational problem MKTP, related to algorithmic information theory. As original contributions, we highlight randomized reductions from the* HIDDEN SUBGROUP PROBLEM *(HSP) and other problems in computational group theory to MKTP, and statistical zero-knowledge proofs for decisions versions of HSP.*

Resumo. *Este artigo é um resumo da dissertação de mestrado de mesmo título, na qual estudamos a complexidade de problemas computacionais candidatos a **NP**-intermediários. Nesse processo, conectamos a classe **SZK**, relacionada a provas de conhecimento zero, com o problema computacional MKTP, relacionado à teoria algorítmica da informação. Como contribuições originais, destacamos reduções aleatorizadas do* PROBLEMA DO SUBGRUPO OCULTO *(HSP) e outros problemas em teoria computacional de grupos para MKTP, e provas de conhecimento zero estatístico para versões de decisão do problema HSP.*

1. Introdução

A questão central da área de complexidade computacional é a questão **P** versus **NP**, ou seja, se os problemas verificáveis em tempo polinomial são também decidíveis em tempo polinomial. Embora historicamente muito da pesquisa na área consista na classificação de problemas como pertencendo a **P** ou então como **NP**-completos (os problemas mais difíceis de **NP**), existe uma classe de problemas que aparenta estar em uma região intermediária: não conhecemos algoritmo polinomial para esses problemas, porém também não sabemos se são **NP**-completos. De fato, o Teorema de Ladner [Ladner 1975] garante que existem problemas **NP**-intermediários, problemas em $\mathbf{NP} \setminus \mathbf{P}$ que não são **NP**-completos, caso $\mathbf{P} \neq \mathbf{NP}$. O tema central deste trabalho consiste em investigar problemas computacionais e classes de complexidade candidatos a **NP**-intermediários.

Provar que um problema é **NP**-intermediário é uma tarefa muito difícil, pois implicaria que $\mathbf{P} \neq \mathbf{NP}$. Sendo assim, a pesquisa nesta área consiste em estabelecer relações entre problemas candidatos a **NP**-intermediários. Alguns candidatos a tal classificação são os problemas de testar se dois grafos são isomorfos [Boppana et al. 1987], se um determinado inteiro é um resíduo quadrático [Goldwasser et al. 1989], o problema da fatoração de inteiros [Arora and Barak 2009], e vários problemas em teoria computacional de grupos [Arvind and Das 2008]. Muitos desses problemas são casos particulares do PROBLEMA DO SUBGRUPO OCULTO (HSP, de *Hidden Subgroup Problem*). A contribuição

central deste trabalho é o esclarecimento da relação do problema HSP com classes de complexidade e problemas candidatos a **NP**-intermediários. Mais especificamente, mostramos que versões de decisão do problema HSP estão contidos na classe **SZK**, e também mostramos reduções aleatorizadas de HSP e outros problemas em teoria computacional de grupos para o problema MKTP.

A classe **SZK** é uma classe definida em termos de *provas interativas*, que definem como ocorre a interação entre uma estratégia de prova P e um verificador V. Nesta interação a estratégia P, sem limitações computacionais, tem o propósito de convencer V, um algoritmo com limite de tempo polinomial, de que determinada asserção (instância de um problema computacional) é verdadeira [Arora and Barak 2009]. Quando V não obtém nenhuma (ou muito pouca) informação além do fato de que a asserção é verdadeira, dizemos que a prova interativa é de *conhecimento zero*. A classe **SZK** contém os problemas que admitem provas de conhecimento zero nas quais o verificador V pode apenas obter, além do fato de que a asserção é verdadeira, informação estatisticamente negligenciável da interação. Essas provas são chamadas de *provas de conhecimento zero estatístico*. A classe **SZK**, além de conter vários problemas candidatos a **NP**-intermediários, ainda é conjecturada estar estritamente contida entre as classes **P** e **NP** [Arora and Barak 2009].

