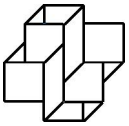


Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Códigos Quânticos de Correção de Erros do tipo CWS

Por

Douglas Frederico Guimarães Santiago

PETRÓPOLIS, RJ - BRASIL

FEVEREIRO DE 2013

CÓDIGOS QUÂNTICOS DE CORREÇÃO DE ERROS DO TIPO CWS

Douglas Frederico Guimarães Santiago

TESE SUBMETIDA AO CORPO DOCENTE DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM MODELAGEM COMPUTACIONAL

Aprovada por:

Prof. Renato Portugal, D.Sc
(Presidente)

Prof. Gilson Antônio Giraldi, D.Sc.

Prof. Francisco Marcos de Assis, D.Sc.

Prof. Giuliano Gadioli La Guardia, D.Sc.

PETRÓPOLIS, RJ - BRASIL
FEVEREIRO DE 2013

Santiago, Douglas Frederico Guimarães

S235c Códigos quânticos de correção de erros do tipo cws / Douglas Frederico Guimarães Santiago. Petropólis, RJ. : Laboratório Nacional de Computação Científica, 2013.

xiv, 94 p. : il.; 29 cm

Orientador: Renato Portugal

Tese (D.Sc.) – Laboratório Nacional de Computação Científica, 2013.

1. Computadores Quânticos. 2. Códigos Quânticos de Correção de Erros. 3. Codeword Stabilized Quantum Codes. 4. Códigos CWS. I. Portugal, Renato. II. LNCC/MCT. III. Título.

CDD 004.1

Coragem não é a ausência de medo, é
enfrentá-lo, não importa quão grande seja.

Dedico esta Tese à minha mãe, Angela Maria Guimarães da Silva.

Agradecimentos

Agradeço, aos meus pais, por minha existência e criação.

Ao meu orientador, pelos ensinamentos e paciência.

A todos os professores de minha vida acadêmica, pelo conhecimento adquirido.

Ao CNPQ, pelo auxílio financeiro.

A todos os amigos que torceram por mim.

Resumo da Tese apresentada ao LNCC/MCT como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

CÓDIGOS QUÂNTICOS DE CORREÇÃO DE ERROS DO TIPO CWS

Douglas Frederico Guimarães Santiago

Fevereiro , 2013

Orientador: Renato Portugal, D.Sc

Em um computador quântico, da mesma forma que em um computador clássico, a informação está sujeita a erros que precisam ser detectados e corrigidos, de onde surge a necessidade dos códigos quânticos de correção de erros. Neste trabalho estudamos os códigos CWS (Codeword Stabilized quantum codes) que generalizam os códigos estabilizadores. Primeiramente, descrevemos detalhadamente os códigos CWS sobre sistemas quânticos de mais de um nível (qudits) a partir de uma nova abordagem. Deixamos claro quais resultados valem em geral e quais valem apenas para qubits, qupits (sistemas com número primo de níveis) e quais valem no caso do código CWS ser baseado em um *estado-grafo*. Apresentamos também um novo resultado que relaciona códigos CWS com códigos estabilizadores generalizando os resultados presentes na literatura. Posteriormente, caracterizamos um tipo de operador de medida para códigos CWS para qubits. Criamos então um procedimento para buscar estes operadores, que nem sempre são suficientes para identificar o erro ocorrido, mas quando são, o fazem de forma eficiente.

Abstract of Thesis presented to LNCC/MCT as a partial fulfillment of the requirements for the degree of Doctor of Sciences (D.Sc.)

CWS QUANTUM ERROR CORRECTING CODES

Douglas Frederico Guimarães Santiago

February, 2013

Advisor: Renato Portugal, D.Sc

Like a classical computer, a quantum computer would be affected by errors. Those need to be identified and corrected, so we need quantum error correcting codes. In this work, we study the Codeword Stabilized Quantum Codes (CWS codes) a generalization of the stabilizers quantum codes. First, we make a detailed description, with a new approach of the results about CWS codes on systems with more than one level (qudits). We make clear what results are correct in general and what results are correct only for qubits, qupits (prime number of levels) or what are correct for graph-states. We also show a new result that relates CWS codes with stabilizer codes generalizing the results found in the literature. After that, but only for qubits and CWS codes in a standard form, we also show new results on the kind of observables we may use to identify the errors in a CWS code. We create than a procedure to find these observables. Those observables not always suffices to identify the error, but when they do, the procedure to identify the errors is made in an efficient way.

Sumário

Lista de Figuras

Figura

Lista de Tabelas

Tabela

Lista de Siglas e Abreviaturas

- $|.\rangle$: Ket.
- $\langle.|$: Bra.
- $\mathcal{H}$: Espaço de Hilbert sobre um qubit.
- $\mathcal{H}_d$: Espaço de Hilbert sobre um qudit.
- $\mathcal{H}^n$: Produto tensorial de n espaços de Hilbert $\mathcal{H}$.
- $\mathcal{H}_d^n$: Produto tensorial de n espaços de Hilbert $\mathcal{H}_d^n$.
- $A \backslash B$: Conjunto A menos conjunto B.
- $\mathcal{G}_d^n$: Grupo de Pauli sobre n qudits.
- $\mathcal{C}_d^n$: O grupo de Clifford sobre $\mathcal{G}_d^n$.
- S: Grupo estabilizador.
- $\mathbb{S}$: Conjunto de geradores do grupo estabilizador.
- W: Conjunto de operadores-palavras de um código CWS.
- $|G|$: Ordem de um grupo G.
- $\#C$: Cardinalidade de um conjunto C.
- $H \leq G$: H é subgrugo de G.
- $C_S(C)$: Centralizador do conjunto C no grupo S.
- $N_S(C)$: Normalizador do conjunto C no grupo S.
- q_d: Raiz d-ésima da unidade.
- $\mathbb{Z}_d$: Anel dos inteiros módulo d.
- $\mathbb{F}_d$: Quando d é primo, $\mathbb{Z}_d$ é o corpo $\mathbb{F}_d$.
- $R(P)$: Se P é um operador de Pauli, é a representação em $\mathbb{Z}_d^{2n}$ de P.

- $R(C)$: Se C é um conjunto de operadores de Pauli, é a Matriz Verificadora sobre um conjunto C.
- $\langle C \rangle$: Se C é um conjunto de operadores de Pauli, é o grupo gerado por C.
- $\langle C' \rangle$: Se C' é uma matriz com entradas em $\mathbb{Z}_d$ é o $\mathbb{Z}_d$-módulo gerado pelas linhas de C'.
- $Im(C')$: Se C' é uma matriz com entradas em $\mathbb{Z}_d$ é o $\mathbb{Z}_d$-módulo gerado pelas colunas de C'.
- $Ker(C')$: Se C' é uma matriz com entradas em $\mathbb{Z}_d$ é o núcleo do homomorfismo entre $\mathbb{Z}_d$-módulos representado pela matriz C'.
- Λ: Matriz de tamanho $2n \times 2n$, $\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, onde 0 e I são respectivamente as matrizes nula e identidade em $n \times n$.
- CZ: Porta Z-controlada.
- CCZ: Porta Z-duplamente controlada.
- Γ: Matriz de Adjacência de um grafo.
- $Cl_S(.)$: Função que transforma operadores de Pauli em palavras clássicas em um código CWS.
- ϵ: Conjunto de erros corrigíveis ou detectáveis de um código quântico.
- $\mathbb{R}[S]$: Álgebra de Grupos gerada pelo grupo S sobre os reais $\mathbb{R}$.

Capítulo 1

Introdução

No final do século XIX, ficou claro que a física previa fenômenos absurdos, como a "catástrofe ultravioleta", envolvendo energias infinitas, ou elétrons espiralando para dentro dos núcleos atômicos (Nielsen e Chuang (2000)). A medida que a compreensão sobre átomos e radiação avançou, estas teorias eram descartadas, e foi surgindo a moderna teoria da mecânica quântica. A mecânica quântica tornou-se indispensável à ciência e tem sido aplicada com sucesso em diversas áreas, desde o estudo do interior do sol, passando pela estrutura dos átomos, pela fusão nuclear, supercondutores, estrutura do DNA, até às estruturas elementares da matéria.

Os efeitos quânticos se tornam mais evidentes no universo do "muito pequeno". Com a miniaturização dos componentes dos computadores, eventualmente efeitos quânticos indesejáveis se tornarão presentes. Na tentativa de usar estes efeitos para fazer uma computação mais eficiente, no final da década de 80, surgem as pesquisas em computação quântica (Benioff (1980), Deutsch (1985) e Feynman (1982)). Estas se desenvolveram e atualmente encontramos vasto material sobre o assunto (Nielsen e Chuang (2000), Kaye et al. (2007), Burda (2005)). Para que a computação quântica seja realmente útil, é preciso desenvolver algoritmos quânticos (Shor (1994), Grover (1996), Mosca (2009) e Childs e van Dam (2010)). Os algoritmos quânticos em geral exibem a grande vantagem de resolver um problema de forma mais rápida que os algoritmos clássicos equivalentes, sendo que alguns chegam a fazê-lo em tempo polinomial enquanto o equivalente clássico o faz em

tempo exponencial.

Com o real desenvolvimento da computação quântica, assim como na computação clássica, o surgimento de mecanismos para detectar e corrigir os eventuais erros devem ser implementados; segue então a necessidade da teoria dos códigos quânticos de correção de erros (Nielsen e Chuang (2000), Knill e Laflamme (1997) Staff (2008), Aharonov e Ben-or (1997), Calderbank e Shor (1996), Bennett et al. (1996) Steane (1996) e Gottesman (1996)). A proteção contra erros quânticos envolve desafios bem diferentes da proteção contra erros clássicos, mas, apesar disso, grande parte da teoria dos códigos clássicos de correção de erros pode ser aproveitada para os códigos quânticos.

Um código quântico é um subespaço de um espaço de Hilbert e costuma ser representado pelos parâmetros $((n, K, e))_d$. O parâmetro d corresponde à quantidade de níveis quânticos sendo considerados, isto é, à quantidade de estados linearmente independentes que um único qudit pode apresentar. O parâmetro n é a dimensão do espaço de Hilbert maior, K é a dimensão do código. O parâmetro e representa a quantidade de qudits que o código pode detectar. Um código de parâmetro e detecta erros em até $e-1$ qudits. Uma forma de se comparar códigos quânticos com parâmetros n e e fixos, é mediante o valor do parâmetro K. Quanto maior o valor de K, melhor o código.

Uma classe de códigos quânticos muito explorada na literatura é a classe dos códigos estabilizadores (Gottesman (1997), Calderbank et al. (1997)). Nestes, o subespaço que define o código é a interseção dos subespaços associados ao autovalor 1 de um conjunto de operadores que forma um subgrupo do grupo de Pauli. Este grupo é chamado de grupo estabilizador S.

Em um código CWS (Codeword Stabilized Quantum Codes) de parâmetros $((n, K, e))_d$, o grupo estabilizador estabiliza um único estado quântico (a menos de multiplicação por constantes) e os elementos da base são construídos aplicando operadores de Pauli distintos (e que satisfazem algumas condições) no estado estabilizado (Chen et al. (2008), Chuang et al. (2009), Cross et al. (2009), Hu et al.

(2008), Yu et al. (2008), Yu et al. (2007) e Yu et al. (2009)). Os códigos CWS são uma generalização dos códigos estabilizadores, pois mostra-se que todo código estabilizador pode ser visto como um código CWS. Reciprocamente, mostra-se que um código CWS satisfazendo certas condições é na verdade um código estabilizador. Há vários resultados na literatura acerca dos códigos CWS e um destes resultados permite, fixados os parâmetros n e e, que o problema de construir bons códigos quânticos CWS (com o parâmetro K grande) se transforme no problema de construir bons códigos clássicos que corrijam um conjunto específico de erros.

A maioria dos trabalhos sobre códigos quânticos exploram a criação de novos códigos e métodos para isto. A própria teoria dos códigos CWS funciona neste sentido, apresentando um método para criar novos códigos quânticos não estabilizadores. Nesta linha também estão os trabalhos envolvendo códigos concatenados (Beigi et al. (2011) e Grassl et al. (2009)).

Dado um código quântico, para se identificar o erro ocorrido, precisamos de um conjunto de operadores de medida que não destruam a informação quântica. Nos códigos estabilizadores, usa-se nesta identificação um conjunto de geradores independentes do grupo estabilizador S, e isto pode ser feito com eficiência. Diferentemente dos códigos estabilizadores, a identificação dos erros em um código quântico geral não é feita de forma eficiente. Apesar de existir um procedimento geral para identificar os erros em um código CWS que apresenta ganho na eficiência (Li et al. (2010) e Melo et al. (2012)), este procedimento continua não sendo eficiente para códigos CWS gerais.

Este trabalho trata dos códigos CWS seguindo a seguinte estrutura. No Capítulo 2 apresentamos as ferramentas necessárias para que se compreenda os códigos CWS, apresentando os postulados da mecânica quântica da forma como é utilizado na computação quântica e apresentando uma introdução aos códigos quânticos de correção de erros. Tal capítulo trata apenas de sistemas de dois níveis (qubits) mas a generalização para sistemas de mais níveis (qudits) é imediata. No caso de códigos CWS binários ($d = 2$), os resultados presentes na literatura

são muito claros, o que não ocorre no caso em que o parâmetro d é genérico, tornando difícil identificar quais resultados são válidos apenas quando d é primo, quais valem quando d não é primo ou quais valem quando o código CWS é tal que o estado estabilizado é um estado-grafo, que representa uma outra possibilidade para códigos CWS. Um dos objetivos do trabalho é deixar isto mais claro. Isto é feito no Capítulo 3. Neste capítulo, também apresentamos o Teorema 10, um resultado novo e geral que auxilia na determinação de quando um código CWS é um código estabilizador. Ainda no Capítulo 3, apresentamos alguns novos códigos, códigos assimétricos, descobertos usando a metodologia fornecida pelos códigos CWS. No Capítulo 4, o trabalho estabelece novos resultados quando $d = 2$ no sentido de achar operadores de medida que possam tornar o processo de identificação do erro mais eficiente (Santiago et al. (2012a) e Santiago et al. (2012b)). Estes resultados culminam com o Teorema 13 e o Corolário 6.

Capítulo 2

Preliminares

Neste capítulo descrevemos o material básico necessário para o entendimento deste trabalho. Na Seção-2.1 descrevemos os postulados da mecânica quântica. Na Seção 2.2 explicamos o que são códigos quânticos de correção de erros. Na Seção 2.3 descrevemos as condições para que um código quântico corrija e detecte um conjunto de erros e na Seção 2.4 descrevemos os códigos quânticos estabilizadores. Decidimos tratar aqui apenas com sistemas quânticos de dois níveis, isto é, sobre qubits. Isto foi feito por considerarmos que, nesta parte do trabalho, a extensão para sistemas de mais níveis (qudits) é imediata.

2.1 Postulados da mecânica quântica

As regras que determinam como funciona a mecânica quântica estão contidas em 4 postulados (Nielsen e Chuang (2000) e Cosme (2008)) O primeiro postulado trata de onde se dá os fenômenos quânticos, o Postulado 2 explica como evolui de um sistema quântico. O Postulado 3 trata da questão da medida em um sistema quântico e o Postulado 4 de sistemas quânticos compostos.

Postulado 1.

A qualquer sistema físico isolado existe associado um espaço vetorial complexo, com produto interno completo (espaço de Hilbert) conhecido como espaço de estados do sistema. O sistema é descrito pelo seu vetor de estado, um vetor unitário no espaço de estados

Este postulado aplicado à computação quântica explica o bit quântico (**qubit**). Um qubit se localiza no espaço de Hilbert de dimensão 2 sobre os complexos, $\mathcal{H}$. Na base computacional pode ser descrito por

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

em que α e *beta* são números complexos e

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ e } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

A notação usada aqui é a notação de Dirac que é a forma como a computação quântica é estudada. O símbolo $|.\rangle$ (lê-se "Ket"), denota um estado quântico, enquanto $\langle .|$ (lê-se "bra") é o transposto conjugado do estado. O produto interno é denotado por $\langle .||.\rangle$. Os estados $|0\rangle$ e $|1\rangle$ denotam a base computacional e são os análogos dos bits 0 e 1 da computação clássica, a diferença é que enquanto na computação clássica só há estas duas possibilidades para um bit, na computação quântica um qubit pode estar simultaneamente no estado $|0\rangle$ e $|1\rangle$, situação representada pela combinação linear dos estados, como descrito acima. Para que o estado seja unitário, $|\psi\rangle$ deve satisfazer e $\langle\psi||\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$.

Uma outra base muito usada para representar o qubit é a base $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, isto é:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ e } |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Postulado 2. *A evolução de um sistema fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ de um sistema em um tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema em t_2 por um operador unitário U que depende somente de t_1 e t_2*

$$|\psi'\rangle = U|\psi\rangle.$$

O postulado como formulado anteriormente trata do caso discreto, que é o caso que lidamos na computação quântica. No caso contínuo, o postulado diz que a evolução temporal do espaço de estados é descrita pela equação de Schrodinger: $ih\frac{d|\psi\rangle}{dt} = H|\psi\rangle$, onde h é uma constante física chamada constante de planck e H é um operador hermitiano conhecido como Hamiltoniano do sistema.

De acordo com este postulado, podemos apresentar algumas portas quânticas mais importantes sobre um qubit. Todas as portas descritas abaixo são transformações unitárias descritas na base computacional. As quatro primeiras são denominadas operadores de Pauli. Todas têm seu correspondente em sistemas generalizados com mais níveis, qudits, como pode ser visto em Hostens et al. (2005). Algumas destas portas generalizadas serão posteriormente descritas neste trabalho, quando isto se tornar necessário.

(1) A transformação Identidade, $I|0\rangle = |0\rangle$ e $I|1\rangle = |1\rangle$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(2) A transformação mudança de bit, $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(3) A transformação mudança de fase, $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(4) A transformação mudança de bit e fase, $Y|0\rangle = i|1\rangle$ e $Y|1\rangle = -i|0\rangle$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

(5) A transformação Hadamard, $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

(6) A transformação Fase, $S|0\rangle = |0\rangle$ e $S|1\rangle = i|1\rangle$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

O próximo postulado descreve as medidas quânticas. Optamos por não enunciar a forma geral do postulado das medidas, mas falar apenas de medidas projetivas que são as medidas que serão utilizadas neste trabalho. Esta opção, de fato, não é restritiva, pois prova-se que realizar medidas projetivas é equivalente a realizar medidas no caso geral, desde que se permita o uso de operadores unitários como no Postulado 2.

Postulado 3. *Uma medida projetiva é descrita por um* ***observável*** M*, um operador no espaço de estados do sistema sendo observado, satisfazendo* $M^2 = I$*. O observável tem uma decomposição espectral*

$$M = \sum_m m P_m$$

em que P_m *é o projetor sobre o auto-espaço de* M *com autovalor* m*. Os possíveis resultados da medida correspondem aos autovalores* m *do observável. Medindo-se o estado* $|\psi\rangle$*, a probabilidade de se obter o resultado* m *é dada por*

$$p(m) = \langle\psi|P_m|\psi\rangle$$

obtido o resultado m*, o estado do sistema logo após a medida será*

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

Neste ponto, é interessante introduzir o conceito de **fase**. Na computação quântica, uma fase é um número complexo γ com norma 1, isto é, $\gamma = e^{i\theta}$. A informação quântica contida em uma fase não é detectável por uma medida. Isto faz com que estados que se diferenciam apenas por uma fase, por exemplo, $|\psi\rangle$ e $\gamma|\psi\rangle$ sejam muitas vezes considerados iguais. Caso se queira dar relevância a esta diferença de fase, muitas vezes é usado o termo "igual a menos de fase".

