CRIPTOGRAFIA: UMA SITUAÇÃO DESENCADEADORA DE APRENDIZAGEM

Pedro Henrique Monferino Mancini
Universidade Tecnológica Federal do Paraná - UTFPR
pedrohmmancini@gmail.com

Luciana Schreiner de Oliveira
Universidade Tecnológica Federal do Paraná - UTFPR
lucianaoliveira@utfpr.edu.br

Maria Lúcia Panossian
Universidade Tecnológica Federal do Paraná - UTFPR
mlpanossian@utfpr.edu.br

Resumo: O trabalho apresentado neste texto trata-se de uma Situação Desencadeadora de Aprendizagem (SDA) explicada conforme a Atividade Orientadora de Ensino, proposta por Moura e outros (2010), desenvolvida no Clube de Matemática, um projeto iniciado no Programa Institucional de Bolsas de Iniciação à Docência, para alunos dos 7º, 8º e 9º de um colégio estadual de Curitiba sobre o conceito de Criptografia e um de seus usos históricos. Buscamos ensinar aos alunos sobre a codificação e decodificação de mensagens para apropriação desse conhecimento tão pertinente a era tecnológica que vivemos, onde precisamos proteger as informações e dados pessoais. A SDA abordada neste texto trata de uma forma de criptografia usada historicamente por Júlio César, a Cifra de César, e possíveis articulações da criptografia ao conhecimento matemático.
Palavras-chave: Criptografia. Situação desencadeadora de aprendizagem. Ensino de matemática.

INTRODUÇÃO

Nesse relato de experiência serão apresentados os resultados do desenvolvimento de uma situação usando a Cifra de César para o ensino da Criptografia. A situação foi realizada com 12 (doze) alunos do 7º, 8º e 9º anos do Ensino Fundamental, divididos em 5 (cinco) grupos, durante aulas do 1º semestre do Clube de Matemática, em um colégio estadual de Curitiba, no contraturno das aulas regulares dos alunos.

O Clube de Matemática é um projeto iniciado dentro do Programa Institucional de Bolsas de Iniciação à Docência (PIBID), Edital Capes 07/2018, como componente curricular do curso de Licenciatura em Matemática, da Universidade Tecnológica Federal do Paraná (UTFPR), Câmpus Curitiba. O objetivo do projeto Clube de Matemática é favorecer que os alunos compreendam a importância do conhecimento matemático.

As situações trabalhadas no projeto têm como objetivo apresentar uma matemática contextualizada para os alunos, para que eles compreendam, analisem e discutam sobre o

conhecimento matemático e deem sentido próprio ao conhecimento apropriando-se dos conceitos abordados. Segundo B. D'Ambrósio (1989, p. 17), "Através de suas experiências com problemas de naturezas diferentes o aluno interpreta o fenômeno matemático e procura explicá-lo dentro de sua concepção da matemática envolvida". Uma das situações realizadas no Clube de Matemática foi sobre a Criptografia, que abordaremos neste texto.

A Criptografia, também conhecida como Cifra, é usada para comunicação de forma segura e sigilosa. Mesmo que seu uso esteja presente em nossas ações diárias, como em mensagens de texto e transações bancárias (TAVARES et al., 2017, p.2), o ensino dela ainda é um conceito pouco explorado pelos professores de Matemática no Ensino Básico, apesar de poder ser trabalhada com articulações históricas e vinculada ao cotidiano dos estudantes.

A palavra Criptografia origina-se do grego, pela união das palavras *kruptós*, que significa "secreto" ou "oculto", e *grafia*, que quer dizer "escrita". Seu uso é tão antigo quanto a invenção da própria escrita. Pode-se considerar que ela foi gerada da necessidade humana de se comunicar de maneira sigilosa e seu princípio é simples, escolher com quem você quer compartilhar suas informações ou dados. De acordo com Weber (1995), criptografia é

> [...] caracterizada como a ciência (ou arte) de escrever em códigos ou em cifras, ou seja, é um conjunto de métodos que permite tornar incompreensível uma mensagem (ou informação), de forma a permitir que apenas as pessoas autorizadas consigam decifrá-la e compreendê-la. (WEBER, 1995, p.1)

Um dos registros mais antigos da Criptografia é do povo egípcio, em 3000 a. C., nas escritas dos hieróglifos. Outro uso histórico interessante foi a Cifra de César, chamada assim por ter sido utilizada por Júlio César e pelo Império Romano no século I a. C.. César a utilizou para se comunicar com seus generais e pessoas relevantes do Império. Na Cifra de César, cada letra do alfabeto é deslocada de sua posição em uma quantidade fixa. Na situação abordada neste texto, utilizamos o deslocamento de 3 (três) posições, em que a letra A seria representada pela letra D, como mostrado na figura abaixo.