Além dos problemas da classe **SZK**, estudamos um problema computacional relacionado à complexidade de Kolmogorov [Li and Vitányi 1997]: o problema MKTP (de *Minimum KT Problem*). A complexidade de Kolmogorov é uma medida de complexidade que visa capturar a quantidade de informação contida em uma string x levando em consideração o tamanho do menor programa que a constrói. Algumas variações dessa medida também levam em consideração o tempo de execução desse programa, de forma que strings que precisam de mais tempo para serem construídas são mais complexas. Esse é o caso da medida de complexidade KT [Allender et al. 2006]. O problema MKTP consiste em decidir, dados uma string x e um inteiro k, se a complexidade KT de x é no máximo k. Além de ser um problema candidato a **NP**-intermediário, o problema é notável pois vários outros problemas candidatos a **NP**-intermediários são redutíveis a ele. Mais precisamente, se o problema for decidível em tempo polinomial aleatorizado, isto é, MKTP $\in$ **BPP**, então **SZK** $\subseteq$ **BPP**. Por outro lado, há evidência de que o problema não é **NP**-completo [Murray and Williams 2014, Hirahara and Watanabe 2015]. A Figura 1 apresenta as relações conjecturadas entre as classes **NP**, **SZK** e o problema MKTP.

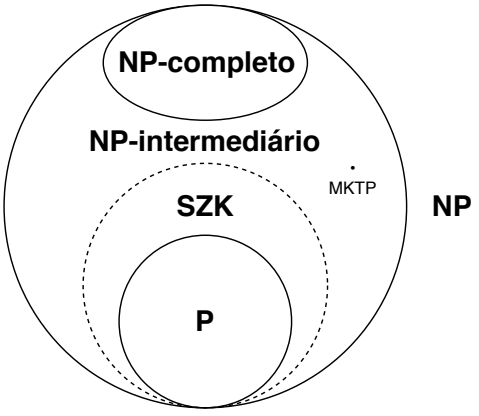

Figura 1. Relações conjecturadas entre as classes NP, SZK e o problema MKTP.

2. Preliminares

Assumimos familiaridade com conceitos e classes da área de complexidade computacional, em especial as classes ligadas à computação aleatorizada: **BPP**, **RP** e **ZPP**, além de reduções e classes de complexidade definidas em termos de oráculos (e.g. $\mathbf{BPP}^{\mathcal{O}}$ é a classe dos problemas decidíveis em tempo polinomial por algoritmos probabilísticos com oráculo para o problema $\mathcal{O}$). O texto da dissertação [Sdroievski 2018] apresenta no Capítulo 2 os conceitos de complexidade computacional, teoria algorítmica da informação, teoria de grupos, teoria de grafos e teoria de números necessários para a compreensão da discussão e dos resultados apresentados.

3. A Classe SZK, o Problema MKTP e Candidatos a NP-intermediários

Durante a revisão de literatura, definimos e estudamos a complexidade de diversos problemas computacionais candidatos a **NP**-intermediários. Além disso, revisamos pertinências conhecidas desses problemas na classe **SZK** e diversas de suas subclasses e também reduções aleatorizadas desses problemas para o problema MKTP.

3.1. Provas de Conhecimento Zero

Em relação a provas de conhecimento zero, revisamos os resultados da Figura 2. Definições precisas de cada um dos problemas computacionais, classes de complexidade e demonstrações dos resultados expostos na figura podem ser encontradas nos Capítulos 2 e 3 do texto da dissertação [Sdroievski 2018].