Exemplo 1. *Considere o observável* $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ *e o estado* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. *Medindo este observável, obtemos uma das duas possibilidades*

(1) $m = 1$ *com probabilidade* $|\alpha|^2$ *e neste caso o estado após a medida será* $|0\rangle$ *(a menos de fase).*

(2) $m = -1$ *com probabilidade* $|\beta|^2$ *e neste caso o estado após a medida será* $|1\rangle$ *(a menos de fase).*

Postulado 4. *O espaço de estados de um sistema composto é o produto tensorial dos estados dos sistemas físicos individuais. Se os sistemas forem numerados de 1 até n, e o sistema i for preparado no estado* $|\psi_i\rangle$*, decorre que o estado do sistema composto será* $|\psi_1\rangle\otimes, \ldots, \otimes|\psi_n\rangle$.

O produto tensorial, identificado pelo símbolo $\otimes$ na verdade é uma forma de se juntar espaços vetoriais para formar um espaço maior. Sejam V e W espaços vetoriais. Por definição, um produto tensorial satisfaz as seguintes propriedades:

(1) Se $z \in \mathbb{C}$, $|v\rangle \in V$ e $|w\rangle \in W$ então:

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$$

(2) Se $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$ então:

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

(3) Se $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$ então:

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |v\rangle + |w_2\rangle \otimes |w_1\rangle$$

As vezes, omite-se o símbolo $\otimes$, escrevendo apenas $|v\rangle|w\rangle$ ou ainda $|vw\rangle$.

Exemplo 2. *Um sistema quântico de dois qubits é modelado em um espaço de Hilbert complexo de dimensão 4, $\mathcal{H}^{\otimes 2}$, com base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. isto é, cada elemento se escreve como*

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle.$$

Uma característica interessante dos sistemas compostos é a existência de estados emaranhados, isto é, estados que não podem ser escritos como o produto tensorial outros estados, por exemplo, o estado $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ pode ser escrito como $|\psi\rangle = |0\rangle \otimes (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))$ portanto não é um estado emaranhado, já o estado $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ é um estado emaranhado, pois facilmente verificamos que este não pode ser escrito como produto tensorial de dois estados.

Uma representação concreta do produto tensorial é o produto de **Kronecker**. O produto de Kronecker se define sobre matrizes, e portanto serve também para vetores. Seja A uma matriz $m \times n$ e B uma matriz $p \times q$, o produto de kronecker $A \otimes B$ é uma matriz de tamanho $mp \times nq$ dada por:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}.$$

2.2 Códigos quânticos de correção de erros

O procedimento de codificação, detecção e correção de erros quânticos apresenta grandes diferenças em relação ao dos códigos clássicos, mas possuem tam-

bém algumas semelhanças. O principal objetivo desta seção é descrever os códigos quânticos, as ideias em que se baseiam e como funcionam os procedimentos anteriormente citados. Com este objetivo, primeiramente descrevemos brevemente os códigos clássicos, para depois fazer uma comparação com os códigos quânticos.

Em linhas gerais, um código clássico se baseia no seguinte procedimento

(1) A informação é codificada, gerando uma redundância.

(2) A informação codificada passa por um canal ruidoso, onde podem ocorrer erros.

(3) Após a passagem pelo canal ruidoso, analisa-se a informação procurando identificar qual erro ocorreu e corrigir.

Como exemplo de código clássico, considere o código de repetição contendo duas palavras-código $C = \{(0,0,0),(1,1,1)\}$. Uma função codificadora para este código é:

$$(0) \mapsto (0,0,0)$$
$$(1) \mapsto (1,1,1)$$

suponha então que enviamos por um canal ruidoso a palavra-código $(0,0,0)$ e após a passagem por este canal, obtemos $(1,0,0)$. Como $(1,0,0)$ não é uma palavra do código, sabemos que ocorreu um erro. Se o canal ruidoso só admite erros em 1 bit, sabemos que o erro foi no primeiro bit e portanto corrigimos o erro.

Com este exemplo trivial vimos então que a correção clássica de erros, ocorre mediante a geração de uma redundância, criando um código que pode ser afetado por erros clássicos que são basicamente erros de troca de bits, e depois a informação contendo erros será decodificada, para que se recupere a informação inicial. Na computação quântica, temos os seguintes problemas:

(1) **Teorema da não-clonagem**. A geração simples de redundância como é

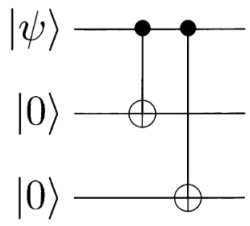
feito na correção clássica não é possível, pois estados quânticos gerais não podem ser duplicados.

(2) **Continuidade dos erros**. Na correção clássica, há apenas erros de inversão de bit, enquanto na correção quântica podem ocorrer uma infinidade contínua de erros distintos.

(3) **Medidas destroem a informação quântica**. Na correção clássica, após a passagem pelo canal ruidoso, temos que observar (medir) a informação. Na correção quântica, medir a informação geralmente destrói a informação, o que torna a recuperação impossível.

Ocorre que apesar destas três grandes dificuldades apresentadas, a correção quântica de erros ainda é possível. Para exemplificar como isto pode ser feito, vamos considerar primeiro um dos códigos quânticos mais simples, o código de três bits para mudança de bits. O Teorema da não clonagem diz que não é possível, a partir de um estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, produzir um estado $|\psi\rangle \otimes |\psi\rangle$, mas podemos por exemplo, a partir do estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ construir, usando portas unitárias, o estado $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$. Isto é feito pelo circuito da Figura 2.1.

Figura 2.1: Circuito Codificador do Código de três bits para mudança de bit



Ocorre que este código, que chamaremos aqui de $\mathcal{Q}$, corrige erros de mudança de bits em até 1 qubit. $\mathcal{Q}$ é um subespaço de dimensão 2 do espaço de Hilbert $\mathcal{H}^{\otimes 3}$ de dimensão 8. A ação dos erros de mudança de bit sobre 1 qubit, envia a informação para subespaços ortogonais a $\mathcal{Q}$, de acordo com a Tabela 2.1

Após a passagem pelo canal ruidoso deve-se tentar descobrir de alguma forma, os possíveis erros que possam ter ocorrido. Para isto devemos efetuar me-

Tabela 2.1: Efeito dos erros em 1 qubit para o código de três bits para mudança de bits

Ausência de erros	$\alpha\|000\rangle + \beta\|111\rangle$
Mudança no primeiro qubit	$\alpha\|100\rangle + \beta\|011\rangle$
Mudança no segundo qubit	$\alpha\|010\rangle + \beta\|101\rangle$
Mudança no terceiro qubit	$\alpha\|001\rangle + \beta\|110\rangle$

didas quânticas, mas sem destruir a informação, para que possamos recuperá-la. Neste exemplo, com medidas consecutivas com os observáveis, ZZI e IZZ, conseguimos deduzir qual o erro de mudança de bit ocorreu, pois se o valor da medida com o observável ZZI é 1, resulta que os estados possíveis são: Ausência de erros ou mudança de bit no terceiro qubit enquanto se o valor da medida é -1, as possibilidades são: mudança no primeiro qubit ou mudança no segundo qubit. Se o valor da medida com o observável IZZ é 1, as possibilidades são: Ausência de erros ou mudança de bit no primeiro qubit, se for -1, as possibilidades são: Mudança de bit no segundo ou no terceiro qubit. Portanto estas medidas combinadas são suficientes para se descobrir o erro.

O código anterior exemplifica como a metodologia dos códigos quânticos pode ser bem parecida com a dos códigos clássicos, gerando primeiro uma redundância para proteger a informação e, após a passagem pelo canal ruidoso, fazendo medidas que não alterem a informação de forma a tentar descobrir o erro ocorrido. O que o exemplo anterior não trata é da questão da continuidade dos erros quânticos, já que o código apenas corrige, de forma análoga aos códigos clássicos, erros discretos de mudança de bit. Um código que exemplifica de maneira eficaz a questão da continuidade de erros é o código de Shor. Este código codifica 1 qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ no estado $|\theta\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. Em cada elemento da base a codificação é feita da seguinte forma

$$|0\rangle \mapsto |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$|1\rangle \mapsto |1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

Este código corrige erros quaisquer desde que em apenas um qubit. Ocorre que qualquer operador de erro E_i agindo no qubit i, pode ser escrito como combinação linear dos operadores de Pauli I, X_i, Y_i e Z_i, por exemplo

$$E_1 = \alpha_1 I + \alpha_2 X_1 + \alpha_3 Y_1 + \alpha_4 Z_1$$

logo

$$E_1|\theta\rangle = \alpha_1 I|\theta\rangle + \alpha_2 X_1|\theta\rangle + \alpha_3 Y_1|\theta\rangle + \alpha_4 Z_1|\theta\rangle$$

para descobrir o erro, podemos medir com os observáveis da Tabela 2.2. Estes observáveis tem uma característica importante. Todos estabilizam o código, isto significa que qualquer informação codificada está no subespaço associado ao autovalor 1 de cada um dos observáveis. Portanto se a informação não sofreu erros, medindo qualquer um deles, o resultado será 1 com probabilidade 1 e a informação não será perdida.

Tabela 2.2: Observáveis de medida para o código de Shor

Z_1Z_2
Z_2Z_3
Z_4Z_5
Z_5Z_6
Z_7Z_8
Z_8Z_9
$X_1X_2X_3X_4X_5X_6$
$X_4X_5X_6X_7X_8X_9$

Suponha então que o erro E_1 descrito acima ocorreu. Como os observáveis estabilizam o código e o erro foi no primeiro qubit, tirando os observáveis Z_1Z_2 e $X_1X_2X_3X_4X_5X_6$, todos os outros comutam com I, X_1, Y_1 e Z_1, logo $E_1|\theta\rangle$ é estabilizado por estes observáveis, o que significa que para estes, a medida será 1 com probabilidade 1 e a informação não será perdida. Em geral, ocorre que se um observável estabiliza o código e anti-comuta com um erro, significa que sob a ação deste erro o estado está completamente no auto-espaço associado ao autovalor -1 do observável, portanto o resultado da medida será -1 com probabilidade 1 e se o

observável comuta com o erro, o resultado será 1 com probabilidade 1.

Medindo consecutivamente os observáveis Z_1Z_2 e $X_1X_2X_3X_4X_5X_6$, as possibilidades são:

(1) Resultado 1 e 1: Dentre os operadores I, X_1, Y_1 e Z_1, o único que comuta com ambos os observáveis Z_1Z_2 e $X_1X_2X_3X_4X_5X_6$ é a identidade; logo após este resultado de medida o estado será $|\theta\rangle$ e não há o que corrigir;

(2) Resultado 1 e -1: Dentre os operadores I, X_1, Y_1 e Z_1, o único que comuta com Z_1Z_2 e anti-comuta com $X_1X_2X_3X_4X_5X_6$ é Z_1; logo após este resultado de medida o estado será $Z_1|\theta\rangle$, e aplicamos Z_1 para corrigir o estado [1] ;

(3) Resultado -1 e 1: Dentre os operadores I, X_1, Y_1 e Z_1, o único que anti-comuta com Z_1Z_2 e comuta com $X_1X_2X_3X_4X_5X_6$ é X_1, logo após este resultado de medida o estado será $X_1|\theta\rangle$, e aplicamos X_1 para corrigir o estado;

(4) Resultado -1 e -1: Dentre os operadores I, X_1, Y_1 e Z_1, o único que anti-comuta com Z_1Z_2 e anti-comuta com $X_1X_2X_3X_4X_5X_6$ é Y_1, logo após este resultado de medida o estado será $Y_1|\theta\rangle$, e aplicamos Y_1 para corrigir o estado.

O exemplo acima representa bem a forma como um código quântico pode proteger a informação mesmo tendo em vista a existência de uma infinidade contínua de erros.

Um canal ruidoso possui um conjunto de elementos de operação, $\epsilon = \{E_i\}$ que representam os erros possíveis de ocorrer neste canal. Um Teorema que é bem conhecido na literatura (Nielsen e Chuang (2000)) é o Teorema da discretização do erro, dado a seguir:

[1] Com este resultado de medida, uma outra possibilidade seria $Z_2|\theta\rangle$ mas o efeito de Z_1 sobre o código é o mesmo de Z_2, donde conseguiríamos corrigir o erro da mesma forma

Teorema 1. *Seja C um código quântico e $\mathcal{R}$ a operação de correção de erros para recuperação de um processo de ruído ϵ com elementos de operação $\{E_i\}$. Seja $\mathcal{F}$ uma operação quântica com elementos de operação F_j que são combinações lineares dos elementos E_i. Resulta que a operação de erro $\mathcal{R}$ também corrige os efeitos do processo de ruído $\mathcal{F}$ sobre o código C*

Como os operadores de Pauli sobre o espaço de Hilbert $\mathcal{H}^{\otimes n}$ formam uma base para todos os operadores de erro possíveis, o Teorema anterior sugere que é interessante escolher nosso conjunto de erros $\epsilon = \{E_i\}$ em que E_i são operadores de Pauli. Daqui para a frente suporemos que esta condição seja sempre satisfeita.

2.3 Condições de correção de erros

Dado um conjunto de erros $\epsilon = \{E_i\}$, e um código C, as condições que garantem que o código corrija estes erros foram deduzidas por Knill e Laflamme (1997).

Teorema 2. *Considere um conjunto de erros $\epsilon = \{E_a\}$ e uma base ortogonal $\{|i\rangle\}$ para um código $\mathcal{Q}$. O código $\mathcal{Q}$ corrige erros em ϵ, se e somente se*

$$\langle i|E_a^\dagger E_b|j\rangle = C_{a,b}\delta_{ij}$$

para todo $E_a, E_b \in \epsilon$ e $|k\rangle, |j\rangle \in \{|i\rangle\}$ em que $C_{a,b}$ é uma constante que só depende dos erros.

Este Teorema significa basicamente que erros atuando em diferentes elementos da base tem que mandar estes para espaços ortogonais, caso contrário, não haveria como distinguir a informação posterior à passagem pelo canal ruidoso. Além disto, dois erros distintos atuando no mesmo elemento da base não precisam enviar tais elementos para espaços ortogonais, mas precisam atuar de forma semelhante, de forma que na correção, independentemente de qual erro ocorreu, E_a ou E_b, seja possível recuperar a informação aplicando quaisquer um dos operadores $E_a^\dagger$ ou $E_b^\dagger$.

Nos códigos CWS, em geral, se lida com condições que garantam que um código detecte um conjunto de erros dados, por isto, decorre do Teorema 2 o seguinte resultado:

Teorema 3. *Considere um conjunto de erros* $\epsilon = \{E_a\}$ *e uma base ortogonal* $\{|i\rangle\}$ *para um código* $\mathcal{Q}$*. O código* $\mathcal{Q}$ *detecta erros em* ϵ *se, e somente se*

$$\langle i|E_a|j\rangle = C_a\delta_{ij}$$

para todo $E_a \in \epsilon$ *e* $|k\rangle, |j\rangle \in \{|i\rangle\}$ *em que* C_a *é uma constante que só depende do erro.*

Destes dois Teoremas, fica claro que se um código $\mathcal{Q}$ corrige erros em um conjunto $\epsilon = \{E_a\}$ então o código $\mathcal{Q}$ detecta erros no conjunto $\epsilon' = \{E_a^\dagger E_b\}$, onde $E_a, E_b \in \epsilon$. Também fica claro que se um código detecta erros em até γ qubits, então ele corrige erros em até $\frac{\gamma}{2}$ qubits, se γ é par e em até $\frac{\gamma-1}{2}$ qubits se γ é ímpar.

2.4 Códigos estabilizadores

Uma classe importante de códigos quânticos são os códigos estabilizadores. Estes códigos foram primeiramente descritos em Gottesman (1997) e sua teoria se encontra bem resumida em Nielsen e Chuang (2000). O formalismo dos códigos estabilizadores se aplica tanto em sistemas de dois níveis (qubits) quanto a sistemas de mais níveis (qudits). As ideias para sistemas de mais níveis são uma generalização do caso de dois níveis (Ketkar et al. (2006)). Nesta parte do trabalho explicamos apenas o formalismo sobre qubits. Tratamos no Capítulo 3 do caso de mais de dois níveis apenas o necessário para descrever os códigos CWS, que representam a parte principal deste trabalho.

Um código quântico sobre o espaço de Hilbert $\mathcal{H}^{\otimes n}$ nada mais é do que um subespaço $\mathcal{Q}$ de $\mathcal{H}^{\otimes n}$. Nos códigos estabilizadores, este subespaço é a interseção dos auto-espaços associados ao autovalor 1 de um grupo estabilizador S, cujos elementos são operadores de Pauli. Para um qubit, consideramos o grupo de Pauli

como sendo o conjunto

$$\mathcal{G}^n(\text{ ou } \mathcal{G}_2^1) = \{I, -I, Z, -Z, X, -X, ZX, -ZX\}.$$

Para vários qubits, consideramos o grupo $\mathcal{G}_2^n$ formado pelo produto tensorial dos operadores em $\mathcal{G}^n$.

Exemplo 3. *É fácil verificar que o código de Shor $\mathcal{Q}$, representado pelos estados $\alpha|0_L\rangle + \beta|1_L\rangle$ onde*

$$\begin{aligned}|0_L\rangle =&|0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}\\ |1_L\rangle =&|1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}\end{aligned}$$

é estabilizado pelo subgrupo abeliano $S \leq \mathcal{G}^n$ cujos elementos são exatamente os observáveis de medida apresentados em 2.2.

O tamanho do subgrupo estabilizador tem relação com a dimensão do código estabilizador. Esta relação se dá através de um resultado que será demonstrado posteriormente de forma geral e portanto não será demonstrado aqui.

Proposição 1. *Seja $S = \langle g_1, \ldots, g_{n-k}\rangle$ gerado por $n-k$ elementos independentes e que comutam de $\mathcal{G}^n$, e suponha que $-I \notin S$. Resulta que o espaço $\mathcal{Q}$ estabilizado por S possui dimensão 2^k*

Além de descrever subespaços vetoriais, podemos utilizar o formalismo dos estabilizadores para descrever a evolução desses subespaços. Suponha que uma operação unitária U atue sobre um subespaço $\mathcal{Q}$ estabilizado por S e seja $|\psi\rangle$ um elemento de $\mathcal{Q}$. Segue-se que para qualquer $g \in S$

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle,$$

isto é, o estado $U|\psi\rangle$ é estabilizado por $UgU^\dagger$. Temos então que o subespaço $U\mathcal{Q}$ é estabilizado por $USU^\dagger = \{UgU^\dagger | g \in S\}$ e se $\{g_i\}$ gera S então $\{Ug_iU^\dagger\}$ gera

$USU^\dagger$.

Uma grande vantagem do formalismo dos estabilizadores é fornecer um meio mais compacto de descrever um sistema quântico e sua evolução. O estado $|0\rangle^{\otimes n}$ por exemplo é o estado estabilizado por $Z^{\otimes n}$. Aplicando a porta Hadamard em cada qubit $H^{\otimes n}$, temos o estado $|+\rangle^{\otimes n}$, que é o estado estabilizado por

$$(H^{\otimes n})Z^{\otimes n}(H^{\otimes n})^\dagger = X^{\otimes n}.$$

Em geral, para descrever um estado de n qubits, precisamos de 2^n amplitudes, mas de acordo com o formalismo dos estabilizadores o estado $|+\rangle^{\otimes n}$ pode ser descrito por n operadores, $\{X_1, \ldots, X_n\}$. Esta forma mais compacta de descrever um estado e sua evolução é uma propriedade interessante dentro deste formalismo.