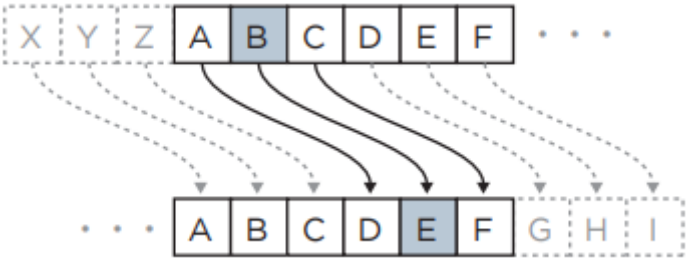

Figura 1 – Exemplo de Cifra de César

Fonte: Thawte (2013, p. 4)

CRIPTOGRAFIA NO ENSINO

Na educação Matemática, a Cifra pode ser usada com o objetivo de ensinar vários conteúdos, além dela mesma. Ainda que não esteja citada diretamente nas propostas curriculares, é um tema que abrange vários conceitos matemáticos, ajudando a contextualizar esse conceito, como salientado pelos PCN+:

> Explorar conteúdos relativos aos temas números, álgebra, medidas, geometria e noções de estatística e probabilidade envolve diferentes formas do pensar em Matemática, diferentes contextos para as aplicações, bem como a existência de razões históricas que deram origem e importância a esses conhecimentos. Mas para evitar a quantidade excessiva de informações, é preciso fazer um recorte, usando alguns critérios orientadores deste processo de seleção de temas (PCN+, 2002, p.119).

Como discutido anteriormente, as Cifras foram invenções essenciais para nossa sociedade atual, pois ela protege nossas informações e dados, desde uma simples mensagem de texto até uma transação bancária (TAVARES et al., 2017, p.2). Um exemplo de seu uso é o envio de uma mensagem por aplicativo de celular, como o Whatsapp, que declara o uso da Criptografia como garantia de proteção à privacidade dos usuários, como mostrado na figura a seguir.

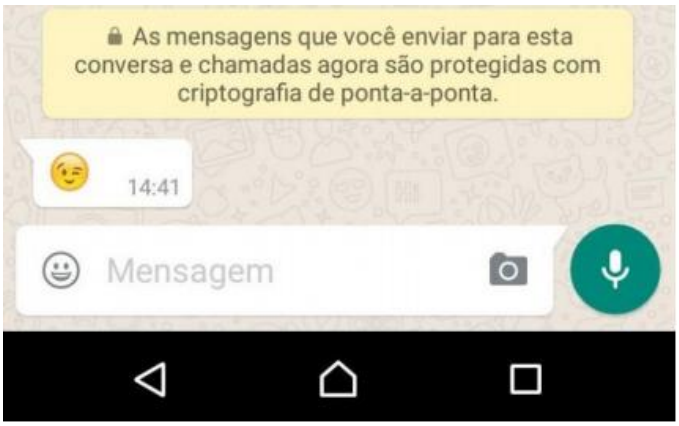

Figura 2 – Criptografia no Whatsapp
Fonte: Dantas (2016, p. 29)

As Cifras estão diretamente relacionadas com a teoria matemática, visto que a maior parte delas, usadas na atualidade, são aplicações matemáticas. Segundo Tavares et al. (2017, p.2) "[...] as técnicas criptográficas mais seguras são fundamentadas em algumas áreas da Matemática, tais como Álgebra Linear, Matemática Discreta e Teoria dos Números.".

O ensino da Criptografia na Educação Básica pode introduzir essa ferramenta, tão utilizada na sociedade, no processo educacional, assim como conceitos matemáticos, por exemplo, matrizes inversas (TAVARES et al., 2017) e funções inversas (GROENWALD, OLGIN, 2011).