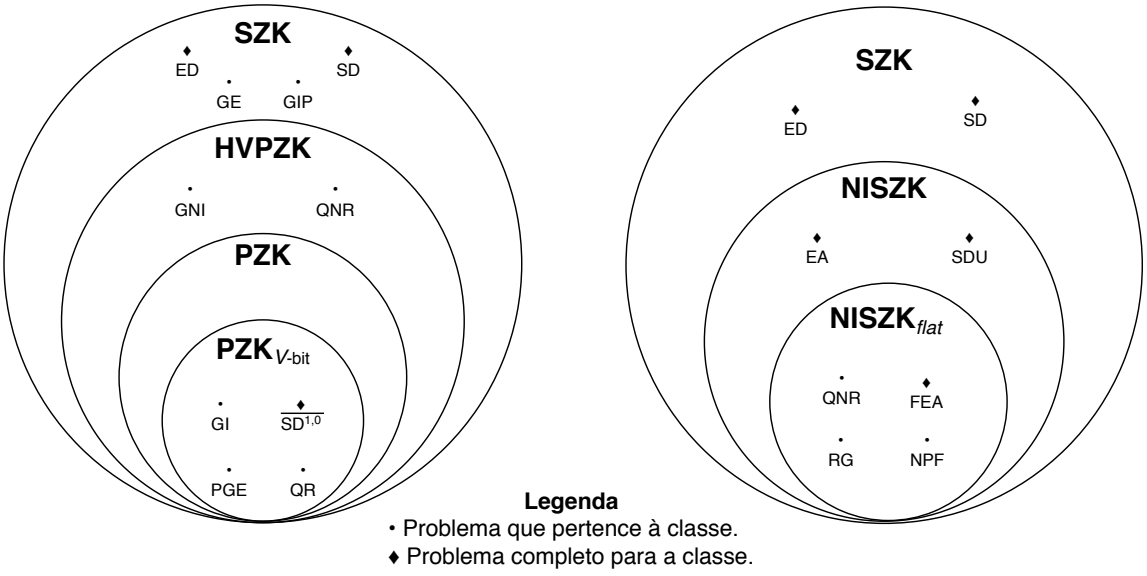

Figura 2. Relações previamente conhecidas entre problemas candidatos a NP-intermediários e subclasses de SZK.

3.2. O Problema MKTP e Técnicas de Redução

Estudamos ainda o problema MKTP, e em especial duas técnicas que permitem mostrar reduções para o problema. A primeira destas faz uso das conexões que a medida de complexidade KT possui com funções unidirecionais e geradores pseudo-aleatórios [Allender et al. 2006]. De fato, um oráculo para o problema é capaz de inverter, na média, qualquer função eficientemente computável, ou que equivalentemente seja computável por um circuito de tamanho polinomial (ver [Sdroievski 2018, Seção 4.1]).

Estudamos ainda uma técnica bastante recente de redução para MKTP [Allender et al. 2018]. Essa técnica consiste no uso do oráculo para MKTP como um *estimador da entropia* (ver [Sdroievski 2018, Seção 4.3]) de uma distribuição de probabilidade eficientemente amostrável. As técnicas estudadas permitem mostrar que a classe **SZK**, e algumas de suas subclasses, são redutíveis ao problema. Esses resultados são resumidos na Figura 3.

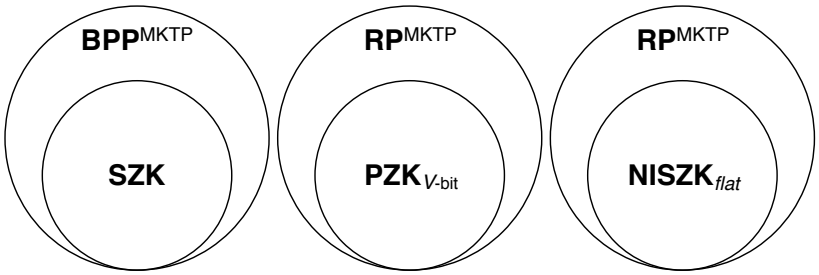

Figura 3. Relações conhecidas entre o problema MKTP e a classe SZK.

Além disso, essas técnicas permitem mostrar reduções mais fortes para uma classe de problemas em grupos que inclui os problemas ISOMORFISMO DE GRAFOS e RESÍDUO QUADRÁTICO [Allender et al. 2018].

4. Resultados Obtidos

Os principais resultados obtidos na dissertação são resumidos na Figura 4. Todos os problemas da figura são em teoria computacional de grupos e estão definidos no Capítulo 2 do texto da dissertação [Sdroievski 2018].