Seguindo as ideias presentes no formalismo dos estabilizadores, a evolução de um estado quântico estabilizado por operadores de Pauli é descrita por uma operação de conjugação, é interessante então definir e tentar caracterizar quais operadores agem por conjugação sobre operadores de Pauli de forma que o resultado desta ação continue sendo um operador de Pauli.

Definição 1. *O* ***grupo de Clifford*** *sobre n qudits, denotado por $\mathcal{C}_d^n$ é o grupo normalizador de $\mathcal{G}_d^n$ em $U(d^n)$, isto é, o grupo das matrizes unitárias U de dimensão d^n que satisfazem $U\mathcal{G}_n^d U^\dagger = \mathcal{G}_d^n$. O* ***grupo local de Clifford****, denotado por $\mathcal{LC}_d^n$, é o subgrupo de $\mathcal{C}_d^n$ consistindo de elementos que são descritos como o produto tensorial de n elementos de $\mathcal{C}_d^1$.*

Ocorre que para *qubits* o grupo de Clifford $\mathcal{C}_2^n$, além de conter elementos de $\mathcal{G}_2^n$ é gerado pelas portas Hadamard, Fase e Não-controlado. A ação destas portas sobre os elementos de $\mathcal{G}_2^n$ é dada pela Tabela 2.3.

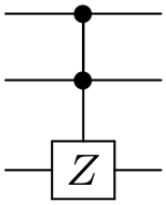
Uma porta importante para os códigos CWS é a porta Z-duplamente controlada, que denotaremos por CCZ (Figura 2.2). Esta porta não pertence a $\mathcal{C}_2^n$ e está presente na codificação dos códigos CWS.

A ação da porta CCZ sobre os operadores de Pauli pode ser deduzida das

Tabela 2.3: Ação dos geradores do grupo de Clifford $\mathcal{C}_2^n$ sobre os operadores de Pauli

Operação	Entrada	Saída
Não-controlado	X_1	X_1X_2
	X_2	X_2
	Z_1	Z_1
	Z_2	Z_1Z_2
H	X	Z
	Z	X
S	X	Y
	Z	Z
X	X	X
	Z	$-Z$
Y	X	$-X$
	Z	$-Z$
Z	X	$-X$
	Z	Z

Figura 2.2: Porta Z duplamente controlada (CCZ)



relações na Tabela 2.4

Tabela 2.4: Ação da porta CCZ sobre os operadores de Pauli

Operação	Entrada	Saída
CCZ	Z_1	Z_1
	Z_2	Z_2
	Z_3	Z_3
	X_1	$X_1 \otimes \frac{I+Z_2+Z_3-Z_2Z_3}{2}$
	X_2	$X_2 \otimes \frac{I+Z_1+Z_3-Z_1Z_3}{2}$
	X_3	$X_1 \otimes \frac{I+Z_1+Z_2-Z_1Z_2}{2}$

Medidas quânticas também podem ser descritas usando o formalismo dos estabilizadores, mas esta descrição não será necessária neste trabalho.

Capítulo 3

Códigos CWS

Neste capítulo estudamos os códigos **CWS** (Codeword Stabilized Quantum Codes). Os códigos CWS podem ser tratados em seu formato mais simples, o binário, quando se lida com qubits, ou ainda em formatos mais gerais, quando se lida com qupits (sistema quânticos com número primo de níveis) ou qudits (sistemas quânticos com número qualquer de níveis). Além disso, podemos estudar os códigos CWS em seu formato de ***estados-grafos***. Embora grande parte dos resultados obtidos neste trabalho estar relacionado aos códigos CWS binários, optamos tratar o caso mais geral, isto é, trabalhando com qudits e, quando necessário, particularizaremos os resultados para o caso binário. Desta decisão de tratar os códigos CWS de forma geral, surgiram novas demonstrações de alguns resultados não facilmente encontrados e não claros na literatura. Conseguimos diferenciar claramente quando um resultado é válido em um formato mas porém não é válido em outro, tornando claro quais resultados são válidos considerando estas diversas formas de tratar os códigos CWS.

A maior novidade deste capítulo quando comparado com os resultados sobre códigos CWS contidos na literatura consiste na forma de alguns destes resultados foram demonstrados. Para isto, utilizamos uma generalização do conceito de matriz verificadora, usada nos códigos estabilizadores (Nielsen e Chuang (2000)). Esta matriz e sua interpretação como uma transformação linear entre espaços vetoriais permite a demonstração de alguns resultados quando estamos lidando com qubits

ou qupits. No caso geral, sobre qudits, a matriz verificadora representa um homomorfismo de $\mathbb{Z}_d$-módulos. Usamos esta estrutura para refazer algumas demonstrações de resultados já existentes. Incluindo um novo resultado (Teorema 10) que generaliza resultados existentes na literatura.

Um código quântico é um subespaço de um espaço de Hilbert $\mathcal{H}_d^n$. Este subespaço pode ser construído de diversas formas. Nos códigos estabilizadores, um código de parâmetros $[[n, k]]_d$ é construído por meio de um subgrupo abeliano do grupo de Pauli $\mathcal{G}_n^d$. Neste caso, o código é então a interseção dos subespaços de $\mathcal{H}_d^n$ associados ao autovalor 1 de todos os geradores deste subgrupo.

Os códigos CWS surgiram nos trabalhos de Smolin et al. (2007); Yu et al. (2008); Cross et al. (2009); Chen et al. (2008); Chuang et al. (2009); Hu et al. (2008) e representam uma extensão natural desta estrutura estabilizadora, no caso dos códigos CWS o grupo estabilizador, que chamaremos de S, estabiliza, a menos de uma fase, apenas um estado $|\psi\rangle$. Os outros estados de uma base associada ao subespaço que representa o código são obtidos por meio de K operadores de Pauli, $\{W_i\}$, chamados de *operadores-palavras* (Codewords Operators), formando K estados linearmente independentes que chamaremos de *palavras* (Codewords) $\mathcal{B} = \{W_1|\psi\rangle, \ldots, W_K|\psi\rangle\}$.

Na primeira seção, explicamos em mais detalhes a estrutura dos códigos CWS, baseado principalmente em Chen et al. (2008). Nesta seção, introduzimos a noção de matriz verificadora. Na segunda seção, apresentamos uma forma particular de estudar os códigos CWS, por meio de *estados-grafos*. Para d primo, mostraremos que todo código CWS é, de fato, equivalente a um código CWS derivado de *estados-grafos*. Na terceira seção, demonstramos o que talvez seja o teorema principal relacionado aos códigos CWS, que permite relacionar estes com códigos clássicos. Na quarta seção, fazemos uma relação entre códigos quânticos estabilizadores e códigos CWS e introduzimos um novo teorema (Teorema 10). Os Corolários 4 e 5 relativos a este teorema representam resultados bem conhecidos na literatura, apesar de não termos encontrado uma demonstração sobre qudits

para tais resultados. Na quinta seção, explicamos como reduzir o problema de achar bons códigos CWS ao problema de achar bons códigos clássicos que corrijam um certo conjunto de erros, apresentando algoritmos para isto. Esta redução se baseia em Chuang et al. (2009). Nesta referência os algoritmos estão apenas sobre qubits; generalizamos tais algoritmos para qudits. Na sexta seção explicamos o que são códigos assimétricos e utilizamos os algoritmos da seção anterior sobre estes, descobrindo, assim, novos códigos assimétricos com bons parâmetros.

3.1 Estrutura dos códigos CWS

Para um qudit, o grupo de Pauli $\mathcal{G}_d^1$ é gerado por X, Z, em que a relação de comutação é dada por

$$ZX = q_d XZ$$

onde $q_d = e^{i\frac{2\pi}{d}}$. Repare que definindo desta forma, para um qubit ($d = 2$) o grupo de Pauli $\mathcal{G}_2^1$, que no caso binário também vamos representar por $\mathcal{G}$, é dado por

$$\mathcal{G}_2^1 = \{I, -I, Z, -Z, X, -X, ZX, -ZX\}.$$

Existe uma representação de $\mathcal{G}_d^1$ e uma base $\{|k\rangle\}_{k=0}^{d-1}$ tal que

$$Z|k\rangle = q_d^k|k\rangle, \quad X|k\rangle = |k+1\rangle, \text{para todo } k \in Z_d.$$

Por exemplo, para $d = 4$ e $q_d = i$, temos a representação

$$Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix} \quad X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

e

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |3\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Segue que $Z^j X^k = q_d^{jk} X^k Z^j$ e a relação geral de comutatividade (Ketkar et al. (2006)) é dada por

$$(q_d^{i_1} Z^{j_1} X^{k_1})(q_d^{i_2} Z^{j_2} X^{k_2}) = q_d^{j_1 k_2 - k_1 j_2} (q_d^{i_2} Z^{j_2} X^{k_2})(q_d^{i_1} Z^{j_1} X^{k_1}). \tag{3.1}$$

Ainda considerando estas relações de comutação, temos que um elemento do grupo de Pauli $\mathcal{G}_d^n = \underbrace{\mathcal{G}_d^1}_{1} \otimes \ldots, \otimes \underbrace{\mathcal{G}_d^1}_{n}$ pode ser escrito como

$$\alpha Z^{\mathbf{V}} X^{\mathbf{U}}$$

em que $\alpha = q_d^k$ e $\mathbf{V}$ e $\mathbf{U}$ representam vetores em $\mathbb{Z}_d^n$ indicando a potência de Z e X em cada qudit respectivamente. Estendendo a relação de comutação 3.1, temos

$$(Z^{\mathbf{U}_1} X^{\mathbf{U}_2})(Z^{\mathbf{V}_1} X^{\mathbf{V}_2}) = q_d^{\langle \mathbf{U}_1, \mathbf{V}_2 \rangle - \langle \mathbf{U}_2, \mathbf{V}_1 \rangle} (Z^{\mathbf{V}_1} X^{\mathbf{V}_2})(Z^{\mathbf{U}_1} X^{\mathbf{U}_2}) \tag{3.2}$$

em que $\langle ., . \rangle$ denota o produto interno canônico restrito à $\mathbb{Z}_d^n$, que não é necessariamente um espaço vetorial (se d for primo Z_d^n é espaço vetorial, pois, neste caso, Z_d é corpo). Isto só ocorre se d for primo.

Podemos representar a menos de fase, um operador de Pauli $E = \alpha Z^{\mathbf{U}_1} X^{\mathbf{U}_2}$ em $\mathcal{G}_n^d$ por um vetor expandido em $\mathbb{Z}_d^{2n}$. Isto é feito por meio da aplicação R definida a seguir:

Definição 2. *Considere $\mathcal{G}_d^n$ o grupo de Pauli de n entradas sobre qudits e o $\mathbb{Z}_d$-*

módulo $\mathbb{Z}_d^{2n}$. *A aplicação* R *é definida por*

$$R : \mathcal{G}_d^n \to \mathbb{Z}_d^{2n}$$
$$\alpha Z^{\mathbf{U}_1} X^{\mathbf{U}_2} \mapsto (\mathbf{U}_1|\mathbf{U}_2).$$

Claramente a função R está bem definida, é sobrejetiva, mas não é injetiva, pois a informação contida na fase α é perdida. Utilizando a representação dos elementos de $\mathcal{G}_d^n$ dado pela função R, podemos representar a fase que aparece na relação de comutação geral (3.2) por meio do operador de dimensão $2n \times 2n$ definido por

$$\Lambda = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}, \tag{3.3}$$

em que 0 e I se referem à submatrizes nula e identidade, respectivamente, de dimensão $n \times n$. Utilizando este operador, notamos que para quaisquer dois operadores de Pauli P_1 e P_2 obedecem a relação de comutação

$$P_1 P_2 = q_d^{R(P_1)\Lambda R^T(P_2)} P_2 P_1.^1 \tag{3.4}$$

A operação $R(P_1)\Lambda R^T(P_2)$ que aparece na equação 3.4 tem importância fundamental não somente para o entendimento do processo que permitirá futuramente, neste trabalho, transformar o problema de achar bons códigos quânticos CWS no problema de achar bons códigos clássicos, mas também na confecção de várias demonstrações apresentadas neste trabalho de tese. Esta operação é conhecida como produto simplético (Ketkar et al. (2006)).

Com o que foi discutido até então, podemos, de acordo com Chen et al. (2008), definir um código CWS não binário por meio de dois conjuntos:

(1) Um grupo abeliano $S = \langle s_1, \ldots, s_r \rangle$ de ordem $|S| = d^n$ e que não contém múltiplos da identidade com exceção da identidade propriamente dita (Ve-

[1] $R(P)$ está sendo considerado como um vetor linha enquanto $R^T(P)$ é a transposta do vetor.

remos que este grupo estabiliza, a menos de uma fase, um único estado $|\psi\rangle \in \mathcal{H}_d^n$);

(2) Um conjunto $W = \{w_i\}_{i=1}^K$ em que $\{w_i\}$ são operadores de Pauli e $\beta = \{w_i|\psi\rangle\}$ representando a base do código.

A exigência do grupo S ser abeliano e não conter múltiplos da identidade além dela própria vem do fato de que, se assim não fosse, o único estado estabilizado por S seria o vetor nulo, pois:

(1) Se S não é abeliano e $|\psi\rangle$ é um estado estabilizado, existem g_1, $g_2 \in S$ e $q_d^k \neq 1$ tal que:

$$|\psi\rangle = g_1 g_2 |\psi\rangle = q_d^k g_2 g_1 |\psi\rangle = q_d^k |\psi\rangle,$$

e assim, $|\psi\rangle$ só pode ser o vetor nulo.

(2) Se existe um múltiplo da identidade que não a própria em S, digamos $q_d^k I$, com $q_d^k \neq 1$, então da mesma forma:

$$|\psi\rangle = q_d^k I |\psi\rangle = q_d^k |\psi\rangle,$$

donde conclui-se da mesma forma que $|\psi\rangle$ só pode ser o vetor nulo.

Além disto, pode-se verificar que estas condições garantem que todos os operadores de S sejam simultaneamente diagonalizáveis, isto é, existe uma base de autovetores comum a todos os operadores de S. Se a ordem de $|S|$ é d^n, veremos que o espaço estabilizado por S tem dimensão 1. Se $|S| < d^n$, verificaremos que S estabiliza um espaço de dimensão maior que 1. Independentemente de S estabilizar um único estado ou não, vamos chamar este grupo de grupo estabilizador.

Para facilitar o entendimento, como exemplo de estabilizador e estado estabilizado, considere n=1, d=6, $S = \langle X^3, Z^2 \rangle$ e $|\psi\rangle = \dfrac{|0\rangle + |3\rangle}{\sqrt{2}}$. S estabiliza $|\psi\rangle$,

pois:

$$X^3|\psi\rangle = \frac{X^3|0\rangle + X^3|3\rangle}{\sqrt{2}} = \frac{|3\rangle + |0\rangle}{\sqrt{2}} = |\psi\rangle$$

e

$$Z^2|\psi\rangle = \frac{Z^2|0\rangle + Z^2|3\rangle}{\sqrt{2}} = \frac{(q_6)^0|2\rangle + (q_6)^6|0\rangle}{\sqrt{2}} = |\psi\rangle$$

Como exemplo mais completo, podemos considerar o código CWS de parâmetros $((5,4))_4$, apresentado em Hu et al. (2008). Este código é baseado em um grupo estabilizador S com os seguintes geradores:

$$s_1 = XZIIZ \quad s_2 = ZXZII \quad s_3 = IZXZI \quad s_4 = IIZXZ \quad s_5 = ZIIZX.$$

Para caracterizar completamente o código, temos que informar os *operadores-palavras*, que neste exemplo são 4: $w_1 = Z^{\mathbf{V}_{R_1}} X^{\mathbf{U}_{R_1}}$, $w_2 = Z^{\mathbf{V}_{R_2}} X^{\mathbf{U}_{R_2}}$, $w_3 = Z^{\mathbf{V}_{R_3}} X^{\mathbf{U}_{R_3}}$ e $w_4 = Z^{\mathbf{V}_{R_4}} X^{\mathbf{U}_{R_4}}$ em que $\mathbf{U}_{R_i} = (0,0,0,0,0)\,\forall i$ e:

$$\mathbf{V}_{R_1} = (0,0,0,0,0) \quad \mathbf{V}_{R_2} = (1,1,1,1,1) \quad \mathbf{V}_{R_3} = (2,3,3,2,3) \quad \mathbf{V}_{R_4} = (3,2,2,3,2)\ .$$

Este código corrige erros de Pauli E de peso 1 ($wt(E) = 1$). Para verificar porque isto ocorre precisamos adentrar mais na teoria dos códigos CWS.

Já vimos que podemos utilizar a a aplicação $R(E)$ para representar operadores de Pauli segundo palavras clássicas em $\mathbb{Z}_d^{2n}$. Da mesma forma podemos representar uma coleção de operadores de Pauli através de uma matriz. Aproveitando a terminologia dos códigos clássicos de correção de erros (MacWilliams e Sloane (1977), Vermani (1996)), denominaremos esta matriz por *matriz verificadora*. Esta terminologia já é usada no formalismo dos códigos estabilizadores (Nielsen e Chuang (2000)) apenas usando os geradores do grupo estabilizador, mas a definiremos aqui de forma geral, para qualquer conjunto de operadores de Pauli.

Definição 3. *Dada uma coleção de operadores de Pauli* $\mathcal{C} = \{p_1, \ldots, p_r\}$ *em* $\mathcal{G}_d^n$,

denominamos ***matriz verificadora*** *de $\mathcal{C}$, $R(\mathcal{C})$, a matriz de tamanho $r \times 2n$ em que cada linha da matriz é o vetor $R(p_i)$.*

A matriz verificadora será útil na demonstração de diversos resultados. Dado um grupo estabilizador S com geradores $\mathbb{S} = \{s_1, \ldots, s_r\}$, $R(\mathbb{S})$ é a matriz verificadora de tamanho $r \times 2n$ sobre a coleção de geradores de S. O $\mathbb{Z}_d$-módulo gerado pelas linhas da matriz verificadora sobre $\mathbb{S}$ será denotado por $\langle R(\mathbb{S})\rangle$. É fácil verificar que $|S| = \#\langle R(\mathbb{S})\rangle$, em que o símbolo $\#$ denota a cardinalidade do conjunto. O conceito de matriz verificadora também será usado sobre a coleção de *operadores-palavras* $W = \{w_i\}_{i=1}^{K}$, gerando uma matriz verificadora $R(W)$ de tamanho $K \times 2n$.