A inserção da Criptografia em materiais didáticos é raramente feita, justamente por ela não ser um conteúdo ou conceito presente nos currículos. Segundo a análise feita por Litoldo e Lazari (2014, p. 145-153), a abordagem da Criptografia em livros didáticos depende muito dos autores, mas numa perspectiva geral é pouco presente. Os autores ainda ponderam que

> [...] a forte presença do tema Criptografia em atividades da vida diária das pessoas, bem como o vínculo do assunto com fatos administrativos e políticos, é possível considerar que a inserção adequada de atividades ligadas a este tema pode ter um impacto positivo no processo de ensino e aprendizagem dos alunos. (LITOLDO e LAZARI, 2014, p.153).

Devido à pouca exploração da Criptografia no ensino, tanto para introdução do conceito quanto para utilização em algum conceito matemático, buscamos neste texto elaborar uma Situação Desencadeadora de Aprendizagem (SDA) enquanto elemento da Atividade Orientadora de Ensino (AOE) proposta por Moura e outros (2010). A SDA foi apresentada no Clube de Matemática, introduzindo uso histórico das Cifras, a Cifra de César, com os estudantes e discutindo a codificação e a decodificação.

SITUAÇÃO DESENCADEADORA DE APRENDIZAGEM

A Atividade Orientadora de Ensino (MOURA, 1996; MOURA et al., 2010) analisa uma interdependência na ação pedagógica entre o conteúdo de ensino, as ações educativas e os sujeitos que participam da atividade de ensino (MOURA et al., 2010), fundamentada nas teorias histórico-cultural e da atividade, cujos principais autores são Vygotski, Leontiev, Rubtsov e Davidov.

Segundo Moura e outros (2010), a escola é vista como um espaço que possibilita a aprendizagem e a apropriação da cultura humana de forma intencional. Nesta concepção, a atividade de ensino do professor desencadeia e potencializa a atividade de aprendizagem do estudante incluindo-os no grupo social que estão presentes. Para Moura et al. (2010),

> O professor que se coloca, assim, em atividade de ensino continua se apropriando de conhecimentos teóricos que lhe permitem organizar ações que possibilitem ao estudante a apropriação de conhecimentos teóricos explicativos da realidade e do desenvolvimento do seu pensamento teórico,

> ou seja, ações que promovam a atividade de aprendizagem de seus alunos.(p.213 e 214)

Na AOE, tanto professores como estudantes estão em atividade e o modo que esses sujeitos realizarão suas ações no processo de ensino e aprendizagem é alterado por suas características como sujeitos portadores de conhecimentos, valores e afetividade. Assim, a apropriação do conhecimento é feita por cada um deles de forma diferente, conforme afirma Moura (1996):

> A atividade de ensino que respeita os diferentes níveis dos indivíduos e que define um objetivo de formação como problema coletivo é o que chamamos de atividade orientadora de ensino. Ela orienta o conjunto de ações em sala de aula a partir de objetivos, conteúdos e estratégias de ensino negociando e definido por um projeto pedagógico (MOURA, 1996, p. 32).

Desta forma, "as ações do professor devem ser organizadas de forma a possibilitar aos estudantes a apropriação dos conhecimentos e das experiências histórico-culturais da humanidade" (MOURA et al., 2010, p. 218 e 219).A busca principal da AOE é que o professor em atividade selecione e estude um conceito, organizando o seu processo de ensino, com o principal objetivo de que o aluno em sua atividade se aproprie e dê sentido próprio ao conhecimento. Assim, para Moura et al. (2010), "Na Atividade Orientadora de Ensino as necessidades, motivos, objetivos, ações e operações do professor e dos estudantes se mobilizam inicialmente por meio da situação desencadeadora de aprendizagem" (MOURA ET AL, 2010, p. 222).