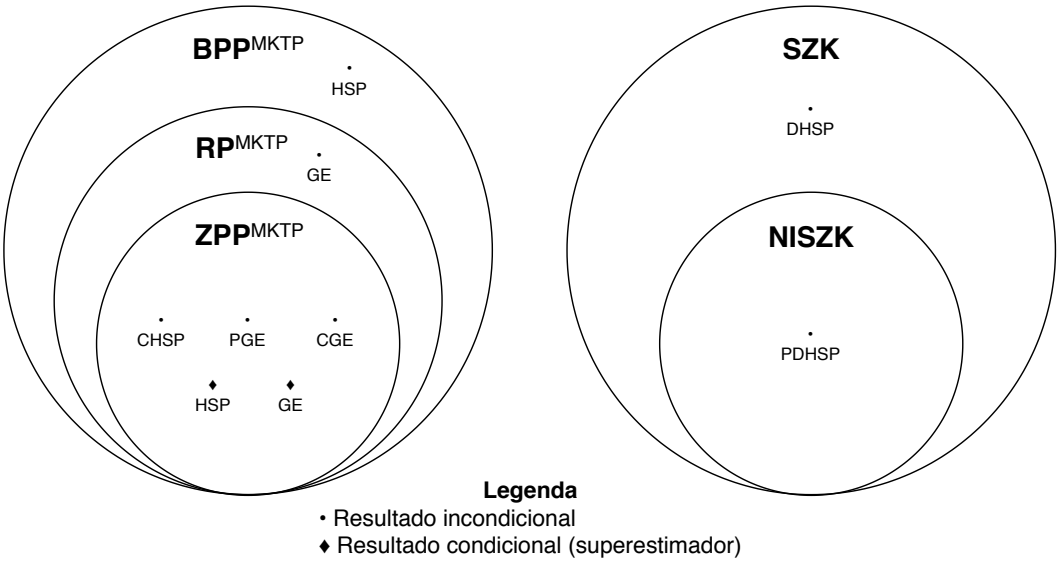

Figura 4. Resumo dos resultados obtidos na dissertação

As principais contribuições são relacionadas ao problema HSP. Esse problema é notável na área de complexidade computacional, dado que muitos problemas computacionais importantes são redutíveis a ele. Em particular, o problema de isomorfismo de grafos e uma série de problemas em teoria de números são casos específicos do problema.

Os últimos incluem o PROBLEMA DA FATORAÇÃO e o PROBLEMA DO LOGARITMO DISCRETO, de forma que muitos dos protocolos de criptografia utilizados atualmente dependem da dificuldade de HSP.

Pouco se conhece sobre a complexidade clássica do problema HSP, pois muita da pesquisa relacionada ao problema é na área de complexidade computacional quântica. Em particular, o famoso algoritmo de fatoração de Shor [Shor 1997] foi estendido para o problema HSP em grupos *abelianos*, e um dos desafios em computação quântica é encontrar algoritmos semelhantes para outras classes de grupos, como grupos simétricos e diedrais. Uma das principais contribuições deste trabalho é analisar o problema sob a luz da complexidade computacional clássica, elucidando sua relação com tais classes de complexidade.

Em relação à provas de conhecimento zero, obtivemos dois resultados relacionados à versões de decisão do problema HSP. Mais especificamente, mostramos que DHSP, o problema de determinar se o subgrupo oculto possui ordem 1 em *grupos de caixa-preta* (ver [Sdroievski 2018, Seção 2.4.6]) está na classe **SZK**. Para obter esse resultado, mostramos uma prova de conhecimento zero estatístico para o problema, baseada no resultado de [Fenner and Zhang 2005]. Além disso, mostramos que PDHSP, o mesmo problema para grupos simétricos, está na classe **NISZK**. Esse resultado foi provado a partir de uma redução para o problema APROXIMAÇÃO DE ENTROPIA, que é completo para **NISZK** [Vadhan 1999].