Uma primeira questão que surge é se o fato do grupo estabilizador S ser abeliano, não conter múltiplos da identidade além da própria identidade e possuir ordem $|S| = d^n$ são condições necessárias e suficientes para que S estabilize a menos de fase um único estado $|\psi\rangle$. A resposta para esta pergunta é positiva. Para o caso binário o resultado está demonstrado em Nielsen e Chuang (2000) e faz uso da matriz verificadora $R(\mathbb{S})$. Podemos estender esta demonstração para o caso d primo. Podemos também demonstrar que o resultado é válido para um d qualquer usando ideias contidas em Arvind et al. (2002). Optamos por fazer uma demonstração similar à feita para qubits, usando a matriz verificadora $R(\mathbb{S})$ e a interpretação da matriz $R(\mathbb{S})\Lambda$ como um homomorfismo de $\mathbb{Z}_d$-módulos. Para fazer esta e outras demonstrações, iremos utilizar constantemente que, dado um homomorfismo entre $\mathbb{Z}_d$-módulos representado por uma matriz $\mathcal{T}$, a cardinalidade do módulo gerado pelas linhas de $\mathcal{T}$, que denotamos por $\langle\mathcal{T}\rangle$ é igual à cardinalidade do módulo gerado pelas colunas de $\mathcal{T}$, que pode ser representado pelo módulo $Im(\mathcal{T})$. De forma resumida faremos referência a estes módulos como módulos-linha e módulos-coluna, respectivamente. O resultado que que demonstra a igualdade está no apêndice B deste trabalho, no Teorema 5.

Queremos primeiramente estabelecer uma relação entre a ordem do grupo estabilizador $|S|$ e a dimensão do código estabilizado $\mathcal{Q}$. Para isto, primeiramente

estabelecemos o seguinte Lema:

Lema 1. *Sejam $S = \langle s_1, \ldots, s_r \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita. Se $|S| < d^n$, então podemos acrescentar um elemento $P \in \mathcal{G}_d^n \backslash S$ de forma que $\overline{S} = \langle s_1, \ldots, s_r, P \rangle$ continue abeliano e sem múltiplos da identidade além da própria.*

Demonstração. O operador Λ não muda a cardinalidade do módulo linha, logo temos $|S| = \#\langle R(\mathbb{S}) \rangle = \#\langle R(\mathbb{S})\Lambda \rangle < d^n$, e como a cardinalidade do módulo linha é igual à do módulo coluna, segue-se que $\#Im(R(\mathbb{S})\Lambda) < d^n$. Pelo primeiro Teorema do isomorfismo de módulos,

$$Im(R(\mathbb{S})\Lambda) \simeq \frac{\mathbb{Z}_d^{2n}}{Ker(R(\mathbb{S})\Lambda)}$$

o que faz com que $\#Ker(R(\mathbb{S})\Lambda) > d^n$, donde existe $\overline{P} \in \mathcal{G}_d^n \backslash S$ que comuta com todos os elementos de S. Seja o o primeiro número natural tal que $\overline{P}^o = \alpha I$. Tome $\beta \in \mathbb{C}$ tal que $\beta^o \alpha = 1$. Portanto $P = \beta \overline{P}$ comuta com todos os elementos de S e $P^o = I$, assim $\overline{S} = \langle s_1, \ldots, s_r, P \rangle$ é um grupo abeliano que não contém múltiplos da identidade que não a própria. □

Lema 2. *Sejam $S = \langle s_1, \ldots, s_r \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita. Então $|S| \leq d^n$.*

Demonstração. A demonstração segue passos análogos à demonstração do Lema 1. Suponha que $|S| > d^n$. Pelo primeiro Teorema do Isomorfismo de módulos temos que

$$Im(R(\mathbb{S})\Lambda) \simeq \frac{\mathbb{Z}_d^{2n}}{Ker(R(\mathbb{S})\Lambda)},$$

donde $\#Ker(R(\mathbb{S})\Lambda) < d^n$, o que é uma contradição pois todos os elementos de $\langle R(\mathbb{S}) \rangle$ pertencem a $Ker(R(\mathbb{S})\Lambda)$. □

O próximo teorema relaciona a ordem do grupo estabilizador com a dimensão do código quântico estabilizado $\mathcal{Q}$. Para entendê-lo, vamos iniciar toda uma

argumentação que culminará no teorema em questão.

Todo operador de Pauli P é um isomorfismo, assim se $\mathcal{Q}$ é um código quântico, $P\mathcal{Q}$ é um código quântico com a mesma dimensão de $\mathcal{Q}$. Se $\mathcal{Q}$ é estabilizado por $S = \langle s_1, \ldots, s_r \rangle$ então de acordo com o formalismo dos estabilizadores, $P\mathcal{Q}$ é estabilizado por $S' = PSP^\dagger$. Os geradores de S' são

$$S' = \langle q_d^{\alpha_1} s_1, \ldots, q_d^{\alpha_r} s_r \rangle$$

onde o vetor $(\alpha_1 \ldots, \alpha_r)$ é obtido usando a equação 3.4 de acordo com a operação a seguir

$$R(\mathbb{S})\Lambda R^T(P).$$

Se $\mathcal{Q}$ é estabilizado por S, então $\mathcal{Q}$ é o auto-espaço associado ao autovalor 1 de cada operador $\mathbb{S} = \{s_i\}$, logo $P\mathcal{Q}$ é o auto-espaço associado aos autovalores $\{q_d^{d-\alpha_i}\}$ de cada operador em $\mathbb{S}$. Considerando então o homomorfismo entre módulos representado pela matriz

$$R(\mathbb{S})\Lambda$$

temos que cada elemento $\mathbf{x}$ da imagem deste homomorfismo, $\mathbf{x} \in Im(R(\mathbb{S})\Lambda)$, representa um subespaço distinto de $\mathcal{H}_d^n$. Sabemos que são distintos pois subespaços associados à autovalores distintos tem apenas interseção trivial. O projetor sobre este subespaço é dado na Definição 16 do apêndice C.

Pelos lemas 1 e 2 sabemos que podemos completar o grupo estabilizador $S = \langle s_1, \ldots, s_r \rangle$ de tal forma que $S' = \langle s_1, \ldots, s_r, P_1, \ldots, P_m \rangle$ é um grupo estabilizador e tem ordem $|S'| = d^n$. Seja $\mathbb{S}' = \{s_1, \ldots, s_r, P_1, \ldots, P_m\}$. Como $|S'| = \#\langle R(\mathbb{S}') \rangle = \#\langle R(\mathbb{S}')\Lambda \rangle$ e a cardinalidade do módulo coluna é igual à do módulo linha, logo

$$\#Im(R(\mathbb{S}')) = d^n.$$

Como cada elemento $\mathbf{x} = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_m)$ de $Im(R(\mathbb{S}'))$ representa um subespaço distinto de mesma dimensão, e a dimensão do espaço todo é $dim(\mathcal{H}_d^n) = d^n$,

segue que cada subespaço $V_{\mathbf{x}}$ estabilizado por $\mathbb{S}' = \langle q_d^{\alpha_1} s_1, \ldots, q_d^{\alpha_r} s_r, q_d^{\beta_1} P_1, \ldots, q_d^{\beta_m} P_m \rangle$ tem dimensão 1 e a união destes cobre todo $\mathcal{H}_d^n$. Como cada $V_{\mathbf{x}}$ é um subespaço do espaço estabilizado por $\mathbb{S} = \langle q_d^{\alpha_1} s_1, \ldots, q_d^{\alpha_r} s_r \rangle$, estes também cobrem $\mathcal{H}_d^n$, tem interseção trivial e mesma dimensão, donde o subespaço $\mathcal{Q}$ estabilizado por S tem dimensão $dim(Q) = \frac{d^n}{|S|}$. Desta forma, acabamos de demonstrar o teorema dado a seguir:

Teorema 4. *Seja $S = \langle s_1, \ldots, s_r \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ em que $\{s_i\}_{i=1}^r$ são geradores independentes, que não contenha múltiplos da identidade que não a identidade propriamente dita. Então o subespaço estabilizado por S tem dimensão $\frac{d^n}{|S|}$.*

Como Corolários do teorema anterior, seguem três resultados importantes. Os dois primeiros serão usados na demonstração do Teorema 9 que, provavelmente, seja o resultado mais importante sobre códigos CWS. O terceiro resultado estabelece a quantidade de geradores de S no caso d primo.

Corolário 1. *Seja $S = \langle s_1, \ldots, s_r \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contém múltiplos da identidade que não a identidade propriamente dita. Se $|S| = d^n$ então S é um conjunto maximal de operadores de Pauli que estabiliza um único estado $|\psi\rangle$.*

Este Corolário diz que todo operador de Pauli $P \in \mathcal{G}_d^n$ que estabiliza $|\psi\rangle$ está em S. A demonstração é dada a seguir.

Demonstração. Pelo Teorema 4 temos que S estabiliza a menos de fase um único estado $|\psi\rangle$. Suponha que exista $P \in \mathcal{G}_d^n$ e $P \notin S$ que estabilize $|\psi\rangle$. Claramente P^t também estabiliza $|\psi\rangle$ para qualquer $t \in \mathbb{N}$; logo não existe $\bar{t} \in \mathbb{N}$ tal que $P^{\bar{t}} = \alpha I$ com $\alpha \neq 1$. Além disto, P comuta com todos os elementos de S pois caso contrário, existiria $s \in S$ e $\beta \neq 1$ tal que

$$|\psi\rangle = P|\psi\rangle = Ps|\psi\rangle = \beta sP|\psi\rangle = \beta|\psi\rangle$$

o que não pode ocorrer. Consequentemente, $S = \langle s_1, \ldots, s_r, P \rangle$ é um grupo abeliano que não contém múltiplos da identidade além da própria com $|S| > d^n$ e estabiliza $|\psi\rangle$, uma contradição com o Teorema 4. □

Corolário 2. *Sob as mesmas hipóteses, a menos de fase, S é um conjunto maximal de operadores abelianos.*

Demonstração. Suponha que $P \in \mathcal{G}_d^n$ seja um operador de Pauli que comuta com todos os elementos de S. Segue-se então que S estabiliza $|\psi\rangle$ e $P|\psi\rangle$, mas estes vetores não podem ser linearmente independentes pelo Teorema 4. Logo $P|\psi\rangle = \alpha|\psi\rangle$, isto é, o operador $\alpha^\dagger P$ estabiliza $|\psi\rangle$. Pelo Corolário anterior, segue-se que $\alpha^\dagger P \in S$. □

Corolário 3. *Sejam $S = \langle s_1, \ldots, s_r \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita e d primo. Então S estabiliza a menos de fase um único estado $|\psi\rangle$ se e somente se $r = n$.*

Demonstração. Se d é primo, então a ordem de cada gerador é $o(s_i) = d \; \forall i$ e segue que $|S| = d^r$. Então S estabiliza a menos de fase um único estado se e somente se $r = n$. □

Para d não primo, pode ocorrer de um gerador s_i de S ter ordem menor que d, sendo assim necessário que a quantidade r de geradores seja maior que n. A quantidade máxima de geradores é $2n$, de forma que, como citado em Hostens et al. (2005), $n \leq r \leq 2n$.

3.2 Códigos CWS baseados em *estados-grafos*

Uma forma de estudar os códigos CWS é por meio da Teoria de Grafos. O papel dos grafos está relacionado com o grupo estabilizador S da seguinte forma. Considere um grafo $\mathcal{G}(V, \Gamma)$ composto de um conjunto V de vértices e um conjunto de arestas definido por uma matriz de adjacência Γ com entradas em $\mathbb{Z}_d$. Considerando Γ_i como sendo as linhas da matriz Γ e X_i o operador X atuando no i-ésimo

qudit, os geradores de S são então construídos segundo a fórmula:

$$s_i = X_i Z^{\Gamma_i}.$$

Fazendo desta forma, é simples verificar que automaticamente $\{s_i\}$ é um conjunto comutativo e S não possui múltiplos da identidade além dela própria. Além disto, a ordem de cada gerador s_i é d, o que faz com que, independentemente de d ser primo ou não, $|S| = d^n$ e portanto, de acordo com o Corolário 1 o grupo estabilizador estabiliza, a menos de uma fase um único estado $|\psi\rangle$. Devido à forma como este estado é construído, ele costuma ser denominado "graphstate" (*estado-grafo*). Vários exemplos de códigos não binários e até mesmo famílias de códigos envolvendo grafos são explorados em Hu et al. (2008). A matriz verificadora de S neste caso é dada por

$$R(\mathbb{S}) = \left[\begin{array}{c|c} \Gamma & I \end{array}\right]$$

Ocorre que no caso de d ser primo, todo código CWS é equivalente à um código CWS na forma padrão. A noção de equivalência usada aqui é a de existir um operador local de Clifford levando um código CWS qualquer em um código CWS na forma padrão. Esta forma padrão é explicada na próxima definição.

Definição 4. *Um código CWS é dito estar na forma padrão se o grupo estabilizador S é baseado num grafo (i.e, o estado estabilizado $|\psi\rangle$ é um estado-grafo) e os operadores-palavras $W = \{w_i\}_{i=1}^K$ são operadores apenas em Z, isto é $w_i = Z^{c_i}$ com $w_1 = I$ (ou $c_1 = (0, \ldots, 0)$).*

Para mostrar que para d primo, todo código CWS é equivalente a um na forma padrão, a primeira coisa a se fazer é mostrar que existe um operador local de Clifford que por conjugação leva o grupo estabilizador $S = \langle s_1, \ldots, s_n \rangle$ para um grupo estabilizador S' baseado em um grafo. A demonstração deste resultado se encontra em Schlingemann (2002) e Grassl e Rötteler (2002), mas de uma forma muito geral e numa terminologia que não é a usual e de difícil compreensão. No caso específico de qubits, a demonstração se encontra de forma muito mais simples

em Van den Nest et al. (2004) e Elliott et al. (2007). Em tais referências, usa-se especificamente uma forma padrão da matriz verificadora $R(\mathbb{S})$, e as portas fase e Hadamard para qubits. Optamos então por generalizar a demonstração deste último artigo usando para isto as portas fase e Hadamard generalizadas para qudits, que são descritas em Hostens et al. (2005). Como as demonstrações se baseiam fortemente na matriz verificadora $R(\mathbb{S})$, vamos estabelecer o seguinte resultado

Teorema 5. *Sejam d primo, $S = \langle s_1, \ldots, s_m \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita e $R(\mathbb{S})$ a matriz verificadora.O conjunto de geradores de S são independentes se e somente se as linhas da matriz $R(\mathbb{S})$ são linearmente independentes.*

Demonstração. Considere $R(\alpha_{\mathbf{V}} Z^{\mathbf{V}_1} X^{\mathbf{V}_2}) = (\mathbf{V}_1|\mathbf{V}_2)$ a representação de um operador de Pauli na forma de vetores em $\mathbb{F}_d^{2n}$ (como d é primo, $\mathbb{Z}_d$ é o corpo $\mathbb{F}_d$). Temos que o produto de dois operadores de Pauli se reflete na soma módulo d

$$R(s_i s_j) = R(s_i) + R(s_j).$$

Suponha então que os geradores não sejam independentes. Isto significa que existem constantes $\alpha_i \in \mathbb{F}_d$ nem todas nulas tal que $\prod_{i=1}^r s_i^{\alpha_i} = I$ isto é, existem constantes nem todas nulas tal que $\sum_{i=1}^r \alpha_i R(s_i) = 0$ o que significa que as linhas de G são L.D.

Reciprocamente, se as linhas de G são L.D, então existem constantes nem todas nulas tal que $\prod_{i=1}^r s_i^{\alpha_i} = \alpha I$ mas α tem que ser 1, pois não há múltiplos da identidade senão a própria identidade em S, isto é, os geradores são L.D. □

Agora vamos estabelecer uma forma padrão da matriz verificadora quando d é primo. Isto é feito fazendo troca de qudits e operações de eliminação gaussiana em $R(\mathbb{S})$. Estas operações podem ser feitas pois equivalem a modificar os geradores $\{s_i\}$. Como já vimos, uma matriz verificadora se divide em dois blocos, o bloco da esquerda que representa os operadores Z e o bloco da direita que representa os

operadores X. Então a simples troca de colunas de $R(\mathbb{S})$ não é permitida; o que podemos fazer é trocar qudits. Ao trocar o qudit i com o qudit j, as colunas i e j de $R(\mathbb{S})$ são trocadas juntamente com as colunas $i+n$ e $j+n$.

O posto de $R(\mathbb{S})$ é n, pois S possui n geradores independentes. Seja P_r o posto da submatriz $n \times n$ de $R(\mathbb{S})$ do bloco à direita e fazendo eliminação gaussiana nesta submatriz obtemos:

$$R^1(\mathbb{S}) = \left[\begin{array}{cc|cc} B & C & I & A \\ D & E & 0 & 0 \end{array}\right],$$

em que I é a matriz identidade $P_r x P_r$. Olhando agora para o bloco esquerdo, considerando s o posto de E e fazendo a eliminação gaussiana em E, obtemos:

$$\left[\begin{array}{ccc|cc} B & C_1 & C_2 & I & A \\ D_1 & I & E_1 & 0 & 0 \\ D_2 & 0 & 0 & 0 & 0 \end{array}\right],$$

em que D_2 teria dimensão $s \times P_r$. Entretanto, procedendo deste modo, a única forma dos últimos s geradores comutarem com os P_r primeiros é fazendo com que D_2 ser a matriz nula, o que não pode ocorrer pois o posto de $R(\mathbb{S})$ é n, logo temos:

$$R^2(\mathbb{S}) = \left[\begin{array}{cc|cc} B & C & I & A \\ D & I & 0 & 0 \end{array}\right].$$

Assim, conseguimos por meio da eliminação gaussiana, zerar todas as entradas de C, depois, multiplicando as últimas $n - P_r$ linhas por -1 e renomeando as submatrizes, obtemos:

$$R^3(\mathbb{S}) = \left[\begin{array}{cc|cc} B & 0 & I & A \\ C & -I & 0 & 0 \end{array}\right].$$

Como os geradores devem comutar entre si, temos por um lado que $R^3(\mathbb{S})\Lambda(R^3(\mathbb{S}))^T$

deve ser a matriz nula e por outro lado este produto resulta em

$$\begin{bmatrix} -B^T + B & -C^T + A \\ C - A^T & 0 \end{bmatrix}.$$

Portanto, segue-se que $B = B^T$ e $C = A^T$, demostrando o seguinte teorema, que define uma forma padrão para $R(\mathbb{S})$ no caso de d primo:

Teorema 6. *Sejam $S = \langle s_1, \ldots, s_n \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita, $\{s_i\}$ um conjunto de geradores independentes e d primo. Então existem operações de troca de qudits e mudança de geradores tal que $R(\mathbb{S})$ assuma uma forma padrão*

$$R(\mathbb{S}) = \left[\begin{array}{cc|cc} B & 0 & I & A \\ A^T & -I & 0 & 0 \end{array}\right].$$

Considere agora os operadores locais de Clifford generalizados fase (P) e Hadamard (H), como descritos em Hostens et al. (2005)

$$H|x\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} q_d^{kx} |k\rangle, \quad P|x\rangle = \zeta^{x(x+d)} |x\rangle$$

em que $\zeta = e^{\frac{(d+1)\pi i}{d}}$. Podemos mostrar que

$$HXH^\dagger = Z, \quad HZH^\dagger = X^\dagger, \quad PXP^\dagger = \overline{\zeta} ZX, \quad PZP^\dagger = Z.$$

De acordo com as considerações anteriores, demonstramos o seguinte teorema:

Teorema 7. *Sejam $S = \langle s_1, \ldots, s_n \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita, $\{s_i\}$ um conjunto de geradores independentes e d primo. Então, trocando-se qudits e mudando geradores, S é equivalente por operações locais de Clifford a S', em que $R(\mathbb{S}') = \left[\begin{array}{c|c} \Gamma & I \end{array}\right]$ e Γ é a matriz de adjacência de algum grafo.*

