2

Códigos de Cobertura

O campo de pesquisa que estuda a teoria dos códigos tem sido alvo de intensos estudos de um grande número de pesquisadores. Estes estudos englobam: aplicações de busca, uso em ferramentas computacionais, estudo de problemas relacionados, estudo de ligações com as mais diversas áreas da matemática como álgebra, combinatória, teoria da informação, entre outros (ver Cohen et al. [8] para uma visão geral da pesquisa em códigos de cobertura). Neste capítulo abordamos a parte da teoria dos códigos que trata dos códigos de cobertura, apresentando teoria, aplicações e trabalhos relacionados. O foco é dado em dois problemas desta área: o problema clássico de códigos de cobertura e o novo problema denominado códigos curtos de cobertura. Os problemas são apresentados com o foco principalmente nos códigos curtos, pois por se tratar de um problema novo, um dos objetivos deste trabalho é justificar seu estudo e mostrar sua relação com os códigos de cobertura clássicos.

PUC-Rio - Certificação Digital Nº 0711266/CA

2.1

Definições Básicas da Teoria dos Códigos

Seja o conjunto $\mathbb{F}_q$ de q símbolos $\mathbb{F}_q = \{0, 1, ..., q-1\}$, chamamos $\mathbb{F}_q$ de alfabeto. Quando q é uma potência de um número primo é conveniente considerar $\mathbb{F}_q$ como um corpo finito (*finite field*) de q elementos, de forma a podermos usar as propriedades provenientes desta estrutura algébrica (para uma descrição detalhada dos corpos ver [17]). Chamamos de palavras os vetores de tamanho n de elementos do alfabeto $\mathbb{F}_q$. Seja $\mathbb{F}_q^n$ o conjunto de todas as palavras de tamanho n sobre $\mathbb{F}_q$. Denomina-se código q-ário qualquer subconjunto não vazio de $\mathbb{F}_q^n$. Exemplificando cada conceito, seja $n = 3$ e $q = 2$, então:

- Alfabeto: $\mathbb{F}_2 = \{0, 1\}$.
- Exemplo de palavra: $x = (001)$.

– Espaço de palavras: $\mathbb{F}_2^3 = \{(000), (001), (010), (011), (100), (101), (110), (111)\}$.
– Exemplo de código q-ário de $\mathbb{F}_2^3$: $C = \{(001), (110), (100)\}$.

Definimos como *distância de Hamming* $d(x, y)$ entre duas palavras $x = (x_1 \dots x_n)$ e $y = (y_1 \dots y_n)$ de tamanho n, como o número de índices i nos quais $x_i \neq y_i$, ou seja, o número de coordenadas nos quais x e y diferem. Como exemplo, se tivermos $x = (010)$ e $y = (111)$, então $d(x, y) = 2$, já que $x_1 \neq y_1$ e $x_3 \neq y_3$. Chamamos de *esfera de Hamming* a esfera de centro na palavra x e raio R denotada por:

$$B(x, R) = \{y \in F_q^n : \ d(x, y) \leq R\}. \tag{2-1}$$

A esfera $B(x, R)$ corresponde ao conjunto de palavras de $\mathbb{F}_q^n$ que diferem em no máximo R coordenadas de x. A figura 2.1 exemplifica a esfera de centro $x = (11)$ e raio $R = 1$ para $\mathbb{F}_3^2$ ($B(x, 1) = \{(11), (12), (01), (21), (10)\}$).

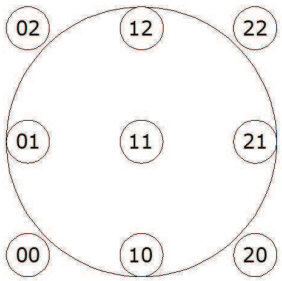

Figura 2.1: *Esfera de Hamming* de centro $x = (11)$, $R = 1$ para $\mathbb{F}_3^2$.

PUC-Rio - Certificação Digital Nº 0711266/CA

2.2
Códigos Corretores de Erros

Uma das principais aplicações da teoria dos códigos são os chamados códigos corretores de erros. Na teoria da informação deseja-se encontrar métodos rápidos e confiáveis para transmissão de informações. É necessário primeiramente codificar a informação usando um *código fonte* apropriado, seja para converter a informação de analógica para digital ou para comprimir os dados. Para atingir uma transmissão confiável sobre um canal ruidoso, a informação é então codificada usando um código de canal apropriado, isto é, um código corretor de erros, conforme [17].

Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade. São

exemplos disso todas as comunicações via satélite, as comunicações internas de um computador, o armazenamento de dados em fitas ou disquetes magnéticos, ou o armazenamento ótico de dados, [16]. Métodos algébricos e combinatórios frequentemente provêem bons códigos, ou seja, códigos tendo uma estrutura rica que tornam fáceis as tarefas de codificação e decodificação (ver [17]).

Seja $d(C)$ a menor *distância de Hamming* entre pares de palavras de um código C. Como exemplo, se considerarmos $C = \{(001), (110), (100)\}$, então $d(C) = 1$, já que $d(110, 100) = 1$.

Assuma que $C \subseteq \mathbb{F}_q^n$ tem uma distância mínima $d(C) = 2e + 1$. Suponha que umas das palavras $c \in C$ é transmitida em um canal ruidoso e durante esta transmissão ocorrem no máximo e erros, isto é, no máximo e coordenadas do vetor c foram alteradas. Se o receptor souber que uma das palavras do código foi transmitida e decodificar a palavra recebida para a palavra do código mais próxima (menor *distância de Hamming*), a palavra c originalmente transmitida pode ser recuperada, simplesmente porque as esferas de Hamming de raio e centradas nas palavras de C são disjuntas. Por esta razão chama-se o código C de e-código corretor de erro. Para estar apto a enviar o máximo de informação possível em uma unidade de tempo, seria interessante que C tivesse a maior cardinalidade possível. O problema de achar o código C de maior cardinalidade possível com distância mínima $d(C) = e$ é um dos problema clássicos da teoria dos códigos, e tem uma importância fundamental na prática, como explicado no início desta seção (detalhes sobre os códigos corretores de erros podem ser encontrados em [17]). Neste trabalho abordamos o problema dual a este dos códigos corretores de erros, o problema clássico de códigos de cobertura, além disto, tratamos também de uma variação dos códigos de cobertura, os denominados códigos curtos de cobertura.

PUC-Rio - Certificação Digital Nº 0711266/CA

2.3

Códigos de Cobertura e Códigos Curtos de Cobertura

Nesta seção abordamos tanto os códigos clássicos de cobertura quanto os códigos curtos, dando ênfase aos códigos curtos, com vistas a justificar o seu estudo, já que este é um problema recente que [29], e não há trabalhos que utilizem buscas computacionais para obtenção de limites para o mesmo.

Seja $\mathbb{F}_q$ um corpo finito de q elementos. Dado inteiros $n \geq 2$ e $0 \leq R \leq n$, $c_q(n, R)$ é definido como a menor cardinalidade de um subconjunto H de $\mathbb{F}_q^n$ de forma que para toda palavra x neste espaço, x seja diferente em no máximo

R coordenadas de um vetor múltiplo escalar de H. O problema de determinar $c_q(n, R)$ para q, n e R arbitrários é chamado problema de códigos curtos de cobertura.

Uma das razões para o estudo de códigos curtos de coberturas é sua relação com o problema clássico de códigos de cobertura. Seja $K_q(n, R)$ o número que denota a cardinalidade mínima de um código C q-ário de tamanho n, de forma que para toda palavra x do espaço, exista uma palavra c em C no qual x e c sejam diferentes em no máximo R coordenadas. Estes números foram apresentados para $R = 1$ por Taussky e Todd [40] de um contexto puramente teórico, mas foram generalizados para um R arbitrário por Carnielli [5].

O chamado problema do football pool é uma interessante aplicação que se tornou um dos problemas mais famosos em teoria dos códigos. Neste problema queremos encontrar o menor número de apostas que devemos fazer de forma a errar o resultado (vitória, empate ou derrota do time mandante) de no máximo um jogo. Isto corresponde ao caso em que $q = 3$ e $R = 1$, pois $K_3(n, 1)$ nos dá a garantia da melhor maneira de garantir $n - 1$ apostas corretas em uma rodada de jogos de futebol com n jogos. O caso em que $n = 6$ tem sido objeto de tremendos esforços na melhoria do limite inferior, hoje em dia está em 71 de acordo com Linderoth et al.[21], enquanto o limite superior permanece em 73 desde 1989 (ver [19]).