As SDA são organizadas pelo professor, a fim de concretizar seus objetivos de ensino, buscando a apropriação do estudante em sua atividade de aprendizagem. Ela deve de apresentar aos estudantes a gênese do conceito, ou seja, explicar a necessidade humana que levou à construção do conceito, buscado a compreensão do aluno sobre as motivações e soluções dos sujeitos em atividade. As ações realizadas pelo professor primeiramente partirão da construção da solução da SDA. Moura e outros (2010, p.222) consideram que as ações do professor,

> [...] ao serem desencadeadas, considerarão as condições objetivas para o desenvolvimento da atividade: as condições materiais que permitem a escolha dos recursos metodológicos, os sujeitos cognoscentes, a complexidade do conteúdo em estudo e o contexto cultural que emoldura os sujeitos e permite as interações sócio-afetivas no desenvolvimento das ações que visam o objetivo da atividade - a apropriação de certo conteúdo e do modo geral de ação de aprendizagem. (MOURA ET AL, 2010, p.222)

As Situações Desencadeadoras de Aprendizagem podem ser materializadas como um jogo, uma situação emergente do cotidiano e uma história virtual do conceito a ser aprendido (MOURA; LANNER DE MOURA, 1998). A SDA apresentada neste texto, buscou as características da história virtual, que é envolver o aluno no processo de solução histórica do problema apresentado, de forma semelhante a feita pela humanidade em seu momento histórico. Para Moura e Lanner de Moura (1998), a história virtual "[...] coloca a criança diante de uma situação problema semelhante àquela vivida pelo o homem (no sentido genérico)" (MOURA; LANNER DE MOURA, 1998, p. 12-14).

A situação analisada neste texto procurou atender aos princípios de uma SDA, considerando todos seus elementos. Ela teve como objetivo principal introduzir o uso da Criptografia para os alunos, estabelecendo o primeiro contato com o deciframento e ciframento de mensagens. Num primeiro momento da SDA, os estudantes teriam que decifrar uma troca de cartas fictícias realizada por Júlio César e seus generais, conforme figura a seguir.

Carta 1: De Júlio César para seu general

"SUHFLVDPRV FRQTXLVWDU QRYRV WHUULWRULRV H HASDQGLU QRVVR LPSHULR, PDQGDUHL PDLV WURSDV SDUD D QRYD LQYDVDR!"

Carta 2: Do general para Júlio César

"FRPHFDUHPRV D LQYDVDR DPDQKD, SUHFLVDUHL GH PDLV WURSDV SDUD GHIHQGHU RV WHUULWRULRV MD FRQTXLVWDGRV."

Carta 3: De Júlio César para seu general

"MD PDQGHL PDLV WURSDV. FXLGDGR FRP RV LQLPLJRV H ERD VRUWH."

Carta 4: Do general para Júlio César

"FRPHFDUHPRV R DWDTXH DPDQKD SHOD PDGUXJDGD."

Figura 3 – Troca de Cartas
Fonte: Autoria Própria

Para ajudar os alunos a descobrir a mensagem, na situação estava escrito que a mudança das letras, na Cifra de César, era feita de maneira regular, como historicamente.

Durante o primeiro momento, os alunos tiveram ideias muito interessantes para decifrar a mensagem, entre as quais, destaca-se um diálogo ocorrido entre professor e o grupo de estudantes 1:

Professor: Como vocês pensaram para decifrar as mensagens?

Sujeito 1: Para que as palavras tenham sentido, as palavras têm que ter vogais no meio.

Sujeito 2: Letras que estão sozinhas também podem representar as vogais A, E ou O.

Destacam-se ainda outros diálogos interessantes, realizado por outro grupo de estudantes:

Sujeito 3: Pensamos que as letras D, R e H, que estão sozinhas podem ser as letras A, E e O.

Sujeito 4: Professor, também imaginamos que as letras que se repetem podem ser RR ou SS.

Um outro aluno do grupo 3 se questionou sobre como teria certeza de que aquela seria a Criptografia correta e foi auxiliado por um dos colegas de seu grupo.

Sujeito 5: Como sabemos que traduzimos certo?

Sujeito 6: É só ver se as palavras fazem sentido.

Todos os alunos conseguiram decifrar as mensagens escritas, analisar de uma forma similar como decifrariam a mensagem, fizeram o uso da frequência das palavras e ideias com base no raciocínio lógico. Depois de decifrarem a mensagem, tiveram que responder as seguintes perguntas mostradas na figura a seguir.

