Estudo e Desenvolvimento em hardware de Códigos Corretores de Erros

Luís Vitório Cargnini

Orientador: Prof. Dr. Rubem Dutra Ribeiro Fagundes

23 de Março de 2007

Dedico este trabalho primeiramente a minha esposa, que sobreviveu ao meu mestrado (e terá que sobreviver ao doutorado). Sempre está comigo, esse mestrado também é seu. Somente quem vive o que você e eu vivemos poderia entender. Claro ao meu "desorientador", Rubinho e sua senhora Regina, ele que foi o grande arquiteto deste trabalho, sem o qual não haveria esta dissertação.

Agradecimentos

Primeiramente e sempre eu agradeço a minha esposa, por estar sempre comigo, acima de tudo.

Agradeço ao meu inigualável, incomparável, único orientador professor Doutor Rubem Dutra Ribeiro Fagundes e sua família. Este trabalho só existe hoje porque o senhor me orientou. Obrigado por nunca exigir menos, sempre mais, se trabalha-se 12 horas, o senhor exigia 20, 21, 24, 48, 72, 96 horas se fosse preciso. Obrigado.

Agradeço a empresa Instramed que financiou o meu mestrado. Agradeço ao CNPQ, órgão de fomento que financiou o meu mestrado no início. Agradeço ao professor Doutor Fabian Luis Vargas por ter me orientado no início do mestrado.

Aos professores Dr. Fabiano Passuelo Hessel e Dr. Eduaro Augusto Bezerra, que me apresentaram ao professor Rubem.

Aos professores Dr. Fernando César Comparsi e Dra. Maria Cristina Felippetto de Castro, por fazerem uso de parte do desenvolvimento que gerou esta dissertação.

A indústria japonsesa de Animes, uma grande fonte de distrações, sem dúvida alguma. Ao mestre Nakatsui Yusuke, quinto Dan de IGO, meu Sensei de IGO e seu filho Alberto. Ao professor Isao Ishibashi que promoveu a turma de IGO.

Agradeço ao pessoal da secretaria do PPGEE (Inelve, Helena, Edelvira, Nádia e Cláudia), que sempre me atenderam prontamente.

Agradeço a todos aqueles que contribuíram direta e indiretamente para meu Mestrado.

Sumário

1 Introdução **14**

1.1 Objetivos 16

2 Fundamentação Teórica **18**

2.1 Álgebra Abstrata 19

2.2 Grupos, Corpos e Espaço Vetorial 20

2.2.1 Grupos 21

2.2.2 Ordem de um elemento do Grupo. 24

2.2.3 Classes Laterais 25

2.2.4 Anéis 26

2.2.5 Corpos 27

2.2.6 Espaço Vetorial 29

2.2.7 Spanning Sets 29

2.2.8 Bases 30

2.2.9 Espaço Vetorial 30

2.2.10 Codificação na forma sistemática 31

2.2.11 Pesos e distâncias 32

2.2.12 Códigos de Hamming 33

2.2.13 O peso é a distância 34

2.3 Códigos de bloco lineares 34

2.3.1 Codificando e decodificando Códigos de bloco lineares . . 35

2.3.2 Matriz de Verificação de Paridade e Matriz Geradora . . . 35

2.3.3 Codificação e decodificação de blocos de códigos lineares . 36

2.3.4 Síndromes 37
2.4 Reed-Solomon 40
2.4.1 Decodificação RS 42
2.5 Bose-Chaudhuri-Hocquenghem 44
2.5.1 Codificação BCH 46
2.6 Algoritmos de ECC para decodificação consagrados 48
2.6.1 Peterson-Gorenstein-Zierler 48
2.6.2 Berlekamp-Massey 53
2.6.3 Euclideano 56

3 Desenvolvimento em hardware de Códigos Corretores de Erros 58
3.1 Descrição 60
3.2 Codificador Reed-Solomon 61
3.2.1 Características do Sistema 62
3.2.2 Paralelismo 63
3.2.3 Robustez 63
3.3 BCH Algébrico 67
3.4 BCH Multidimensional 72