Demonstração. Trocando qudits e mudando geradores, de acordo com o Teorema 6 podemos considerar

$$R(\mathbb{S}) = \left[\begin{array}{cc|cc} B & 0 & I & A \\ A^T & -I & 0 & 0 \end{array}\right]$$

em que B de tamanho $P_r \times P_r$ é uma matriz simétrica. Aplicando por conjugação H nos últimos $n - P_r$ qudits, obtemos

$$R(\mathbb{S}'') = \left[\begin{array}{cc|cc} B & A & I & 0 \\ A^T & 0 & 0 & I \end{array}\right].$$

Podemos zerar os valores B_{ii} da diagonal de B aplicando $P^{d-B_{ii}}$ nos primeiros P_r qudits para obter

$$R(\mathbb{S}''') = \left[\begin{array}{c|c} \Gamma & I \end{array}\right]$$

□

Resta então demostrar que para d primo todo código CWS é equivalente a um código CWS em um formato padrão:

Teorema 8. *Sejam $S = \langle s_1, \ldots, s_n \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita, $\{s_i\}$ um conjunto de operadores independentes, d primo, $|\psi\rangle$ o estado estabilizado por S e $W = \{w_i\}_{i=1}^K$ os operadores-palavras que definem um código CWS $\mathcal{Q}$. Então $\mathcal{Q}$ é equivalente a um código CWS $\mathcal{Q}'$ baseado em um estado-grafo com um conjunto de operadores-palavras $W' = \{w_i'\}_{i=1}^K$ formado apenas por operadores Z com $w_1' = I$.*

Demonstração. Segundo o Teorema 7, trocando qudits e geradores de S, existe um operador local de Clifford C tal que $C\mathcal{Q} = \mathcal{Q}'$, $S' = \langle s_1', \ldots, s_n' \rangle = CSC^\dagger$ e tal que $R(S') = \left[\begin{array}{c|c} \Gamma & I \end{array}\right]$. Uma base para o novo código $\mathcal{Q}'$ equivalente a $\mathcal{Q}$ é $\{Cw_1|\psi\rangle, \ldots, Cw_K|\psi\rangle\}$. $\{Cw_i|\psi\rangle\}$. $C|\psi\rangle$ é estabilizado por S'. Considerando os

vetores $\mathbf{V}^i$ e $\mathbf{U}^i \in \mathbb{F}_d^n$ satisfazendo $Cw_iC^\dagger = Z^{\mathbf{V}^i}X^{\mathbf{U}^i}$, temos que

$$Cw_i|\psi\rangle = Cw_iC^\dagger C|\psi\rangle = Z^{\mathbf{V}^i}X^{\mathbf{U}^i}C|\psi\rangle.$$

Podemos então transformar (a menos de fase), o operador Cw_i em um operador apenas em Z fazendo

$$Cw_i|\psi\rangle = Z^{\mathbf{V}^i}X^{\mathbf{U}^i}\prod_{k=1}^{n} s_k'^{d-\mathbf{U}^i_k}C|\psi\rangle = \alpha_i Z^{\mathbf{V}^i}\prod_{k=1}^{n} Z^{\mathbf{d}-\Gamma_k}C|\psi\rangle$$

onde $\mathbf{d}$ é o vetor com as n entradas assumindo o valor d. Então mostramos que $\mathcal{Q}'$ é um código CWS com *operadores-palavras* $w_i' = \alpha_i Z^{\mathbf{V}^i}\prod_{k=1}^{n} Z^{\mathbf{d}-\Gamma_k}$ e *estado-grafo* $C|\psi\rangle$ estabilizado por S'. Podemos considerar $w_1' = I$ aplicando em acréscimo a operação local de Clifford $w_1^\dagger$. □

3.3 Códigos CWS e códigos clássicos

Uma das grandes vantagens dos códigos CWS consiste em transformar o problema de achar bons códigos quânticos no problema de achar bons códigos clássicos. Códigos CWS no formato padrão oferecem vantagens neste processo que ainda serão discutidas neste capítulo, mas esta passagem do quântico para o clássico pode ser feita em um código CWS qualquer, independentemente do valor d. Para entender como isto é feito, primeiramente temos que analisar como tanto os erros quânticos como os *operadores-palavras* podem ser encarados como palavras clássicas em $\mathbb{Z}_d^r$, em que r é a quantidade de geradores de S.

Como o conjunto de dos operadores de erros de Pauli formam uma base para todos os possíveis erros que a informação quântica pode sofrer, consideraremos aqui apenas erros de Pauli $\{E_j\} \in \mathcal{G}_n^d$. Os *operadores-palavras* também pertencem a $\mathcal{G}_n^d$ e a passagem do quântico para o clássico na verdade pode ser feita para um operador de Pauli P qualquer, abrangendo assim tanto os erros como os *operadores-palavras*.

Seja $S = \langle s_1, \ldots, s_r\rangle$ o grupo estabilizador de um código CWS. Um operador de Pauli P em $\mathcal{G}_n^d$ pode então através de uma função que chamaremos de Cl_S, ser

transformado em um vetor $Cl_S(P) \in \mathbb{Z}_d^r$. Para cada entrada $Cl_S(P)_i$ de $Cl_S(P)$ esta função é definida da seguinte forma

Definição 5. *Seja $P \in \mathcal{G}_d^n$ e $\{s_i\}_{i=1}^r$ os geradores do grupo estabilizador S então*

$$Cl_S(P)_i = t, \quad se \;\; Ps_iP^\dagger = q_d^t s_i \tag{3.5}$$

Repare que o valor t está associado à fase que aparece na comutação de dois operadores de Pauli que por sua vez está associado ao operador Λ na definição da equação 3.3 e à equação 3.4. Estendendo esta equação para matrizes e considerando a matriz verificadora $R(\mathbb{S}) = \left[\begin{array}{c|c} A & B \end{array} \right]$ e a representação em $\mathbb{Z}_d^{2n}$ de P, $R(P)$, podemos também escrever

$$Cl_S(P) = R(\mathbb{S})\Lambda R^T(P) \tag{3.6}$$

isto é, considerando a representação em $\mathbb{Z}_d^{2n}$ dos erros e *operadores-palavras*, a função Cl_S é calculada através de um operador linear de $\mathbb{Z}_d^{2n}$ para $\mathbb{Z}_d^r$. Este fato junto com o fato de que, dado dois operadores de Pauli P_1 e P_2, temos $R(P_1P_2) = R(P_1) + R(P_2)$ faz com que Cl_S satisfaça

$$Cl_S(P_1P_2) = Cl_S(P_1) + Cl_S(P_2).$$

Consideraremos, então $\epsilon = \{E\}$ o conjunto de erros que desejamos que o código CWS detecte. $W = \{w_i\}_{j=1}^K$ é o conjunto de *operadores-palavras*. Considere também respectivamente os conjuntos $Cl_S(\epsilon)$ e $Cl_S(W) = \{c_j\}_{j=1}^K$. Observe que Cl_S não precisa ser injetiva, isto é, podem existir mais de um erro quântico tendo por imagem o mesmo erro clássico, por isto a cardinalidade de $Cl_S(\epsilon)$ pode ser menor que a cardinalidade de ϵ. Quanto aos *operadores-palavras*, a exigência de que $\{w_i|\psi\rangle\}_{j=1}^K$ forme um conjunto linearmente independente implica na condição de que $w_i^\dagger w_j \neq \alpha s$, com $s \in S$, para todo i, j e segundo o Corolário 2 o fato de S a menos de fase ser um conjunto abeliano maximal implica que $Cl_S(w_j^\dagger w_i) =$

$Cl_S(w_j) - Cl_S(w_i) \neq 0$ para todo $i \neq j$, donde a cardinalidade de W e $Cl_S(W)$ é a mesma.

A condição de detecção de erros para códigos quânticos quaisquer, deduzida em Knill e Laflamme (1997) e adaptada para os códigos CWS diz que, dado o conjunto $\epsilon = \{E\}$ de erros quânticos e uma base ortonormal $\{w_j|\psi\rangle\}_{j=1}^{K}$ para o código $\mathcal{Q}$, então $\mathcal{Q}$ detecta os erros em ϵ se e somente se para todo os possíveis trios (E, i, j), $E \in \epsilon$, $i, j = (1 \ldots, K)$

$$\langle\psi|w_i^\dagger E w_j|\psi\rangle = C_E \delta_{ij}, \tag{3.7}$$

em que C_E é uma constante que depende apenas do erro (não depende dos *operadores-palavras* w_i).

Temos então duas possibilidades:

(1) Se $w_i^\dagger E w_j = \alpha s$, onde $s \in S$ então

$$\langle\psi|w_i^\dagger E w_j|\psi\rangle = \alpha;$$

(2) Se $w_i^\dagger E w_j \neq \alpha s$, em que $s \in S$ pelo Corolário 2 $w_i^\dagger E w_j$ anti-comuta com algum $\overline{s} \in S$ donde

$$\langle\psi|w_i^\dagger E w_j|\psi\rangle = \langle\psi|w_i^\dagger E w_j \overline{s}|\psi\rangle = \langle\psi|q_d^{k_s} w_i^\dagger E w_j|\psi\rangle = q_d^{k_s}\langle\psi|w_i^\dagger E w_j|\psi\rangle$$

com $q_d^{k_s} \neq 1$. Então, decorre que

$$\langle\psi|w_i^\dagger E w_j|\psi\rangle = 0.$$

Segue que para $i \neq j$ a condição 3.7 é satisfeita se e somente se, para todos os possíveis trios (E, i, j), $w_i^\dagger E w_j \neq \alpha s$ onde $s \in S$. Isto ocorre se e somente se

$$0 \neq Cl_S(w_i^\dagger E w_j) = Cl_S(w_j) + Cl_S(E) - Cl_S(w_i)$$

para todos os possíveis trios (E, i, j), isto é, se e somente se $Cl_S(w_j) + Cl_S(E) \neq Cl_S(w_i)$, $\forall i \neq j$ e $E \in \epsilon$, o que equivale a dizer que o código clássico $Cl_S(W)$ detecta os erros clássicos $Cl_S(\epsilon)$.

Tudo o que foi discutido acima é válido para $i \neq j$. Se quisermos que o código quântico detecte os erros em ϵ temos ainda que considerar, para todas as possíveis duplas (E, i) que

$$\langle\psi|w_i^\dagger E w_i|\psi\rangle = C_E$$

em que C_E é uma constante que só depende do erro. Se $w_i^\dagger E w_i \neq \alpha s$ em que $s \in S$, caso em que $Cl_S(w_i^\dagger E w_i) \neq 0$, temos $\langle\psi|w_i^\dagger E w_i|\psi\rangle = 0$ e a condição 3.7 está automaticamente satisfeita, caso contrário, isto é, quando $Cl_S(w_i^\dagger E w_i) = 0$, ou, em outras palavras, quando $w_i^\dagger E w_i = \alpha_i s$, onde $s \in S$ temos

$$\langle\psi|w_i^\dagger E w_i|\psi\rangle = \alpha_i$$

e para que a condição de detectabilidade 3.7 seja satisfeita, é preciso que as constantes α_i sejam a mesma, independente de i. Como podemos considerar sem perda de generalidade que $w_1 = I$, as equações $\alpha_i = \langle\psi|E|\psi\rangle$ precisam ser satisfeitas para todo i, e isto ocorre se e somente se $Ew_i = w_i E$ para todo i.

Do que foi discutido anteriormente, está provado Teorema 9, dado a seguir:

Teorema 9. *Sejam $\mathcal{Q}$ um código CWS com operadores-palavras $W = \{w_i\}_{i=1}^K$, $w_1 = I$ e $\epsilon = \{E\}$ um conjunto de erros de Pauli. $\mathcal{Q}$ detecta erros em ϵ se e somente se $Cl_S(W)$ detecta erros em $Cl_S(\epsilon)$ e além disto, se $Cl_S(E) = 0$ então*

$$Ew_i = w_i E \tag{3.8}$$

para todo i.

O Teorema 9 cumpre o prometido de transformar o problema de achar bons códigos quânticos no problema de achar bons códigos clássicos, desde que a condição 3.8 seja satisfeita. Chamaremos esta condição a partir deste ponto de condição

quântica de correção de erros em oposição à condição clássica que também tem de ser satisfeita.

Uma outra importante característica dos códigos CWS diz respeito à função Cl_S. Nestes códigos, esta função separa os erros em classes de degenerescência. Dois erros E_1 e E_2 estão na mesma classe de degenerescência se possuem o mesmo efeito no código, isto é, $\langle\psi_i|E_1^\dagger E_2|\psi_i\rangle = \alpha$, onde $\{|\psi_i\rangle\}$ é uma base para o código e $\alpha \neq 0$. Mas como já discutido, neste caso temos que $E_1^\dagger E_2 = \alpha s$, com $s \in S$ e $Cl_S(E_2) - Cl_S(E_1) = 0$ logo $Cl_S(E_1) = Cl_S(E_2)$.

Nesta seção, vimos que há uma relação entre códigos quânticos CWS e códigos clássicos. A grande utilidade dos códigos CWS está em fornecer uma metodologia para encontrar novos códigos quânticos. Para isto usa-se a recíproca do Teorema 9. Na Seção 3.5 discutiremos em mais detalhes o algoritmo usado para isto, mas resumidamente, dado um grupo estabilizador S e um conjunto de erros de Pauli $\epsilon = \{E\}$ que desejamos que nosso código detecte, determinamos $Cl_S(\epsilon)$ e por meio de um código clássico $C = \{c_i\}_{i=1}^K$ que detecte os erros em $Cl_S(\epsilon)$, conseguimos nosso código quântico descobrindo um conjunto de operadores de Pauli $W = \{w_i\}_{i=1}^K$ tal que $Cl_S(W) = C$. Uma grande vantagem dos códigos no formato padrão (baseado em *estados-grafos*), está justamente nesta etapa, pois se o código está neste formato, encontrando-se o código clássico $C = \{c_i\}$ que detecte erros em $Cl_S(\epsilon)$, facilmente encontraremos os *operadores-palavras* W fazendo simplesmente $w_i = Z^{c_i}$. Se o código não está no formato padrão, encontrar tais operadores pode ser difícil, podendo mesmo não existir um conjunto de operadores W tais que $Cl_S(W) = C$.

3.4 Códigos CWS e códigos estabilizadores

Esta seção pretende estabelecer relações entre códigos CWS e códigos estabilizadores. Existem vários exemplos de códigos que não são construídos com o formalismo CWS, como vemos em Grassl e Beth (1997), Grassl e Rötteler (2008a), Grassl e Rötteler (2008b) e Smolin et al. (2007). Existem também vários códigos

CWS que não são estabilizadores, como podemos conferir em Chen et al. (2008), Cross et al. (2009), Yu et al. (2008), Yu et al. (2007), Yu et al. (2009). Ocorre que todo código estabilizador é na verdade um código CWS e todo código CWS com *operadores-palavras* W formando um grupo, é um código estabilizador. Estes resultados encontram-se demonstrados no caso binário em Cross et al. (2009); o caso mais geral de *estados-grafos* para d qualquer encontra-se demonstrado em Looi et al. (2007), mas não encontramos na literatura uma demonstração geral, válida para qualquer d, e não estando baseada em *estados-grafos*, assim fizemos uma demonstração baseada na estrutura da matriz verificadora (Definição 3). Dado um conjunto de operadores de Pauli $\mathcal{C}$, definiremos a matriz verificadora com coeficientes em $\mathbb{Z}_d$, $R(\mathcal{C})$. Se a quantidade de operadores em $\mathcal{C}$ é l, $R(\mathcal{C})$ representa um homomorfismo entre os $\mathbb{Z}_d$-módulos, $\mathbb{Z}_d^{2n} \to \mathbb{Z}_d^l$, portanto faz sentido falar dos módulos núcleo e imagem, respectivamente $Ker(R(\mathcal{C}))$ e $Im(R(\mathcal{C}))$. O módulo $Im(R(\mathcal{C}))$ é o módulo gerado pelas colunas de $R(\mathcal{C})$ enquanto para denotar o módulo gerado pelas linhas de $R(\mathcal{C})$, escolheremos a notação $\langle R(\mathcal{C})\rangle$.

Lema 3. *Seja $\mathcal{Q}$ um código CWS com estabilizador S gerado por $\mathbb{S} = \{s_1, \ldots, s_r\}$ e operadores-palavras $W = \{w_i\}_{i=1}^K$. Então há uma relação de igualdade entre as cardinalidades do centralizador de W em S, $C_S(W)$ e a cardinalidade do $\mathbb{Z}_d$-módulo $\langle R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda)$, isto é*

$$\#C_S(W) = \#\langle R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda)$$

Demonstração. Basta mostrar que a função

$$\begin{array}{rccc} f: & C_S(W) & \to & R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda) \\ & g & \mapsto & R(g) \end{array}$$

está bem definida, e é bijetiva.

(1) f é bem definida pois pois tome $g_1, g_2 \in C_S(W)$. Se $R(g_1) \neq R(g_2)$ então

$R(g_1^\dagger g_2) \neq \mathbf{0}$ [2] segue que $g_1 \neq g_2$.

(2) f é injetiva, pois tome $g_1, g_2 \in C_S(W)$. Se $R(g_1) = R(g_2)$ então $R(g_1^\dagger g_2) = \mathbf{0}$, logo $g_1^\dagger g_2 = \alpha I$ e $\alpha = 1$ pois não existe múltiplos da identidade que não a própria em S.

(3) f é sobrejetiva pois tome $\mathbf{v} \in \langle R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda)$. Existe $\overline{g} \in \mathcal{G}_d^n$ tal que $R(\overline{g}) = \mathbf{v}$. Como $\mathbf{v} \in \langle R(\mathbb{S})\rangle$ e a menos de fase $\langle R(\mathbb{S})\rangle$ é um conjunto abeliano maximal, existe $g = \alpha\overline{g}$ com $g \in S$ e $R(g) = \mathbf{v}$.

Como $\mathbf{v} \in Ker(R(W)\Lambda)$, $R(W)\Lambda R^T(g) = \mathbf{0}$ segue que g comuta com todos elementos de W, logo $g \in C_S(W)$.

□

Teorema 10. *Seja $\mathbb{Q}$ um código CWS com estabilizador S gerado por $\mathbb{S} = \{s_1, \ldots, s_r\}$. e operadores-palavras $W = \{w_i\}_{i=1}^K$ com $w_1 = I$ [3] . Então $\mathbb{Q}$ é um código estabilizador se e somente se satisfaz $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle} = K$.*

Demonstração. Seja $|\psi\rangle$ o estado estabilizado por S e $\beta = \{w_i|\psi\rangle\}_{i=1}^K$ uma base para $\mathbb{Q}$. Temos que $\mathbb{Q}$ é um código estabilizador se e somente se existe um subgrupo $H \leq \mathcal{G}_d^n$ abeliano, que não contém múltiplos da identidade que não a própria e que estabiliza $\mathbb{Q}$. Em particular H precisa estabilizar $|\psi\rangle$ e como S é um subgrupo maximal que estabiliza $|\psi\rangle$ (Corolário 1), logo $H \leq S$. Além disso, todo elemento $h \in H$ precisa satisfazer $hw_i = w_i h$ para todo i, logo o subgrupo H é o centralizador de W em S, isto é $H = C_S(W)$. Resta então mostrar que $\frac{d^n}{|C_S(W)|} = \frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle}$, assim de acordo com o Teorema 4 garantimos que $C_S(W)$ estabiliza $\mathbb{Q}$ se e somente se $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle} = K$.