1- Quais são as traduções das mensagens?
2- Como essas mensagens foram criptografadas?
3- Considerando as letras do alfabeto como números, como na tabela abaixo

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figura 4 – Perguntas da Situação Desencadeadora de Aprendizagem
Fonte: Autoria Própria

As traduções da mensagem foram todas iguais e todos os alunos responderam de maneira correta e satisfatória. Para exemplificar a resposta dos alunos, usaremos a apresentada pelo grupo 2.

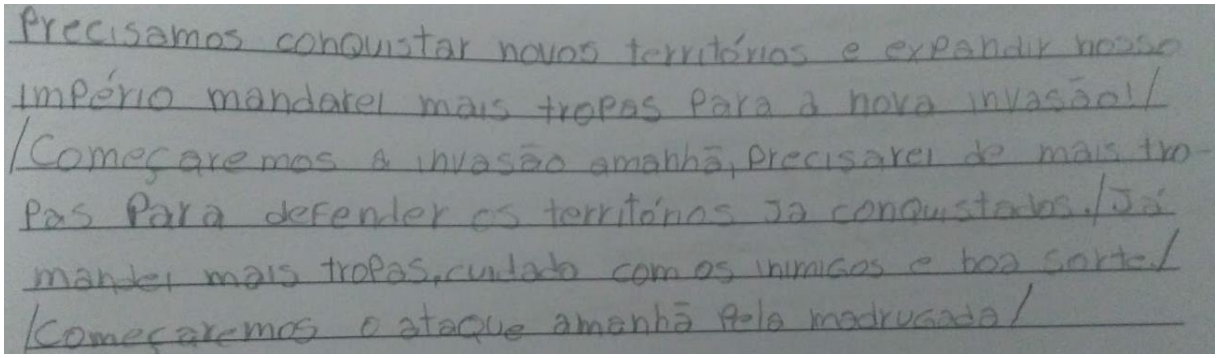

Figura 5 – Resposta da 1 questão feita pelos alunos do grupo 2
Fonte: Autoria Própria

A maior parte dos alunos, na segunda questão, respondeu que as letras “andaram” 3 posições fixas. Para a terceira questão, que podemos relacionar com diversos conteúdos matemáticos como álgebra, funções, equações e aritmética modular, grande parte dos alunos conseguiu perceber que foram transladadas e substituídas, começando por 3 que representa a letra A. Um grupo escreveu que as mudanças eram feitas adicionando 3 para representar a letra desejada e para as letras X,Y e Z adicionamos 3 e subtraímos 26, como mostra a figura a seguir.

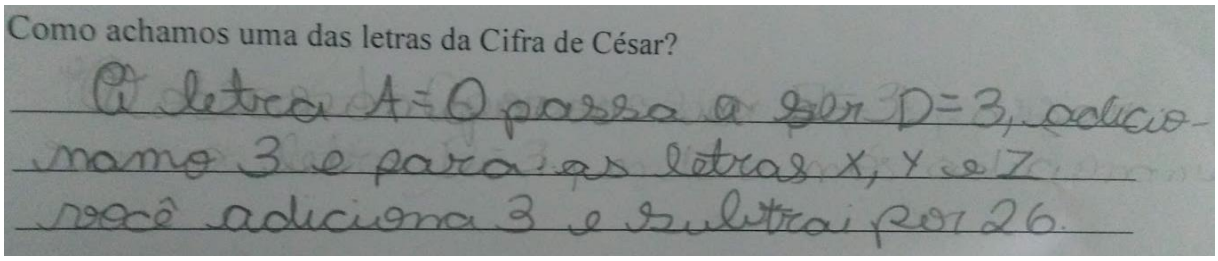

Figura 6 – Resposta da questão 3 do grupo 1
Fonte: Autoria Própria

Para finalizar a situação, os alunos criptografaram mensagens usando a Cifra de César para que os colegas decifrassem. A maior parte dos alunos conseguiu escrever a mensagem, entretanto alguns alunos erraram algumas letras, o que não inviabilizou o desenvolvimento da tarefa.