Algumas das motivações para o estudo de coberturas curtas de códigos são listadas abaixo:

- Do ponto de vista teórico, coberturas curtas parecem ser uma estrutura mais rica algebricamente do que as coberturas clássicas, já que as coberturas curtas são invariantes sobre a multiplicação escalar. Além disto, coberturas curtas estão conectadas com diversos conceitos algébricos (ver [28, 29]).
- Do ponto de vista prático, coberturas curtas nos dão uma maneira de armazenar códigos utilizando menos memória que no caso da cobertura clássica.
- Resultados obtidos para as coberturas curtas podem levar a resultados recordes para o problema clássico de cobertura de códigos.

Vamos descrever mais formalmente os códigos clássicos e os curtos de cobertura. Para $n \geq 2$ a $q \geq 2$, V_q^n seja o conjunto de todas as palavras

PUC-Rio - Certificação Digital Nº 0711266/CA

$(x_1x_2\ldots x_n)$ com tamanho n e componentes x_i do alfabeto de q símbolos. Um subconjunto C é uma *R-cobertura* de V_q^n quando:

$$\bigcup_{c\in C} B(c,R) = V_q^n.$$

Então, o número $K_q(n,R)$ denota a menor cardinalidade de uma *R-cobertura* de V_q^n. Os principais resultados e ferramentas nestes números são apresentados em [8].

Por outro lado, um subconjunto H no espaço de vetores $\mathbb{F}_q^n$ é uma *R-cobertura curta de* $\mathbb{F}_q^n$ quando $\mathbb{F}_q.H = \{\alpha h, \alpha \in \mathbb{F}_q \text{ and } h \in H\}$ é uma R-cobertura de $\mathbb{F}_q^n$. Em outras palavras, H é uma R-cobertura curta de $\mathbb{F}_q^n$ se todo x em $\mathbb{F}_q^n$ pode ser escrito como a soma de um múltiplo $h \in H$ e uma combinação linear de no máximo R vetores canônicos. O problema induzido $c_q(n,R)$ é definido como a menor cardinalidade deste subconjunto H, isto é:

$$c_q(n,R) = \min\{\ |H| : H \text{ é uma } R\text{-cobertura curta de } \mathbb{F}_q^n\ \}.$$

É importante notar que H é uma cobertura curta se o conjunto que contém H e todos seus múltiplos escalares gera uma cobertura de $\mathbb{F}_q^n$. Por exemplo, a menor 1-cobertura curta de $\mathbb{F}_q^2$ precisa apenas de um vetor $(c_q(2,1) = 1)$, em contraste com o fato que q vetores são necessários na menor cobertura clássica de $\mathbb{F}_q^2$ $(K_q(2,1) = q)$.

2.3.1

Resultados Teóricos

Nesta seção apresenta-se alguns resultados em $c_q(n,R)$ demonstrados em [29]. Estes resultados servem de base para análise dos resultados obtidos pelos métodos computacionais propostos neste trabalho. As provas dos teoremas e proposições são suprimidas pois estão descritas em [29].

Proposição 2.1 *(Limite Superior Trivial) Para uma potência de primo q,* $0 \leq R < n$,

$$c_q(n,R) \leq \frac{q^{n-R}-1}{q-1}.$$

O limite inferior abaixo é similar ao limite clássico de esferas de cobertura para as coberturas clássicas $K_q(n,R)$. Seja v o número que denota o número

PUC-Rio - Certificação Digital Nº 0711266/CA

de vetores em uma esfera de $\mathbb{F}_q^n$ de raio R, isto é, $v = 1 + \sum_{i=1}^{R} \binom{n}{i}(q-1)^i$.

Proposição 2.2 *(Limite de Esfera de Cobertura em c) Para uma potência de primo q,*

$$c_q(n, R) \geq \left\lceil \frac{q^n - v}{(q-1)v} \right\rceil .$$

O próximo resultado constitui uma maneira sistemática de traduzir limites entre os problemas de códigos de cobertura.

Teorema 2.3 *Para uma potência de primo q e $n > R > 0$,*

$$c_q(n, R) + 1 \leq K_q(n, R) \leq (q-1)c_q(n, R) + 1.$$

PUC-Rio - Certificação Digital Nº 0711266/CA

Ambas desigualdades são exatas pelo menos para $q = 2$, assim $c_2(n, R) = K_2(n, R) - 1$. O teorema 2.5 abaixo descreve outra classe de onde a segunda desigualdade é exata.