Também obtivemos resultados relacionando os problemas HSP e MKTP. Mostramos que $\mathbf{HSP} \in \mathbf{BPP}^{\mathrm{MKTP}}$ adaptando um resultado de [Allender et al. 2018]. Além disso, mostramos que é possível tornar essa redução mais forte quando há uma maneira eficiente de estimar a ordem do grupo dado como entrada para o problema, implicando que, nesses casos, $\mathbf{HSP} \in \mathbf{ZPP}^{\mathrm{MKTP}}$. Vários grupos importantes, como grupos simétricos e diedrais, satisfazem essa condição, e portanto o problema HSP para esses grupos está em $\mathbf{ZPP}^{\mathrm{MKTP}}$. Finalmente, adaptando um resultado de [Babai and Beals 1998], mostramos que é possível calcular de maneira exata a ordem de grupos cíclicos dados através de um elemento gerador com um oráculo para MKTP, cumprindo a condição também para esta classe de grupos.

4.1. Publicações

Os resultados mais importantes do trabalho estão presentes em um artigo aceito para publicação no periódico *Theoretical Computer Science*. O mesmo artigo foi anteriormente disponibilizado no *Electronic Colloquium on Computational Complexity* (ECCC), um fórum com o objetivo de tornar a publicação visível enquanto passa por um processo mais longo de revisão em um periódico qualificado. Ainda assim, os artigos publicados nesse fórum passam por um processo rápido de revisão por um membro do comitê de especialistas altamente reconhecidos na área. A referência para o artigo é apresentada abaixo.

- Sdroievski, N. M., da Silva, M. V. G., e Vignatti, A. L. (2018). The Hidden Subgroup Problem and MKTP.
  - Aceito para publicação no periódico *Theoretical Computer Science*.
  - Versão preliminar disponível no *Electronic Colloquium on Computational Complexity (ECCC)*, Report TR18-193. ISSN 1433-8092. URL: `https://eccc.weizmann.ac.il/report/2018/193/`.

5. Agradecimentos

O presente trabalho foi realizado com apoio do CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico - Brasil.

Referências

Allender, E., Buhrman, H., Koucký, M., van Melkebeek, D., and Ronneburger, D. (2006). Power from random strings. *SIAM Journal on Computing*, 35(6):1467–1493.

Allender, E., Grochow, J. A., van Melkebeek, D., Moore, C., and Morgan, A. (2018). Minimum Circuit Size, Graph Isomorphism, and Related Problems. In Karlin, A. R., editor, *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:20, Dagstuhl, Germany. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

Arora, S. and Barak, B. (2009). *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition.

Arvind, V. and Das, B. (2008). Szk proofs for black-box group problems. *Theory of Computing Systems*, 43(2):100–117.

Babai, L. and Beals, R. (1998). A Polynomial-time Theory of Black-box Groups I (manuscrito).

Boppana, R. B., Hastad, J., and Zachos, S. (1987). Does co-np have short interactive proofs? *Inf. Process. Lett.*, 25(2):127–132.

Fenner, S. A. and Zhang, Y. (2005). Quantum algorithms for a set of group theoretic problems. In Coppo, M., Lodi, E., and Pinna, G. M., editors, *Theoretical Computer Science*, pages 215–227, Berlin, Heidelberg. Springer Berlin Heidelberg.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208.

Hirahara, S. and Watanabe, O. (2015). Limits of minimum circuit size problem as oracle. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:198.

Ladner, R. E. (1975). On the structure of polynomial time reducibility. *J. ACM*, 22(1):155–171.

Li, M. and Vitányi, P. (1997). *An introduction to Kolmogorov complexity and its applications*. Springer-Verlag, 2 edition.

Murray, C. and Williams, R. (2014). On the (non) np-hardness of computing circuit complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:164.

Sdroievski, N. M. (2018). Conhecimento Zero Estatístico e Reduções Eficientes para o Problema MKTP. Dissertação de mestrado, Departamento de Informática, Universidade Federal do Paraná (UFPR).

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509.

Vadhan, S. P. (1999). *A Study of Statistical Zero-knowledge Proofs*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA. AAI0801528.