Um exemplo incorreto feito pelos alunos foi a mensagem “L ELJBJ AH IHOOL PLOOB BJ XOQFJDQL”. Conversando com o aluno, descobrimos que a frase escolhida era “O HOMEM DE FERRO MORRE EM ULTIMATO”. Fazendo uma análise do erro do grupo, percebemos que ele estabeleceu uma relação errada entre as letras da Cifra de César. Por exemplo, na palavra “AH” que deveria significar “DE”, ele estabeleceu que o uso da letra D para representar o A, implicaria no uso do A para representar o D, o que contraria a regra da Cifra de César, pois a letra D seria representada por G. Quando os alunos do outro grupo

foram decifrar a mensagem até conseguiram identificar o erro e escreveram algumas palavras, mas não conseguiram compreender a mensagem passada.

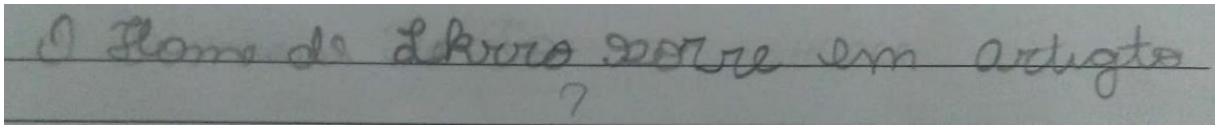

Figura 7 – Mensagem incorreta decifrada
Fonte: Autoria Própria

CONSIDERAÇÕES FINAIS

A possibilidade de organizar uma situação desencadeadora de aprendizagem a partir dos princípios teóricos da Atividade Orientadora de Ensino, dentro do projeto Clube de Matemática, vinculado à participação do PIBID, e considerando o crescente uso de dados e informações em algumas ferramentas de uso cotidiano, como o celular, entende-se que a compreensão do funcionamento da Criptografia e sua necessidade em nossa sociedade atual é algo relevante para os alunos. Considera-se que SDA apresentada aos estudantes teve resultado satisfatório e que os alunos se apropriaram e compreenderam esse conceito, assim como, o uso histórico e atual da Criptografia.

REFERÊNCIAS

BRASIL. Ministério da Educação e Cultura. **PCN+ Ensino Médio**: Orientações Educacionais complementares aos Parâmetros Curriculares Nacionais. v. 2, Brasília, 2002.

DANTAS, A. A. **A Criptografia no Ensino Fundamental e Médio**. 2016. 42 f. il Monografia (Especialização em Ensino de Matemática) – Universidade Federal do Rio Grande do Norte, Caicó, 2016.

D'AMBROSIO, B. S. Como ensinar matemática hoje? Temas e Debates. **SBEM**. Ano II. n. 2. Brasília p. 15-19. 1989.

GROENWALD, C. L. O.; OLGIN, C. A. Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia. In: CONFÊRENCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA, 8., 2011, Recife. **Anais...** Recife: CIAEM, 2011. Disponível em: < https://ciaem-redumate.org/ocs/index.php/xiii_ciaem/xiii_ciaem/index>. Acesso em: 03 jun. 2019.

TAVARES, N. P. et al. Criptografia: Uma ferramenta de ensino das operações matriciais. In: IV CONEDU, 2017, Joao Pessoa. **Anais...** Campina Grande: CONEDU, 2017. Disponível em: < http://conedu.com.br/2017/>. Acesso em: 03 jun. 2019.

THAWTE. **History of Cryptography**: an easy way to undestand history of cryptography. Estados Unidos da América. 2013.

LITOLDO, B. F.; LAZARI, H. Uma Análise do uso da Criptografia nos Livros Didáticos De Matemática Do Ensino Médio. **Revista Matemática, Ensino e Cultura**, n. 17, p. 135 – 156, set. - dez., 2014.

MOURA, M. O. de. A atividade de ensino como unidade formadora. **Bolema**, Ano II, n. 12. p. 29-43, 1996.

MOURA, M. O. de et al. Atividade Orientadora de Ensino: unidade entre ensino e aprendizagem. **Revista Diálogo Educacional**. v. 10, n. 29, Curitiba, p. 205-229, jan-abr. 2010.

MOURA, M. O. de; LANNER de MOURA, A. R. **Escola**: um espaço cultural. Matemática na educação infantil: conhecer, (re)criar - um modo de lidar com as dimensões do mundo. Diadema, 1998.

WEBER, R. F. **Criptografia Contemporânea**. VI Simpósio de Computadores Tolerantes a Falhas, Instituto de Informática - UFRGS, Porto Alegre, 1995.