Não é de surpreender que nosso conhecimento em classes exatas em $c_q(n, R)$ seja bastante escasso, já que a computação de $c_q(n, R)$ parece ser tão difícil quanto a dos números clássicos $K_q(n, R)$. Abaixo revemos algumas classes exatas apresentadas em [29].

Teorema 2.4 *Para toda potência de primo q, e n de forma que $n = (q^t - 1)/(q-1)$ para algum t,*

$$c_q(n, 1) = \frac{q^{n-t} - 1}{q - 1}.$$

Teorema 2.5 *Têm-se $c_q(n, n-t) = 1$ se e somente se existe $n \geq (t-1)q + 1$.*

Teorema 2.6 *Para uma potência de primo $q \geq 4$, $c_q(q, q-2) = 2$.*

Teorema 2.7 *Para todo n, $c_3(3n, 2n-1) = 3$.*

2.3.2

Códigos de Cobertura e Conjuntos Dominantes em Grafos

Nesta seção nós relembramos o problema de conjuntos dominantes em grafos e mostramos como os problemas de códigos de cobertura podem ser reduzidos ao mesmo.

Seja $G = (V, E)$ um grafo direcionado com um conjunto de vértices V e uma coleção E de pares ordenados em $V \times V$. Como usual, u é adjacente a v (ou v é vizinho de u) quando $(u, v) \in E$. O subconjunto de vértices $U \subseteq V$ é chamado de *conjunto dominante* de G se, para todo v em V, ou v está em U ou existe um vértice u em U de forma que u é adjacente a v (*i.e.*, $(u, v) \in E$). O problema de conjuntos dominantes em grafos é o problema de encontrar o conjunto dominante de G de menor cardinalidade. Este problema é fortemente *NP*-difícil (ver Garey e Johnson [13]).

Teorema 2.8 *Códigos curtos de cobertura correspondem a uma classe de conjuntos dominantes em grafos direcionados.*

A tradução de códigos curtos de cobertura para teoria dos grafos é descrita a seguir. Dado o espaço de vetores $\mathbb{F}_q^n$ e $0 \leq R \leq n$, construímos um grafo direcionado $G(n, q, R) = (V, E)$ como se segue. Para cada vetor u em $\mathbb{F}_q^n$ associamos um vértice u em V. A aresta $e = (u, v)$ está em E se e somente se $\alpha \in \mathbb{F}_q$ de forma que $0 < d(\alpha u, v) \leq R$. O conjunto E não é uma relação simétrica para $n \geq 2$. De fato, $(u, 0) \in E$ para cada vetor não-nulo u, mas $(0, u) \in E$ apenas quando $0 < d(0, u) \leq R$. Note que conjuntos dominantes em $G(n, q, R)$ estão em correspondência um-para-um com os códigos que são R-coberturas curtas em $\mathbb{F}_q^n$. Assim, o problema de encontrar o menor código que é uma R-cobertura curta em $\mathbb{F}_q^n$ corresponde ao problema de encontrar o menor conjunto dominante em $G(n, q, R)$.

O problema clássico de determinar o menor código que é uma R-cobertura de V_k^n também pode ser mapeado no problema de achar o conjunto dominante mínimo em um grafo. Isto pode ser feito fazendo as seguintes modificações na construção descrita acima: *(i)* usar k no lugar de q, *(ii)* usar V_k^n no lugar de $\mathbb{F}_q^n$, *(iii)* substituir a regra "existir $\alpha \in \mathbb{F}_q$ de forma que $0 < d(\alpha u, v) \leq R$"pela regra "$0 < d(u, v) \leq R$"(ver [6]).

A figura 2.2 mostra o grafo resultante para o problema de determinar $K_2(3, 1)$, onde cada retângulo representa um vértice do grafo (palavra de V_2^3) e cada ligação entre dois retângulos x e y representa uma aresta do mesmo, ou

PUC-Rio - Certificação Digital Nº 0711266/CA

seja, $d(x, y) = 1$. Como podemos notar pela figura, o grafo resultante possui muita simetria e regularidade, esta característica é intrínseca aos problemas de códigos de cobertura e aumenta significativamente a dificuldade dos mesmos.

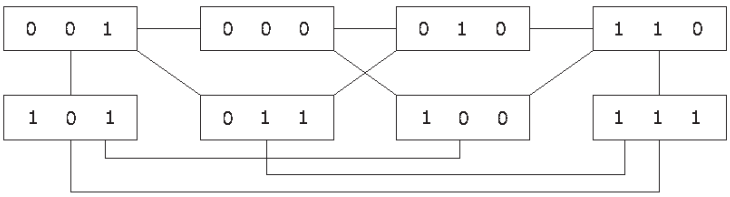

Figura 2.2: Grafo para $K_2(3, 1)$.