De acordo com o Lema 3, temos que

$$\#C_S(W) = \#\langle R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda)$$

[2] Nesta seção, $\mathbf{0}$ representa o vetor nulo em $\mathbb{Z}_d^{2n}$

[3] Esta condição não é restritiva pois todo código CWS é equivalente a um com $w_1 = I$. Basta fazer $w_i' = w_1^\dagger w_i$.

Como S representa a menos de fase um conjunto abeliano maximal em $\mathcal{G}_d^n$ (Corolário 2), temos que $\langle R(\mathbb{S})\rangle = Ker(R(\mathbb{S})\Lambda)$, donde segue-se que

$$\langle R(\mathbb{S})\rangle \bigcap Ker(R(W)\Lambda) = Ker(R(\mathbb{S})\Lambda) \bigcap Ker(R(W)\Lambda) = Ker(M)$$

em que $M = \begin{bmatrix} R(\mathbb{S})\Lambda \\ R(W)\Lambda \end{bmatrix} = \begin{bmatrix} R(\mathbb{S}) \\ R(W) \end{bmatrix} \Lambda$. Estimaremos então $\#Ker(M)$.

Temos que $\langle M\rangle = \langle R(\mathbb{S})\Lambda\rangle + \langle R(W)\Lambda\rangle$. Pelo segundo Teorema do isomorfismo para módulos, temos que

$$\frac{\langle R(\mathbb{S})\Lambda\rangle + \langle R(W)\Lambda\rangle}{R(\mathbb{S})\Lambda} \simeq \frac{\langle R(W)\Lambda\rangle}{\langle R(W)\Lambda\rangle \cap \langle R(\mathbb{S})\Lambda\rangle},$$

e como o operador Λ não altera a cardinalidade do módulo linha, temos que $\#\langle M\rangle = \frac{\#\langle R(\mathbb{S})\rangle \#\langle R(W)\rangle}{\#\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle}$ e portanto como $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle} = K$ e $\#\langle R(\mathbb{S})\rangle = |S| = d^n$, temos que $\#\langle M\rangle = Kd^n$. Como visto anteriormente, a cardinalidade do módulo linha é igual a cardinalidade do módulo coluna, assim $\#Im(M) = Kd^n$. Finalmente, pelo primeiro Teorema do isomorfismo, temos que $\#Ker(M) = \dfrac{d^{2n}}{Kd^n} = \frac{d^n}{K}$. □

.

Exemplo 4. *Tome o código* $((3,3,2))_3$ *com estabilizador* $S = \langle s_1, s_2, s_3\rangle$ *onde* $s_1 = XZI$, $s_2 = ZXZ$ *e* $s_3 = IZX$ *e operadores-palavras* $W = \{I, (XZ)\otimes Z \otimes Z^2, (XZ^2)\otimes Z\otimes Z\}$. *Temos respectivamente:*

$$R(\mathbb{S}) = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ e } R(W) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

o módulo linha de $R(W)$, $\langle R(W)\rangle$ é representado pelos seguintes vetores:

000000	112100
010100	211100
020200	221200
	122200
	201000
	102000

onde à esquerda estão aqueles pertencentes a $\langle R(\mathbb{S})\rangle \cap \langle R(W)\rangle$. Vemos então que $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle\cap\langle R(\mathbb{S})\rangle} = K$ e logo o código é estabilizador pelo Teorema 10. Na verdade conseguimos ver que através da transformação local de Clifford $s_1 = XZI \in S$ este código é equivalente ao código $[[3,1,2]]_3$ presente em Hu et al. (2008) com mesmo estabilizador e operadores-palavras $W' = \{I, ZIZ^2, Z^2IZ\}$.

Deste teorema, resultam dois Corolários que representam resultados mais utilizados na literatura.

Corolário 4. *Seja $\mathcal{Q}$ um código CWS com estabilizador $S = \langle s_1, \ldots, s_r\rangle$ e operadores-palavras $W = \{w_i\}_{i=1}^K$ formando um grupo. Então $\mathbb{Q}$ é um código estabilizador.*

Demonstração. Se W é um grupo, então as linhas de $R(W)$ também formam um grupo aditivo, logo $\#\langle R(W)\rangle = \#W = K$. Além disto, pela construção dos códigos CWS, $\langle R(W)\rangle \cap \langle R(\mathbb{S})\rangle = \{0\}$, portanto $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle\cap\langle R(\mathbb{S})\rangle} = K$ □

Corolário 5. *Seja $\mathbb{Q}$ um código CWS com estabilizador $S = \langle s_1, \ldots, s_r\rangle$, operadores-palavras $W = \{w_i\}_{i=1}^K$ com $w_1 = I$ e estado estabilizado $|\psi\rangle$. Se as palavras clássicas $Cl_S(W)$ formam um grupo, então o código é estabilizador.*

Demonstração. Para mostrar que $\frac{\#\langle R(W)\rangle}{\#\langle R(W)\rangle\cap\langle R(\mathbb{S})\rangle} = K$ basta mostrar que todo elemento $r_w \in \langle R(W)\rangle$ é da forma $r_w = R(w_j)+r_s$, com $r_s \in \langle R(\mathbb{S})\rangle$. A transformação Cl_S está definida em $\mathcal{G}_d^n$. cada elemento de $\mathcal{G}_d^n$ tem uma representação em $\mathbb{Z}_d^{2n}$. Como já visto (equação 3.6), podemos descrever a transformação Cl_S sobre $\mathbb{Z}_d^{2n}$ como um homomorfismo de módulos representado pela matriz $\mathcal{T} = R(\mathbb{S})\Lambda$.

Tome então $r_w \in \langle R(W)\rangle$. Logo $r_w = \alpha_1 R(w_1) + \ldots + \alpha_k R(w_k)$ e

$$\begin{aligned}\mathcal{T}(r_w) &= \alpha_1 \mathcal{T}(R(w_i)) + \ldots + \alpha_k \mathcal{T}(R(w_k)) \\ &= \alpha_1 c_1 + \ldots + \alpha_k c_k\end{aligned}$$

Como $Cl_S(W)$ forma um grupo, temos que o último somatório é $\mathcal{T}(R(w_j)) = c_j \in Cl_S(W)$, isto é, $\mathcal{T}(r_w) = \mathcal{T}(R(w_j))$ logo

$$r_w = R(w_j) + r_s$$

onde $r_s \in Ker(\mathcal{T}) = \langle R(\mathbb{S})\rangle$. □

Segue também que todo código estabilizador pode ser visto como um código CWS, como mostrado no próximo teorema

Teorema 11. *Todo código estabilizador $\mathcal{Q}$ pode ser visto como um código CWS.*

Demonstração. Seja $S' = \langle s_1, \ldots, s_m\rangle$ o grupo estabilizador do código $\mathcal{Q}$ e seja $dim(\mathcal{Q}) = K$. Como já discutido, S' pode então ser estendido para um grupo maximal $S = \langle s_1, \ldots, s_m, g_1, \ldots, g_l\rangle$ com cardinalidade $|S| = d^n$. Este grupo estabiliza a menos de fase um único estado $|\psi\rangle \in \mathcal{Q}$. Considere a matriz verificadora $R(\mathbb{S})$. Temos que $\#\langle R(\mathbb{S})\rangle = d^n$. Como a cardinalidade do módulo linha é a mesma do módulo coluna, temos que $\#Im(R(\mathbb{S})) = d^n$ e por sua vez também $\#Im(R(\mathbb{S})\Lambda) = d^n$. Esta igualdade implica que para cada $\mathbf{x} \in Im(R(\mathbb{S})\Lambda)$, existe um operador de Pauli $P_{\mathbf{x}}$ tal que $\mathcal{H}_d^n = \bigoplus P_{\mathbf{x}}|\psi\rangle$ e cada estado $P_{\mathbf{x}}|\psi\rangle$ é a interseção dos auto-espaços associados aos autovalores $q_d^{d-x_i}$ de cada gerador de S. Como $\mathcal{Q}$ é um código estabilizador e $dim(\mathcal{Q}) = K$ sabemos que existem K destes operadores de Pauli formando um conjunto $W = \{P_{x_i}\}_{i=1}^K$ que formam uma base para $\mathcal{Q}$. Basta então tomar o conjunto W como os *operadores-palavras*. □

3.5 Algoritmos para encontrar códigos CWS

Podemos utilizar o Teorema 9 para descobrir códigos quânticos baseados no formalismo CWS. A referência Chuang et al. (2009) explicita algoritmos que podem ser usados com este propósito, mas faz apenas para o caso binário e no formato padrão. Neste trabalho optamos por descrever algoritmos que tratam o caso geral. No final, o problema de achar bons códigos quânticos se transforma no problema de achar o clique máximo em um grafo, que é NP-completo.

Como parâmetros de entrada teremos $R(\mathbb{S})$ a matriz verificadora de tamanho $d \times 2n$ sobre os geradores de S e $R(\epsilon)$, a matriz verificadora sobre o conjunto de erros que se quer detectar. Como saída, será fornecido o conjunto de K *operadores-palavras* W, representado pela matriz verificadora $R(W)$ de tal forma que $Cl_S(W)$ detecte os erros em $Cl_S(\epsilon)$ e satisfaça a condição 3.8 do Teorema 9. Nos algoritmos, os elementos de uma matriz (considerado também um conjunto de vetores) serão acessados por colchetes, Ex: $R(\epsilon)[i]$ e vamos representar um vetor coluna como o transposto de um vetor linha, Ex: $R^T(\epsilon)[i]$ ou $(R(\epsilon)[i])^T$.

O primeiro algoritmo guarda na variável $ErrosS$ os erros em $R(\epsilon)$ que pertencem a S e na variável $ErrosClassicos$ a representação clássica dos erros que não pertencem a S. Precisaremos do primeiro conjunto para tratar a condição 3.8 do Teorema 9 e do segundo conjunto para tratar a parte clássica do teorema.

Entrada: $R(\epsilon)$, $R(\mathbb{S})$
Saida : $ErrosClassicos$, $ErrosS$

$j := 1$, $k := 1$;
para $i = 1 : \#R(\epsilon)$ **faça**
  se $R(\mathbb{S})\Lambda R^T(\epsilon)[i] = 0^r$ **então**
    $ErrosS[j] := R(\epsilon)[i]$; $j := j + 1$;
  fim
  se $R(\mathbb{S})\Lambda R^T(\epsilon)[i] \neq 0^r$ **e** $R(\mathbb{S})\Lambda R(\epsilon)[i] \notin ErrosClassicos$ **então**
    $ErrosClassicos[k] := R(\mathbb{S})\Lambda R^T(\epsilon)[i]$; $k := k + 1$;
  fim
fim

Algoritmo 1: Procedimento que separa os erros que pertencem ou não a S e transforma os que não pertencem em erros clássicos.

O segundo algoritmo usa os erros que pertencem a S, guardados em $ErrosS$

e percorre todos os vetores em $\mathbb{Z}_d^{2n}$, de $(0,\ldots,0)$ até $(d-1,\ldots,d-1)$ identificando quais *operadores-palavras* que satisfazem a condição quântica do teorema (caso em que a variável *sinal* assume o valor 1), guardando um representante de cada classe de degenerescência na variável $Palavras$ e sua representação clássica em vetores pertencentes a $\mathbb{Z}_d^r$ é guardado em $PalavrasClassicas$. O segundo conjunto será usado para achar um código clássico C que detecte os erros clássicos em $ErrosClassicos$ e, achando C, o primeiro conjunto será usado para associar cada palavra clássica em C à um operador-palavra em $Palavras$. É importante frisar que este algoritmo é desnecessário caso o código CWS esteja no formato padrão e não existam erros em $\epsilon = \{E\}$ que pertençam a S.

Entrada: $ErrosS$
Saida : $Palavras$, $PalavrasClassicas$

$j := 1$;
para $v = (0,\ldots,0) : (d-1,\ldots,d-1)$ **faça**
  $sinal := 1$;
  para $i = 1 : \#ErrosS$ **faça**
    se $v\Lambda(ErrosS[i])^T \neq 0$ **então** $sinal := 0$;
  fim
  se ($sinal = 1$ **e** $R(\mathbb{S})\Lambda v^T \notin PalavrasClassicas$) **então**
    $Palavras[j] := v$;
    $PalavrasClassicas[j] := R(\mathbb{S})\Lambda v$;
    $j := j + 1$;
  fim
fim

Algoritmo 2: Procedimento que cria o conjunto de operadores de Pauli que podem ser candidatos a *operadores-palavras* e sua representação clássica.

Com o Algoritmo 2, temos armazenado na variável $Palavras$ todas as palavras clássicas que satisfazem a condição quântica do Teorema 9 e na variável $PalavrasClassicas$ um representante clássico de cada palavra em $Palavras$. O que precisamos agora é achar um código com palavras pertencentes ao conjunto $PalavrasClassicas$ que detectem os erros clássicos em $ErrosClassicos$.

Para achar então o código quântico com o maior K possível, usaremos a seguinte estratégia. Construiremos um super-grafo em que os vértices são todas as palavras em $PalavrasClassicas$ e dois vértices (i,j) estarão conectados se não

existir erro clássico em $ErrosClassicos$ que leve a palavra $PalavrasClassicas[i]$ na palavra $PalavrasClassicas[j]$ ou vice-versa. Conseguiremos então o nosso código quântico otimal achando o clique máximo neste super-grafo. O Algoritmo 3 explicita o Algoritmo de construção da matriz de adjacência M deste super-grafo.

Entrada: $PalavrasClassicas$
Saida : M

Faça $M[i,j] = 0 \forall i,j$;
para $i = 1 : \#PalavrasClassicas$ **faça**
  para $j = i+1 : \#PalavrasClassicas$ **faça**
    se
    $(PalavrasClassicas[i] - PalavrasClassicas[j]) \notin ErrosClassicos$
    e
    $(PalavrasClassicas[j] - PalavrasClassicas[i]) \notin ErrosClassicos$
    então
      $M[i,j] := 1$; $M[j,i] := 1$;
    fim
  fim
fim

Algoritmo 3: Procedimento que cria a matriz de adjacência do super-grafo, onde se irá procurar o clique máximo.

Após o Algoritmo 3, resta acionar uma rotina para encontrar o clique máximo do super-grafo representado pela matriz de adjacência M. Tendo encontrado este clique máximo, usamos então o conteúdo armazenado em $Palavras$ para exibir os *operadores-palavras* que definem o código. O problema de achar um clique máximo de um grafo é um problema muito estudado na computação e há vários algoritmos conhecidos que fazem esta tarefa, por isso não será descrito aqui neste trabalho, mas seu custo, como citado em Chuang et al. (2009) é aproximadamente de d^r, por causa da representação em $\mathbb{Z}_d^r$ de $PalavrasClassicas$.

3.6 Códigos CWS assimétricos

Os Algoritmos 1, 2 e 3 descritos na seção anterior podem ser usados da seguinte forma. Dados o grupo estabilizador S, um conjunto de erros quânticos que se deseja detectar $\epsilon = \{E\}$ e n fixos, podemos então achar um código CWS otimal, isto é, com maior parâmetro K possível que detecte os erros em ϵ. Normalmente

os erros que se deseja detectar são erros dados por um parâmetro δ de forma que os erros em ϵ representam erros quânticos de peso até $\delta - 1$ e o código quântico encontrado tenha parâmetros $((n, K, \delta))_d$. A maior parte dos exemplos encontrados na literatura se encaixam neste padrão, mas isto não é necessário, podendo os erros em ϵ serem descritos de forma diferente. Nesta seção iremos explorar a aplicação dos algoritmos no caso binário ($d = 2$) e buscando códigos CWS que detectem erros quânticos de Pauli compostos separadamente de operadores Z em até $d_Z - 1$ qubits e X em até $d_X - 1$ qubits. Estes códigos são chamados de assimétricos e seus parâmetros são dados por $((n, K, d_Z/d_X))_d$. Famílias de códigos CWS apresentando n e K crescentes são raros na literatura. Nesta seção apresentaremos o resultado da aplicação dos algoritmos para códigos assimétricos, tentando encontrar famílias de códigos com n e K crescentes. Para isto, usaremos uma metodologia interessante, encontrando-se deste modo, alguns códigos novos. A metodologia é interessante pois de certa forma ataca um problema ainda em aberto dentro do formalismo dos códigos CWS, que é o problema de determinar a forma que o grupo estabilizador S precisa ter para se encontrar códigos quânticos com bons parâmetros K.

A metodologia utilizada consiste basicamente em buscar grupos estabilizadores baseados em grafos satisfazendo a propriedade $S \bigcap \epsilon = \emptyset$, isto é, sem erros detectáveis em S. A grande maioria dos exemplos de códigos CWS encontrados na literatura satisfazem esta restrição. A ausência desta restrição, isto é, a existência de erros detectáveis em S, exige considerarmos a condição quântica 3.8 do Teorema 9, e consequentemente, há a necessidade de aplicação do Algoritmo 2, que tem por incumbência identificar as palavras que podem ser usadas na procura do código.

Para esclarecer a metodologia usada, vamos pensar em $d_Z = d_X = 3$. Primeiramente, temos que escolher os geradores s_i de S de forma que nenhum deles possua erros Z e X atuando, ao mesmo tempo em uma quantidade menor que 3 qubits, pois desta forma os geradores pertenceriam a S. Duas formas sistemáticas de se fazer isto mantendo a estrutura baseada em grafo do código CWS consistem

em:

(1) Escolher os geradores de forma parecida com uma estrutura cíclica, fazendo

$$s_i = Z_{i-2}Z_{i-1}X_iZ_{i+1}Z_{i+2}$$

onde $1 \leq i \leq n$ e as somas e subtrações representadas no índice dos operadores são operações em $\mathbb{Z}_n$;

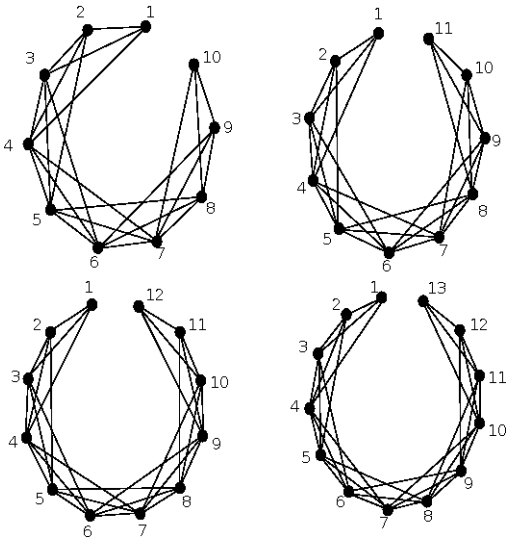
(2) Não obedecer uma estrutura cíclica escolhendo os geradores no formato

$$s_i = Z_{i-3}Z_{i-2}Z_{i-1}X_iZ_{i+1}Z_{i+2}Z_{i+3}$$

para $3 < i < n-3$. Para $i = 1, 2, 3$, fazer, respectivamente $X_1Z_2Z_3Z_4$, $Z_1X_2Z_3Z_4Z_5$, $Z_1Z_2X_3Z_4Z_5Z_6$ e para $i = n-2, n-1, n$, fazer de forma análoga.

Computacionalmente a segunda estrutura se mostrou mais rápida na procura dos códigos, portanto os exemplos encontrados com os parâmetros $d_Z = d_X = 3$ seguem esta estrutura. Para $n = 10, 11, 12, 13$ os grafos associados exibem o formato mostrado na Figura 3.1.

