DOI: 10.20396/revpibic2720192268

Estudo do Rendimento do Código SPC Produto

Natália S. Parra*, Sara D. Cardell, Marcelo Firer

Resumo

Códigos Single Parity Check (SPC) são [n, k]-códigos binários lineares, onde k = n -1, cujas palavras sempre possuem peso de Hamming par. Além disso, todo código SPC é MDS, implicando em distância mínima d=2. Códigos SPC produto são construidos a partir do produto tensorial entre códigos SPC. Nesse caso, estudamos apenas o produto entre um código SPC consigo mesmo, resultando nos parâmetros [n², (n-1)², 4]. Sobre um canal binário de apagamentos (BEC), são capazes de corrigir qualquer padrão de até 3 apagamentos e, em alguns casos, corrigem padrões de 4 a 2n-1 erros. Para estudar este problema, utilizou-se abordagens baseadas em análise combinatória, teoria dos grafos bipartidos e dependência linear em matrizes binárias, com intuito de realizar a contagem de padrões corrigíveis para n>8.

Palavras-chave:

Canal de Apagamentos, Código Produto, Código Single-Parity Check.

Introdução

O canal binário de apagamentos é um dos modelos de canais mais simples, consistindo de bits transmitidos que podem ser recebidos perfeitamente ou apagados. O problema de decodificação trata-se de obter a informação perdida dadas as posições dos apagamentos e a parte não apagada da palavra. Um código linear de parâmetros [n,k,d] pode recuperar até d-1 apagamentos.

Neste trabalho, considerou-se o código gerado pelo produto entre o mesmo código de parâmetros [n, n-1, 2], chamado de código SPC, corrigindo apenas 1 apagamento. O código resultante possui parâmetros [n², (n-1)², 4], porém pode corrigir até 2n-1 apagamentos em casos especiais. Para estudá-los, utilizam-se matrizes n×n, denominadas padrões de erro, com t ≤ n² entradas indicando posições dos apagamentos na palavra do código SPC produto. Se há apenas um bit é apagado em uma linha ou coluna, este pode ser recuperado, se não, é pulado. O decodificador percorre iterativamente as linhas e colunas do padrão, até que nada mais possa ser corrigido. Um padrão de apagamentos é dito corrigível se a palavra pode ser recuperada cada completamente, caso contrário, é incorrigível.

É provado que se t ≤ 3 o padrão é sempre corrigível, enquanto é incorrigível para t ≥ 2. O objetivo deste projeto é contar o número de padrões corrigíveis (ou incorrigíveis) possíveis com t apagamentos, onde 4 ≤ t ≤ 2n − 1.

Resultados e Discussão

Para tentar resolver o problema de contagem de padrões, utilizou-se abordagens variadas. A mais simples foi análise combinatória, posicionando os apagamentos de maneira a gerar padrões incorrigíveis

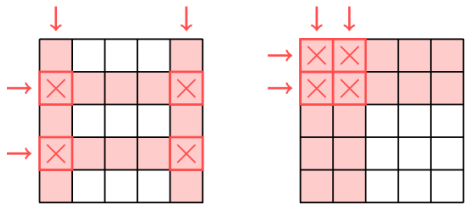

Figura 1. Exemplo de padrões incorrigíveis com t=4 e n=5.

para um t fixado e calculando todas as permutações possíveis. Conforme t aumenta, o processo torna-se exaustivo, sendo t=8 a última contagem realizada por este método.

Um padrão de erro com t apagamentos pode ser representado por um grafo bipartido balanceado de t arestas e 2n vértices, coincidindo com sua matriz de biadjacência. Partindo do teorema de que um apagamento é incorrigível se, e somente se, existe um ciclo no grafo bipartido correspondente, o problema passa a ser a contagem de grafos bipartidos com n vértices em cada classe, t arestas, que contêm pelo menos um ciclo. Uma maneira equivalente de interpretar é como o número de árvores contidas neste grafo sendo a quantidade de padrões corrigíveis.

Por último, obteve-se um resultado inédito, indicando que, se as posições dos apagamentos correspondem a colunas linearmente dependentes da matriz de checagem de paridade, o padrão é incorrigível. Como consequência direta, segue o limitante inferior 2^{2n-1} para padrões estritamente incorrigíveis.

Conclusão

O problema do número de padrões incorrigíveis de tamanho n × n com t apagamentos, para 4 ≤ t ≤ 2n − 1, permanece um problema em aberto. Porém, estudando os resultados já conhecidos de análise combinatória e grafos, foi possível compreender o problema e surgir com uma nova abordagem, baseada em álgebra de matrizes.

Agradecimentos

Agradecemos ao apoio financeiro da Fapesp a ao apoio institucional do Prof. LD Marcelo Firer.

[1] CARDELL, S. D.; CLIMENT, J. J.; An Approach to the Performance of SPC Product Codes on the Ereasure Channel; Advances in Mathematics of Communications; 2016.

[2] CARDELL, S. D.; CLIMENT, J. J.; SPC Product Codes over the Erasure Channel; CIM Series in Mathematical Sciences, volume 3.; 2014.

[3] COVER, T. M.; THOMAS, J. A.; Elements of Information Theory; Wiley-Interscience; 2006.

[4] JUSTESEN, J.; HOHOLDOT T.; A Course in Error-Correcting Codes; Euro-
pean Mathematical Society; 2004.

[5] TRAPPE, W.; WASHINGTON, L. C.; Introduction to Cryptography with Coding Theory; Prentice Hall; 2006.