Na figura 2.3 ilustramos um conjunto dominante de cardinalidade três para o grafo do $K_2(3, 1)$, ou seja, uma 1-cobertura de V_2^3, sendo a mesma formada pelo código $C = \{(000), (010), (111)\}$. Os retângulos destacados em preto representam as palavras do código C, as ligações destacadas com linhas espessas representam as arestas que ligam as palavras de C aos seus vizinhos e os retângulos hachurados em cinza representam as palavras cobertas por C. Como neste caso C é uma 1-cobertura (conjunto dominante) todos os retângulos estão hachurados.

A figura 2.4 ilustra uma solução inviável, um código de cardinalidade dois que não é um conjunto dominante para o grafo do $K_2(3, 1)$, ou seja, não é uma 1-cobertura para V_2^3, já que as palavras (101) e (111) não são cobertas. As convenções da figura são as mesmas descritas anteriormente.

A figura 2.5 ilustra uma solução ótima para $K_2(3, 1)$, um código de

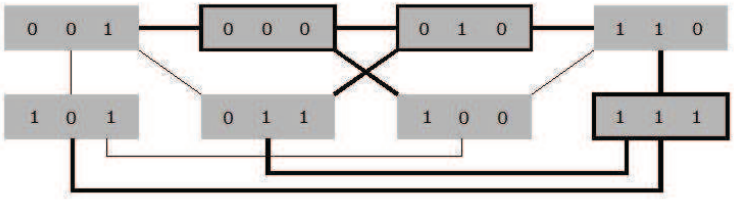

Figura 2.3: Conjunto dominante para o grafo do $K_2(3, 1)$.

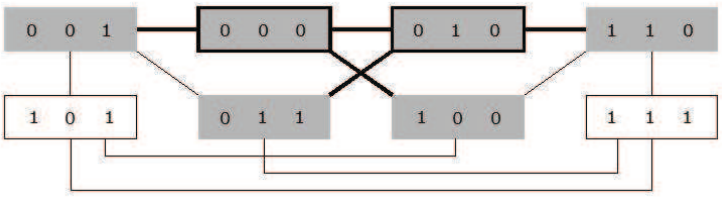

Figura 2.4: Solução inviável para $K_2(3, 1)$.

PUC-Rio - Certificação Digital Nº 0711266/CA

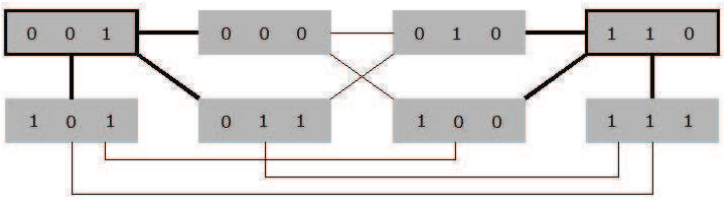

Figura 2.5: Solução ótima para $K_2(3,1)$.

cardinalidade dois que é uma 1-cobertura de V_2^3 ($C = \{(001),(110)\}$), o que equivale a um conjunto dominante de cardinalidade dois para o grafo do $K_2(3,1)$.

As heurísticas apresentadas neste trabalho tratam os problemas de códigos de cobertura usando justamente esta formulação como conjuntos dominantes em grafos.

2.4 Trabalhos Relacionados

Em 1948, Taussky e Todd [40] introduziram o seguinte problema da teoria dos grupos: Seja G um grupo abeliano com n geradores independentes g_1; g_2; ...; g_n , cada um de ordem q. Um subconjunto $H \in G$ é chamado de cobertura de G se, para cada $g \in G$, exista um $h \in H$ de forma que $g = hg_i^a$ para algum $1 \leq i \leq n$, $0 \leq a \leq q-1$. O problema é então, para dados n e q, encontrar o subconjunto $H \in G$ de menor cardinalidade que seja uma cobertura de G. Neste contexto da teoria dos grupos o problema foi abordado por inúmeros trabalhos, como em [23] e [25].