Figura 3.1: Grafos associados aos códigos $((n, K, 3/3))$, $10 \leq n \leq 13$



Mas não basta que os geradores não pertençam a ϵ, isto é, que os geradores não sejam erros detectáveis; requer-se ainda que não exista nenhum elemento de S em ϵ, por isso precisamos verificar todas as combinações dos geradores de S. Neste sentido, o segundo passo consiste em fazer n crescer e descobrir se existem valores de n de tal forma que $S \bigcap \epsilon = \emptyset$. Como estamos lidando com grupos estabilizadores no formato padrão, para $d_Z = d_X = 3$ basta verificarmos todos os elementos de S que são o produto de 2 geradores apenas, pois elementos de S que são produtos de mais geradores automaticamente não satisfazem a condição $d_X = 3$. Podemos verificar, no caso deste exemplo, isto é, $d_Z = d_X = 3$ e geradores de S no formato não cíclico que para qualquer $n > 4$, a condição $S \bigcap \epsilon = \emptyset$ será sempre satisfeita.

Tendo concluído os passos 1 e 2, agora usamos os algoritmos para testar se realmente existem códigos com os parâmetros n encontrados. Fazendo isto encontramos códigos com os seguintes parâmetros.

Tabela 3.1: Parâmetros n e K para códigos $((n, K, 3/3))$ com $10 \leq n \leq 13$

Códigos $((n, K, 3/3))$	
n	K
10	2
11	4
12	8
13	16

Para $n > 13$, por motivos de eficiência computacional, não foi possível verificar se o padrão observado na tabela seria mantido, isto é, se conseguiríamos códigos com parâmetro $K = 32, 64, \ldots$. Apesar disso, sabemos que o padrão não pode perdurar para sempre, pois com esta metodologia, os códigos sempre satisfazem $\epsilon \bigcap S = \emptyset$, isto é, $Cl_S(E) \neq 0$ para qualquer erro E no conjunto de erros detectáveis ϵ, o que faz com que estes códigos sejam não degenerados, satisfazendo desta forma, a versão assimétrica do limitante quântico de Hamming facilmente computável. O conjunto de erros corrigíveis é composto de erros X e Z atuando cada um separadamente em 1 qubit, isto é, podemos ter:

(1) Ausência de erros: quantidade - 1.

(2) Um erro X e nenhum erro Z: quantidade - n.

(3) Um erro X e um erro Z: quantidade - n^2.

(4) Nenhum erro X e um erro Z: quantidade - n.

No total a quantidade de erros corrigíveis é $(n+1)^2$. Um código não degenerado de parâmetros $((n, K, 3/3))$ satisfaz a seguinte desigualdade:

$$2^n \geq (n+1)^2 K.$$

Podemos verificar que neste exemplo, já para $n > 22$ a permanência deste padrão se torna impossível. Resta então descobrir se o padrão é satisfeito até $n = 21$ ou não. Mesmo que o padrão não seja observado até este valor, ainda assim seria interessante tentar descobrir o quão perto do limite de Hamming esta família alcança.

Utilizando-se a mesma metodologia, encontramos os seguintes códigos.

Tabela 3.2: Códigos $((n, K, 2/2))$

Códigos $((n, K, 2/2))$	
n	K
6	8
7	16
8	32
9	64

Tabela 3.3: Códigos $((n, K, 3/2))$

Códigos $((n, K, 3/2))$	
n	K
7	2
8	4
9	8
10	16

Tabela 3.4: Códigos $((n, K, 4/2))$

Códigos $((n, K, 4/2))$	
n	K
9	4
10	8
11	8
12	32

3.7 Considerações finais

Na Seção 3.1, demonstramos para qudits, que um grupo estabilizador S de ordem $|S|$ estabiliza um subespaço de $\mathcal{H}_d^n$ de dimensão $\frac{d^n}{|S|}$. Apesar de já existir uma demonstração deste resultado, criamos uma que generaliza a demonstração sobre qubits contida em Nielsen e Chuang (2000) e faz uso da matriz verificadora

da Definição 3 e da interpretação da matriz $R(\mathbb{S})\Lambda$ como um homomorfismo de $\mathbb{Z}_d$-módulos.

Na Seção 3.2 demonstramos que todo código CWS sobre qupits é equivalente à um código CWS no formato padrão. Apesar de algumas referências fazerem menção a esta demonstração, não a achamos na literatura e optamos então por fazer uma que também generaliza a demonstração sobre qubits e que também faz uso da matriz verificadora sobre os geradores do grupo estabilizador $R(\mathbb{S})$ e das portas generalizadas descritas em Hostens et al. (2005).

Na Seção 3.3, demonstramos o resultado que permite a busca por bons códigos CWS tendo por base códigos clássicos que corrijam um conjunto determinado de erros. Usamos a demonstração usual encontrada na literatura.

Na Seção 3.4 utilizamos novamente a matriz verificadora $R(\mathbb{S})$ e a interpretação da matriz $R(\mathbb{S})\Lambda$ como um homomorfismo entre $\mathbb{Z}_d$-módulos para demonstrar o Teorema 10 que generaliza os resultados contidos nos Corolários (4 e 5). Estes últimos, resultados aceitos na literatura, mas difíceis de se encontrar para qudits.

Na Seção 3.5, descrevemos para qudits, os algoritmos necessários para se encontrar bons códigos quânticos do tipo CWS. Estes estão descritos em Chuang et al. (2009) mas apenas para qubits.

Na Seção 3.6, mostramos para qubits, alguns novos códigos CWS assimétricos que foram descobertos usando os algoritmos da Seção 3.5.

Capítulo 4

Observáveis para identificação de erros em códigos CWS binários

Neste capítulo, estabelecemos uma condição para a existência de observáveis que não são operadores de Pauli mas podem ser usados como observáveis de medida para códigos CWS e que podem ser escritos em termos dos geradores do grupo estabilizador associado ao código CWS. Também descrevemos um procedimento para achar estes observáveis. Este procedimento é especialmente útil para códigos CWS que são "próximos" aos códigos estabilizadores. Esta noção de proximidade será discutida mais adiante.

Poucos artigos discutem métodos de decodificação para códigos CWS; a principal exceção é o trabalho de Li et al. (2010), que descreve um método geral baseado numa álgebra de medidas complexa, exigindo a definição de uma nova estrutura chamada de códigos USt (Union-Stabilizers Codes), primeiramente descrita em Grassl e Rötteler (2008a). Neste capítulo, descrevemos um procedimento para achar um conjunto alternativo de observáveis que podem ser usados para detecção dos erros. Estes são mais simples e quando suficientes para identificação dos erros, reduz o número de medidas necessárias.

4.1 Observáveis para identificação de erros em códigos quânticos

Nesta seção explicamos de forma geral como a identificação dos erros em um código quântico pode ser feita, isto é, quais observáveis podemos usar para iden-

tificar o erro ocorrido e assim tentar corrigí-lo. Depois explicamos, para códigos CWS, o ganho que medir com os observáveis do procedimento usado em Li et al. (2010) fornece quando comparado ao procedimento geral. Depois explicamos brevemente os observáveis que usamos para medida, discutindo algumas ideias que serão usadas no trabalho. Diferentemente do conjunto de observáveis descritos em Li et al. (2010) que sempre conseguem identificar o erro, nosso conjunto de observáveis nem sempre é suficiente para identificar o erro em um código CWS, mas quando é, a complexidade do procedimento de identificação do erro é feito de forma mais eficiente.

De acordo com Li et al. (2010), dado um código quântico $\mathcal{Q}$ e um conjunto de erros corrigíveis $\epsilon = \{E\}$, podemos determinar um conjunto suficiente de observáveis para detectar o erro ocorrido utilizando o seguinte procedimento:

(1) Considere $\{|w_i\rangle\}_{i=1}^{K}$ uma base ortonormal para o código $\mathcal{Q}$. Primeiramente construímos o projetor $P_{\mathcal{Q}}$ sobre o código fazendo:

$$P_{\mathcal{Q}} = \sum_{i=1}^{K} |w_i\rangle\langle w_i|;$$

(2) A partir deste projetor, construímos o observável

$$M_{\mathcal{Q}} = 2P_{\mathcal{Q}} - I.$$

Este observável mede 1 se o estado pertence ao código e -1 caso contrário; portanto é capaz de detectar os erros em ϵ, mas não é capaz de identificá-los.

(3) Finalmente, para construir nosso conjunto de observáveis capazes de identificar os erros, fazemos para cada erro de Pauli $E \in \epsilon$ de classes de degenerescência diferentes,

$$M_E = EM_{\mathcal{Q}}E^{\dagger}.$$

De acordo com o descrito, a complexidade do procedimento de identificação

dos erros depende da complexidade de realizar a medida com o observável $M_{\mathcal{Q}}$ e da quantidade de classes de degenerescência distintas considerando os erros em ϵ. Como um código de distância d pode corrigir erros em até $t = [(d-1)/2]$ qubits, a quantidade de erros de Pauli distintos em ϵ é

$$B(n,t) = \sum_{i=0}^{t} \begin{pmatrix} n \\ i \end{pmatrix} 3^i.$$

Para códigos CWS, segundo Li et al. (2010), a complexidade ao medir com o observável $M_{\mathcal{Q}}$ é $(1+K)O(n^2)$, portanto se o código é não degenerado, isto é, a quantidade de classes de degenerescência diferentes dos erros é exatamente a quantidade de erros em ϵ, a complexidade total do procedimento de medida será

$$B(n,t)(1+K)O(n^2).$$

Na referência Li et al. (2010), para códigos CWS gerais, conseguiu-se um procedimento de identificação dos erros cuja complexidade é

$$\left[\begin{pmatrix} n \\ i \end{pmatrix} + 2t - 1 \right] 2K(n^2+n).$$

Nesta referência, o maior ganho representa a quantidade total de medidas que precisam ser feitas. No caso geral eram $B(n,t)$ e para o método apresentado em Li et al. (2010) é $N(n,t) = \left[\binom{n}{t} + 2t - 1\right]$. Ainda assim, para t e K grandes, o método ainda não é eficiente.

Nosso método tem como primeiro resultado analisar quais operadores de Pauli podem ser usados como observáveis para códigos CWS. Seja S o grupo estabilizador e W o conjunto de *operadores-palavras*. Se $g \in N_S(W)$, isto é, se g é um elemento do normalizador de W em S, então g pode ser usado como um

operador Pauli de medida. Isto segue das igualdades

$$gE_iW_j|\psi\rangle = m_iE_igW_j|\psi\rangle = m_iE_iW_jg|\psi\rangle = m_iE_iW_j|\psi\rangle,$$

onde $m_i = \pm 1$. A partir da expressão anterior, segue-se que $E_iW_j|\psi\rangle$ pertence ao auto-espaço associado ao autovalor m_i de g, então não há perda de informação após a medida. Quando um código CWS é um código estabilizador, o procedimento de decodificação usa um conjunto gerador de $N_S(W)$ como observáveis e o número de geradores é $n - \log_2(K)$. Se o código CWS não é um código estabilizador, podemos usar a ordem do grupo normalizador $N_S(W)$ como parâmetro para medir o quão perto o código CWS está de ser um código estabilizador. Se a ordem é 1 (no caso $N_S(W) = \{I\}$), o código CWS está longe de ser estabilizador e podemos usar apenas observáveis que não são operadores de Pauli no procedimento de decodificação.

Se o código CWS é também estabilizador, utilizamos apenas operadores de Pauli para identificar erros. No caso geral, precisamos completar o conjunto de observáveis com operadores que não são operadores de Pauli. Neste capítulo, ainda estabelecemos resultados sobre a existência e forma de observáveis de medida para códigos CWS que pertencem a álgebra de grupo sobre $\mathbb{R}$ gerada por S, $\mathbb{R}[S]$.

4.2 Caracterização dos observáveis do tipo-4

Um operador $A \in \mathbb{R}[S]$ pode ser escrito como

$$A = \sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}} \mathcal{S}^{\mathbf{V}},$$

em que usamos a notação $\mathcal{S}^{\mathbf{V}}$ para representar um elemento de $S = \langle s_1, \ldots, s_n \rangle$ da forma

$$\mathcal{S}^{\mathbf{V}} = s_1^{v_1} \cdots s_n^{v_n},$$

onde $\mathbf{V} = (v_i, \ldots, v_n)$ é um vetor binário. Nos vamos definir um "tipo" ao operador A e função do número de coeficientes $\alpha_{\mathbf{V}}$ não nulos.

Definição 6. *Um observável do tipo-i é um operador $A \in \mathbb{R}[S]$ que satisfaz $A^2 = I$ e é exatamente uma combinação linear de i diferentes elementos de S.*

Note que esta definição faz sentido por que o grupo S é um subconjunto de uma base para o espaço de Hilbert $\mathcal{H}^n$, e logo $A = \sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}} \mathcal{S}^{\mathbf{V}}$ é escrito de forma única.

Observáveis do tipo-1 são operadores de Pauli. Não há observáveis do tipo-2, porque se $A = \alpha_1 \mathcal{S}^{\mathbf{U}_1} + \alpha_2 \mathcal{S}^{\mathbf{U}_2}$ com $\mathbf{U}_1 \neq \mathbf{U}_2$ e α_1, α_2 diferentes de 0, então

$$A^2 = (\alpha_1^2 + \alpha_2^2) I + 2\alpha_1 \alpha_2 \mathcal{S}^{\mathbf{U}_1 + \mathbf{U}_2}$$

não pode ser igual a I. De forma análoga, podemos mostrar que não há observáveis do tipo-3. Neste trabalho consideraremos apenas operadores do tipo-4.

Se um operador unitário A é um observável, então $A^2 = I$. Como estamos lidando com observáveis em $\mathbb{R}[S]$, temos as seguintes proposições:

Proposição 2. *Sejam S o grupo estabilizador de um código CWS na forma padrão e $A = \sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}} \mathcal{S}^{\mathbf{V}}$ um elemento de $\mathbb{R}[S]$. Então $A^2 = I$ se e somente se*

$$\sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}}^2 = 1 \ e \ \sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}} \alpha_{\mathbf{V}+\mathbf{U}} = 0, \forall \mathbf{U} \in \mathbb{F}_2^n \setminus \{0\}. \tag{4.1}$$

Demonstração. Tome

$$A^2 = \sum_{\mathbf{V} \in \mathbb{F}_2^n} \alpha_{\mathbf{V}}^2 I + \sum_{\mathbf{V} \neq \mathbf{V}'} \alpha_{\mathbf{V}} \alpha_{\mathbf{V}'} \mathcal{S}^{\mathbf{V}} \mathcal{S}^{\mathbf{V}'}.$$

Todos os termos $\mathcal{S}^{\mathbf{U}} \in S \setminus \{I\}$ estão presentes no segundo somatório, cada um tantas vezes quanto $\mathbf{V} + \mathbf{V}' = \mathbf{U}$, isto é, 2^n. Então, podemos reescrever esta

equação como

$$\begin{aligned} A^2 &= \sum_{\mathbf{V}\in\mathbb{F}_2^n} \alpha_{\mathbf{V}}^2 I + \sum_{\mathbf{U}\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\mathbf{V}+\mathbf{V}'=\mathbf{U}} \alpha_{\mathbf{V}}\alpha_{\mathbf{V}'}\mathcal{S}^{\mathbf{U}} \\ &= \sum_{\mathbf{V}\in\mathbb{F}_2^n} \alpha_{\mathbf{V}}^2 I + \sum_{\mathbf{U}\in\mathbb{F}_2^n\setminus\{0\}} \mathcal{S}^{\mathbf{U}} \sum_{\mathbf{V}\in\mathbb{F}_2^n} \alpha_{\mathbf{V}}\alpha_{\mathbf{V}+\mathbf{U}}. \end{aligned}$$

donde segue o resultado (4.1). □

Os Observáveis do tipo-4 podem ser restringidos pelo teorema que segue.

Teorema 12. *A é um operador do tipo-4 se e somente se*

$$A = \pm\frac{\mathcal{S}^{\mathbf{V}}}{2}\left(-I + \mathcal{S}^{\mathbf{V}_1} + \mathcal{S}^{\mathbf{V}_2} + \mathcal{S}^{\mathbf{V}_1+\mathbf{V}_2}\right) \tag{4.2}$$

com $\mathbf{V}_1 \neq \mathbf{V}_2 \in \mathbb{F}_2^n \setminus \{0\}$ *e* $\mathbf{V} \in \mathbb{F}_2^n$.

Demonstração. Se A é dado pela equação (4.2), então é simples verificar que $A^2 = I$. logo, A é um observável do tipo-4.

Reciprocamente, tome um observável do tipo-4 $A = \alpha_1\mathcal{S}^{\mathbf{U}_1}+\alpha_2\mathcal{S}^{\mathbf{U}_2}+\alpha_3\mathcal{S}^{\mathbf{U}_3}+\alpha_4\mathcal{S}^{\mathbf{U}_4}$. Temos:

$$\begin{aligned} A^2 &= \left(\sum_{i=1}^{4}\alpha_i^2\right) I + 2\alpha_1\alpha_2\mathcal{S}^{\mathbf{U}_1+\mathbf{U}_2} + 2\alpha_1\alpha_3\mathcal{S}^{\mathbf{U}_1+\mathbf{U}_3} + 2\alpha_1\alpha_4\mathcal{S}^{\mathbf{U}_1+\mathbf{U}_4} + \\ &\quad 2\alpha_2\alpha_3\mathcal{S}^{\mathbf{U}_2+\mathbf{U}_3} + 2\alpha_2\alpha_4\mathcal{S}^{\mathbf{U}_2+\mathbf{U}_4} + 2\alpha_3\alpha_4\mathcal{S}^{\mathbf{U}_3+\mathbf{U}_4}. \end{aligned}$$

os α's não são zero, logo, $A^2 = I$ implica que

$$\sum_{i=1}^{4}\alpha_i^2 = 1$$

e a soma dos últimos 6 termos é zero, o que implica que $\mathbf{U}_1 + \mathbf{U}_2 = \mathbf{U}_3 + \mathbf{U}_4$, $\mathbf{U}_1 + \mathbf{U}_3 = \mathbf{U}_2 + \mathbf{U}_4$ e $\mathbf{U}_1 + \mathbf{U}_4 = \mathbf{U}_2 + \mathbf{U}_3$.