4 Metodologia 80
4.1 Ferramentas de desenvolvimento 80
4.1.1 Sintetizadores 89
4.1.2 Ferramentas Matemáticas 94
4.1.3 Simulação dos códigos 97

5 Resultados 100
5.1 Resultados da Síntese 102
5.2 BCH encoder algébrico $(63, 57)$ 102
5.3 BCH decoder Algébrico 103
5.4 BCH encoder Algébrico XCV4SX35 $(63, 57)$ 104
5.5 BCH decoder Algébrico xc4vsx35 104
5.6 Codificador Reed-Solomon $(204, 188)$ 104
5.7 Decodificador Reed-Solomon Euclideano 104

5.8 BCH Multidimensional 108
5.8.1 Relatório de síntese do codificador 108
5.8.2 Relatório de síntese do decodificador 109
5.8.3 BCH MultiDimensional x Reed-Solomon 109

6 Conclusões **118**
6.1 Trabalhos Futuros 119

A Trabalhos Relacionados **127**

B Paper Aceito sobre BCH Algébrico **134**

C Paper "na fila de avaliação"sobre BCH Algébrico **135**

Abstract

This work has been developed error correcting codes: the Bose-Chaudhuri-Hocquenghem (BCH) and the Reed-Solomon (RS). Coders BCH had been implemented directly from the algebraic approach, using as tool, a hardware description language (VHDL), as well as the implementation of prototypes using Field Programable Gate Arrays (FPGA).

The achieved results had clearly showed that the increasing performance of these code algorithms, either in the aspect of execution speed, and in FPGA device area usage. The achieved success in the code implementation in FPGA was not about the implementation itself, since there are some similar accomplishments in the market and the academy. The main stone is the fact of using the original algebraic formulation, that is, without the job of usual iterative algorithms (sequential) in the implementation of the BCH. With the results of the BCH algebraic a new code for symbols based in the BCH, has been proprosed, that will be presented as a new alternative to the Reed-Solomon, for surpassing it, as much in time as area to be implemented.

Thus, this work test that, with the advance of the resources for rapid prototyping of Very Large Scale Integration (VLSI) technologies, and the hardware description of the code using it original algebraic description, results in a system with impressive performance, as consequence of the paradigm changing, based until the moment in polynomial sequential processing, to a new paradigm of hardware parallelism, executing the algebraic model.

Resumo

Neste trabalho foram desenvolvidos códigos corretores de erros, como Bose-Chaudhuri-Hocquenghem (BCH) e o Reed-Solomon (RS). Os codificadores BCH foram implementados diretamente de suas abordagens algébricas, empregando como ferramenta uma linguagem de descrição de hardware (VHDL), bem como a implementação de um protótipo utilizando Field Programable Gate Arrays (FPGA).

Os resultados obtidos demonstraram claramente que o desempenho destes algoritmos de codificação aumentam consideravelmente, tanto no aspecto de velocidade de execução, quanto a área ocupada do dispositivo FPGA. O sucesso deste trabalho não está na implementação em FPGA destes codificadores, uma vez que existem no mercado e na academia várias realizações similares, mas no fato de empregar como abordagem de implementação e desenvolvimento dos codificadores a formulação **algébrica** original, isto é, sem o emprego de algoritmos iterativos usuais (seqüenciais) na implementação do BCH. Não obstante, com os resultados do BCH algébrico propõe-se um novo código para símbolos, que será apresentado como uma nova alternativa ao Reed-Solomon, por superá-lo, tanto em tempo de codificação, como área para ser implementado.

Assim, este trabalho prova que, com o avanço dos recursos de prototipação e desenvolvimento de tecnologias VLSI, e com a descrição em hardware do código na sua formulação algébrica original, obtém-se um sistema com impressionante desempenho, resultante da mudança de paradigma, baseado até o momento em processamento seqüencial polinomial, para um novo paradigma de paralelismo de hardware, executando o modelo algébrico do código.