Na realidade, muito antes do paper [40] de Taussky e Todd aparecer existia um grande interesse neste problema entre os entusiastas de apostas em jogos de futebol nos países nórdicos. O chamado problema do football pool abordado na seção 2.3, que é equivalente ao problema clássico de códigos de cobertura, é um problema mais geral do que o introduzido por Taussky e Todd, sendo que a ligação entre os dois problemas só foi percebida e explicitada em 1950 no trabalho de Mattioli [24]. O grande entusiasmo no estudo do problema do football pool foi o que impulsionou a pesquisa nos problemas de códigos de cobertura, [33].

A pesquisa nos códigos de cobertura resultou no surgimento de diversas variações do problema clássico como o problema dos códigos mistos de cobertura (ver [33]) e o problema dos códigos curtos de cobertura, abordado ante-

PUC-Rio - Certificação Digital Nº 0711266/CA

riormente. O estudo de problemas relacionados tem como um dos principais motivos a aplicação no problema clássico. Diversos resultados apresentados nessas variações resultaram em melhorias nos resultados do problema clássico, como mostrado em [33].

O problema de encontrar códigos de cardinalidade mínima que satisfazem um conjunto de propriedades de cobertura esta longe de ser trivial. Valores exatos têm sido obtidos apenas para casos especiais ou de tamanho bastante reduzido. Para casos gerais, os esforços se concentram na obtenção de limites inferiores e superiores sobre a cardinalidade mínima dos códigos de cobertura. Bons limites inferiores podem ser obtidos por uma vasta gama de métodos analíticos, como demonstrado em [9] e [10]. Já os limites superiores, por outro lado, são encontrados pela construção explícita dos códigos de cobertura. Este trabalho está inserido justamente neste contexto, ele apresenta técnicas para obtenção de bons limites superiores, pela construção explícita dos códigos de cobertura, para dois problemas: o problema clássico de códigos de cobertura e o problema dos códigos curtos de cobertura. As técnicas apresentadas fazem parte de um tipo especial de algoritmos de otimização combinatória: as heurísticas de busca local (as buscas locais são detalhadas no capítulo 3). Para um histórico detalhado sobre técnicas de construção de códigos de cobertura ver os trabalhos [19] e [22].

Os primeiros trabalhos [17] que usaram heurísticas de busca local para determinar limites para os códigos clássicos de cobertura utilizavam quase que exclusivamente a metaeurística *Simulated Annealing*(para uma descrição da metaeurística simulated annealing ver [37]). O objetivo da heurística era encontrar códigos viáveis, ou seja, que cobrissem todas as palavras do espaço, para um determinado tamanho(número de palavras) M de código fixado a priori. Cada vez que a heurística encontrasse um código viável de tamanho M este valor era então diminuído de um e a heurística reiniciava buscando por códigos viáveis de tamanho $M-1$. A função objetivo utilizada correspondia ao número de palavras não-cobertas pela solução atual. Já a estrutura de vizinhança consistia em alterar i $(1 \leq i \leq R)$ coordenadas de uma das palavras do código.

Esta versão do simulated annealing e pequenas variações dela foram utilizadas em diversos trabalhos para melhoria dos limites para os códigos de cobertura. Esta abordagem foi usada por Wille [41] para mostrar que $K_3(6,1) \leq 74$, por Van Laarhoven et al. [19] para provar que $K_3(6,1) \leq 73$ e $K_3(7,1) \leq 186$, por Östergård ([32], [33], [34]) e Wille [42] para obter inúmeros outros limites recordes. Outros resultados interessantes utilizando o simulated

PUC-Rio - Certificação Digital Nº 0711266/CA

annealing podem ser encontrados nos trabalhos de Aarts et. al [1] e Van Lint [22].

O primeiro trabalho utilizando a busca tabu para obter limites para os códigos de cobertura foi o trabalho de Östergård [35]. Neste trabalho ele mostrou que o tempo para obtenção de determinados limites poderia ser melhorado pelo uso da busca tabu. A lista tabu utilizada consistia dos índices das palavras perturbadas recentemente, ou seja, se a palavra c_i do código fosse perturbada(alterada), então o índice i da mesma era incluído na lista tabu. W.A. Carnielli et. al [6] utilizam também a busca tabu para o problema dos códigos de cobertura. Este trabalho difere dos outros por utilizar um espaço de busca diferente, o qual é detalhado no capítulo 4 na seção 4.1.1. A busca tabu proposta no capítulo 4 é baseada na busca tabu apresentada no referido trabalho.

PUC-Rio - Certificação Digital Nº 0711266/CA