Podemos reescrever A tomando $\mathbf{V} = \mathbf{U}_1$, $\mathbf{V}_1 = \mathbf{U}_1 + \mathbf{U}_2$ e $\mathbf{V}_2 = \mathbf{U}_1 + \mathbf{U}_3$,

então $\mathbf{V}_1 + \mathbf{V}_2 = \mathbf{U}_1 + \mathbf{U}_4$ e

$$A = \frac{\mathcal{S}^{\mathbf{V}}}{2}\left(\alpha_1 I + \alpha_2 \mathcal{S}^{\mathbf{V}_1} + \alpha_3 \mathcal{S}^{\mathbf{V}_2} + \alpha_4 \mathcal{S}^{\mathbf{V}_1+\mathbf{V}_2}\right).$$

Note que $\mathbf{V}_1 \neq \mathbf{V}_2$ e $\mathbf{V}_1 \neq 0 \neq \mathbf{V}_2$ porque se $i \neq j$, $\mathbf{U}_i \neq \mathbf{U}_j$. As soluções obedecendo as restrições (4.1)pertencem ao conjunto

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \ \pm\tfrac{1}{2}\{\ \ (-1,1,1,1),(1,-1,1,1),(1,1,-1,1),(1,1,1,-1)\}.$$

As últimas três soluções podem ser obtidas da primeira tomando $\mathcal{S}^{\mathbf{V}_1}$, $\mathcal{S}^{\mathbf{V}_2}$ e $\mathcal{S}^{\mathbf{V}_1+\mathbf{V}_2}$, respectivamente e absorvendo estes termos em $\mathcal{S}^{\mathbf{V}}$. □

4.3 Condições para a medida com observáveis do tipo-4

Agora vamos introduzir a seguinte notação:

$$\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)} = \frac{1}{2}\left(-I + \mathcal{S}^{\mathbf{V}_1} + \mathcal{S}^{\mathbf{V}_2} + \mathcal{S}^{\mathbf{V}_1+\mathbf{V}_2}\right). \tag{4.3}$$

Note que para qualquer $\mathbf{V}_1, \mathbf{V}_2 \in \mathbb{F}_2^n$, $\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ estabiliza $|\psi\rangle$. No próximo Lema, uma função $F : \mathcal{G}_n \mapsto \mathbb{F}_2^n$ que depende implicitamente de $\mathbf{V}_1$ e $\mathbf{V}_2$ é definida por

$$F(G) = \begin{cases} \mathbf{V}_1 + \mathbf{V}_2 & \text{se } G \text{ anti-comuta com } \mathcal{S}^{\mathbf{V}_1} \text{ e } \mathcal{S}^{\mathbf{V}_2}; \\ \mathbf{V}_1 & \text{se } G \text{ anti-comuta apenas com } \mathcal{S}^{\mathbf{V}_2}; \\ \mathbf{V}_2 & \text{e } G \text{ anti-comuta apenas com } \mathcal{S}^{\mathbf{V}_1}; \\ \mathbf{0} & \text{comuta com ambos.} \end{cases} \tag{4.4}$$

Lema 4. *Seja G um operador de Pauli. Se G não comuta com $\mathcal{S}^{\mathbf{V}_1}$ ou $\mathcal{S}^{\mathbf{V}_2}$, então $\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}G = -\mathcal{S}^{F(G)}G\,\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)} = -G\,\mathcal{S}^{F(G)}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)} = -G\,\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}\mathcal{S}^{F(G)}$.*

Demonstração. A verificação é imediata. □

As condições que garantem que possamos usar um operador A como um observável para um código CWS estão intimamente relacionadas com as condições

que garantem que A estabilize o código.

Proposição 3. *Seja* $\mathbf{C}_i = (c_i^1, \ldots, c_i^n)$, $i = 1, \ldots, K$ *as palavras clássicas de um código CWS no formato padrão. Sejam* $\mathbf{V}_1$, $\mathbf{V}_2$, $\mathbf{V} \in \mathbb{F}_2^n$ *e* $p_i = \langle \mathbf{C}_i, \mathbf{V}_1 \rangle \vee \langle \mathbf{C}_i, \mathbf{V}_2 \rangle$, *onde* $\vee$ *é o operador de disjunção lógica. Então, um operador do tipo-4* A *estabiliza o código se e somente se* $A = \mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)}$ *e* $\langle \mathbf{C}_i, \mathbf{V} \rangle = p_i$ *para todo* i.

Demonstração. Suponha que $A = \mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)}$ e $\langle \mathbf{C}_i, \mathbf{V} \rangle = p_i$ para todo i. então,

(1) se $Z^{\mathbf{C}_i}$ comuta com $\mathcal{S}^{\mathbf{V}_1}$ e $\mathcal{S}^{\mathbf{V}_2}$, então $Z^{\mathbf{C}_i}$ também comuta com $\mathcal{S}^{\mathbf{V}}$ and $\mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)}$, isto é,

$$\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} Z^{\mathbf{C}_i} |\psi\rangle = Z^{\mathbf{C}_i} |\psi\rangle,$$

(2) se $Z^{\mathbf{C}_i}$ não comuta com $\mathcal{S}^{\mathbf{V}_1}$ ou $\mathcal{S}^{\mathbf{V}_2}$, então $Z^{\mathbf{C}_i}$ anti-comuta com $\mathcal{S}^{\mathbf{V}}$. assim, o Lema 4 implica que

$$\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} Z^{\mathbf{C}_i} |\psi\rangle = \mathcal{S}^{\mathbf{V}} (-\mathcal{S}^{F(Z^{\mathbf{C}_i})}) Z^{\mathbf{C}_i} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} |\psi\rangle = -\mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} \mathcal{S}^{F(Z^{\mathbf{C}_i})} |\psi\rangle =$$
$$- \mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} |\psi\rangle = Z^{\mathbf{C}_i} \mathcal{S}^{\mathbf{V}} |\psi\rangle = Z^{\mathbf{C}_i} |\psi\rangle.$$

em qualquer caso, A estabiliza o código.

Reciprocamente, seja A um observável do tipo-4. Pelo Teorema 12, $A = \pm \mathcal{S}^{\mathbf{V}} \mathcal{S}^{\{\mathbf{V}_1, \mathbf{V}_2\}}$, donde, $A|\psi\rangle = \pm \mathcal{S}^{\mathbf{V}} \mathcal{S}^{\{\mathbf{V}_1, \mathbf{V}_2\}} |\psi\rangle = \pm |\psi\rangle$. Por hipótese, A estabiliza o código, assim, $A = \mathcal{S}^{\mathbf{V}} \mathcal{S}^{\{\mathbf{V}_1, \mathbf{V}_2\}}$. logo, para estabilizar o código, temos:

(1) Se um operador-palavra $W_i = Z^{\mathbf{C}_i}$ comuta com $\mathcal{S}^{\mathbf{V}_1}$ e $\mathcal{S}^{\mathbf{V}_2}$ então

$$\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} Z^{\mathbf{C}_i} |\psi\rangle = \mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} |\psi\rangle = \mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} |\psi\rangle = Z^{\mathbf{C}_i} |\psi\rangle.$$

A última igualdade implica que $\mathcal{S}^{\mathbf{V}}$ comuta com $Z^{\mathbf{C}_i}$. logo, $\langle \mathbf{C}_i, \mathbf{V} \rangle = 0$.

(2) Se $W_i = Z^{\mathbf{C}_i}$ não comuta com $\mathcal{S}^{\mathbf{V}_1}$ ou $\mathcal{S}^{\mathbf{V}_2}$, o Lema 4 implica que

$$\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} Z^{\mathbf{C}_i} |\psi\rangle = \mathcal{S}^{\mathbf{V}} (-\mathcal{S}^{F(Z^{\mathbf{C}_i})}) Z^{\mathbf{C}_i} \mathcal{S}^{(\mathbf{V}_1, \mathbf{V}_2)} |\psi\rangle = -\mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} \mathcal{S}^{F(Z^{\mathbf{C}_i})} |\psi\rangle$$
$$= -\mathcal{S}^{\mathbf{V}} Z^{\mathbf{C}_i} |\psi\rangle = Z^{\mathbf{C}_i} |\psi\rangle.$$

A última igualdade implica que $\mathcal{S}^{\mathbf{V}}$ anti-comuta com $Z^{\mathbf{C}_i}$, e assim, $\langle \mathbf{C}_i, \mathbf{V} \rangle = 1$.

□

Tomando $\mathbf{V} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ e $p_i = \langle \mathbf{C}_i, \mathbf{V}_1 \rangle \vee \langle \mathbf{C}_i, \mathbf{V}_2 \rangle$, as equações $\langle \mathbf{C}_i, \mathbf{V} \rangle = p_i$ podem ser colocadas em notação matricial

$$C \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} p_1 \\ \vdots \\ p_k \end{bmatrix}, \tag{4.5}$$

em que C é a matriz de todas as palavras clássicas.

$$C = \begin{bmatrix} c_1^1 & \ldots & c_1^n \\ \vdots & \vdots & \vdots \\ c_K^1 & \ldots & c_K^n \end{bmatrix}. \tag{4.6}$$

Dado um conjunto de erros corrigíveis de um código CWS, se estes podem ser identificados medindo-se com um conjunto de observáveis sem que haja perda de informação, independentemente de quais erros ocorreram, então chamaremos ambos estes observáveis de **Operadores de Decodificação** ou **Observáveis de Decodificação**.

Um operador A pode então ser usado como Operador de Decodificação se a informação codificada não é perdida após a medida com A. Temos que garantir que para cada i e para todo j, $E_i W_j |\psi\rangle$ pertença ao auto-espaço de $E_i W_j$ associado aos autovalores 1 ou -1, isto é,

$$A E_i W_j |\psi\rangle = E_i W_j |\psi\rangle, \ \forall j$$

ou

$$A E_i W_j |\psi\rangle = -E_i W_j |\psi\rangle, \ \forall j.$$

Tendo isto em vista, temos o seguinte teorema:

Teorema 13. *Seja $\mathcal{E} = \{E_i\}_{i=1}^{T}$ um conjunto de erros de Pauli corrigíveis de um código CWS no formato padrão, Então, um observável do tipo-4 $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ pode ser usado como operador de decodificação se e somente se para todo $i \in \{1,\ldots,T\}$ existe uma solução $\mathbf{V}_i'$ da Equação. (4.5) com $\mathbf{V} = \mathbf{V}_i' + F(E_i)$.*

Demonstração. Suponha que $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ satisfaz $\mathbf{V} = \mathbf{V}_i + F(E_i)$, para todo i, onde $\mathbf{V}_i$ é uma solução da equação (4.5). Tome $\mathcal{S}^{\mathbf{V}}E_i = m_iE_i\mathcal{S}^{\mathbf{V}}$, onde $m_i = \pm 1$. Então, pelo Lema 4 temos

(1) se E_i comuta com $\mathcal{S}^{\mathbf{V}_1}$ e $\mathcal{S}^{\mathbf{V}_2}$, então $F(E_i) = (0,\ldots,0)$ (4.4) e

$$\begin{aligned} AE_iW_j|\psi\rangle &= \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}E_iW_j|\psi\rangle = \mathcal{S}^{\mathbf{V}}E_i\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle \\ &= m_iE_i\mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle = m_iE_i\mathcal{S}^{\mathbf{V}+F(E_i)}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle \\ &= m_iE_i\mathcal{S}^{\mathbf{V}_i'}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle = m_iE_iW_j|\psi\rangle. \end{aligned}$$

A última igualdade é verdadeira porque $\mathcal{S}^{\mathbf{V}_i'}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ estabiliza o código.

(2) Se E_i não comuta com $\mathcal{S}^{\mathbf{V}_1}$ ou $\mathcal{S}^{\mathbf{V}_2}$, então

$$\begin{aligned} AE_iW_j|\psi\rangle &= \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}E_iW_j|\psi\rangle = -\mathcal{S}^{\mathbf{V}+F(E_i)}E_i\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle \\ &= -m_iE_i\mathcal{S}^{\mathbf{V}_i'}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle = -m_iE_iW_j|\psi\rangle. \end{aligned}$$

De novo, usamos que $\mathcal{S}^{\mathbf{V}_i'}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ estabiliza o código.

Reciprocamente, suponha que $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ pode ser usado como observável. Usando $\mathcal{S}^{\mathbf{V}}E_i = m_iE_i\mathcal{S}^{\mathbf{V}}$, onde $m_i = \pm 1$, e repetindo as operações de comutação, temos

(1) se E_i comuta com ambos $\mathcal{S}^{\mathbf{V}_1}$ e $\mathcal{S}^{\mathbf{V}_2}$, então

$$AE_iW_j|\psi\rangle = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}E_iW_j|\psi\rangle = m_iE_i\mathcal{S}^{\mathbf{V}+F(E_i)}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle$$

onde $F(E_i) = (0,\ldots,0)$.

(2) Se E_i não comuta com $\mathcal{S}^{\mathbf{V}_1}$ ou $\mathcal{S}^{\mathbf{V}_2}$, então

$$AE_iW_j|\psi\rangle = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}E_iW_j|\psi\rangle = -m_iE_i\mathcal{S}^{\mathbf{V}+F(E_i)}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}W_j|\psi\rangle.$$

Estamos assumindo que A pode ser usado como observável, em ambos os casos temos

$$AE_iW_j|\psi\rangle = E_iW_j|\psi\rangle,\ \forall j$$

ou

$$AE_iW_j|\psi\rangle = -E_iW_j|\psi\rangle,\ \forall j.$$

isto implica que $\mathcal{S}^{\mathbf{V}+F(E_i)}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ estabiliza o código para todo i, e pela Proposição 3 existe uma solução $\mathbf{V}_i'$ para a Equação (4.5) tal que $\mathbf{V} + F(E_i) = \mathbf{V}_i'$ para todo i. □

O Teorema 13 nos permite fazer uma busca exaustiva por observáveis do tipo-4, usando a expressão $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$. Temos que considerar todos os pares $(\mathcal{S}^{\mathbf{V}_1}, \mathcal{S}^{\mathbf{V}_2})$ em S tal que $\mathbf{V}_1 \neq \mathbf{V}_2$ e procurar por soluções da equação (4.5) para cada par. Este processo pode ser custoso. O próximo corolário fornece uma forma mais eficiente de procurar estes observáveis restringindo o espaço de busca a elementos em $N_S(\mathcal{E})$, mas, neste caso, algumas soluções podem não ser consideradas.

Corolário 6. *Sejam $\mathcal{E} = \{E_i\}_{i=1}^T$ um conjunto de erros corrigíveis de um código CWS no formato padrão e $N_S(\mathcal{E})$ o normalizador de $\mathcal{E}$ em S. Se $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ é um observável do tipo-4,onde $\mathcal{S}^{\mathbf{V}_1}, \mathcal{S}^{\mathbf{V}_2} \in N_S(\mathcal{E})$ e $\mathbf{V}$ é uma solução da Equação* (4.5)*, então A pode ser usado como observável para o código CWS.*

Demonstração. Se ambos $\mathcal{S}^{\mathbf{V}_1}$ e $\mathcal{S}^{\mathbf{V}_2}$ estão em $N_S(\mathcal{E})$, então $F(E_i) = (0, \ldots, 0)$ para todo i, e o Teorema 13 implica que $\mathbf{V} = \mathbf{V}_i$, onde $\mathbf{V}_i$ é uma solução da Equação (4.5). □

4.4 Procedimento para determinar os operadores de medida

O Corolário 6 auxilia na construção de um procedimento para achar observáveis do tipo-4.

Procedimento 1. *Sejam $\mathcal{E} = \{E_i\}$ o conjunto de erros corrigíveis e $W = \{W_j\}$ o conjunto de operadores-palavras.*

(1) Ache geradores independentes de $N_S(W)$;

(2) Meça com estes geradores. Para cada síndrome, existe um conjunto $\mathcal{E}'$, contido em $\mathcal{E}$, de erros que não foram detectados pelas medidas;

(3) Para cada $\mathcal{E}'$ faça

(a) Ache todos os elementos do grupo $N_S(\mathcal{E}')$;

(b) Tome pares $(\mathcal{S}^{\mathbf{V}_1}, \mathcal{S}^{\mathbf{V}_2})$ em $N_S(\mathcal{E}')$ tal que $\mathbf{V}_1 \neq \mathbf{V}_2$ até achar uma solução $\mathbf{V}$ da equação (4.5) que distingue alguns erros em $\mathcal{E}'$. Este passo deve dividir $\mathcal{E}'$ em subconjuntos menores;

(c) Repita os passos (a) e (b) com os subconjuntos menores tantas vezes necessárias até que possamos distinguir os erros de Pauli em $\mathcal{E}'$.

Para achar geradores de $N_S(W)$ no passo 1, usamos a relação de comutação

$$Z^{\mathbf{C}_i}\mathcal{S}^{\mathbf{O}_j} = (-1)^{\langle \mathbf{C}_i, \mathbf{O}_j \rangle}\mathcal{S}^{\mathbf{O}_j}Z^{\mathbf{C}_i}, \tag{4.7}$$

para mostrar que $\mathcal{S}^{\mathbf{O}_j} \in N_S(W)$ se e somente se $\langle \mathbf{C}_i, \mathbf{O}_j \rangle = 0$ para todo i. Isto implica que $\mathbf{O}_j$ está no núcleo da transformação linear descrita pela matriz C na equação (4.6). Os geradores independentes de $N_S(W)$ são obtidos a partir de uma base para o núcleo de C.

No passo 3, para achar todos os elementos em $N_S(\mathcal{E}')$, convertemos os erros em $\mathcal{E}'$ para palavras clássicas usando a função Cl_S e construímos uma nova matriz. O núcleo desta matriz tem correspondência um para um com os elementos

de $N_S(\mathcal{E}')$. Cada par $(\mathcal{S}^{\mathbf{V}_1}, \mathcal{S}^{\mathbf{V}_2})$ e uma solução $\mathbf{V}$ da equação (4.5) gera um observável do tipo-4 para erros em $\mathcal{E}'$. Para aumentar a eficiência do procedimento, podemos então testar quando cada observável encontrado pode ser utilizado nos outros conjuntos $\mathcal{E}'$ gerados no passo 2.

4.5 Implementação das medidas com observáveis do tipo-4

Usando uma notação parecida a $\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ na equação 4.3, considere o seguinte operador sobre a matriz de Pauli X ao invés de $\mathcal{S}$:

$$\mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)} = \frac{1}{2}\left(-I + X^{\mathbf{V}_1} + X^{\mathbf{V}_2} + X^{\mathbf{V}_1+\mathbf{V}_2}\right).$$

Se $\mathbf{V}_1 = (1,0)$ e $\mathbf{V}_2 = (0,1)$, no caso de 2 qubits, $\mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)}$ é o operador de Grover, dado por $2|\psi\rangle\langle\psi| - I$ onde $|\psi\rangle = \frac{1}{2}\sum_{i=0}^{3}|i\rangle$. O circuito para este operador é amplamente conhecido Grover (1996); Nielsen e Chuang (2000).

Seja $\mathbb{E}$ o conjunto das arestas do grafo representado pela matriz de adjacência M, e defina

$$\mathcal{U} = \prod_{(i,j)\in\mathbb{E}} P_{(i,j)},$$

em que $P_{(i,j)}$ é a porta Z controlada atuando nos *qubits* i e j. O operador $\mathcal{U}$ é usado no procedimento de codificação dos códigos CWS Cross et al. (2009)

Usando as fórmulas básicas do formalismo dos estabilizadores, obtemos

$$\mathcal{U}X^{\mathbf{V}}\mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)}\mathcal{U}^{\dagger} = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}. \tag{4.8}$$

Também facilmente verifica-se que $\mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)} = \mathcal{X}^{(\mathbf{V}_2,\mathbf{V}_1)}$ e

$$\mathcal{X}^{(\mathbf{V},\mathbf{W}_1+\mathbf{W}_2)} = X^{\mathbf{V}}\mathcal{X}^{(\mathbf{V},\mathbf{W}_1)}\mathcal{X}^{(\mathbf{V},\mathbf{W}_2)}.$$

A fórmula anterior pode ser estendida para mais termos, gerando-se

$$\mathcal{X}^{(\mathbf{V},\mathbf{W}_1+\cdots+\mathbf{W}_n)} = X^{(n-1)\mathbf{V}} \prod_{j=1}^{n} \mathcal{X}^{(\mathbf{V},\mathbf{W}_j)}. \tag{4.9}$$

Expandindo $\mathbf{V}_1$ e $\mathbf{V}_2$ na base canônica e_i de $\mathbb{F}_2^n$, obtemos $\mathbf{V}_1 = \sum_{i=1}^{n} v_i^{(1)} e_i$ e $\mathbf{V}_2 = \sum_{i=1}^{n} v_i^{(2)} e_i$, em que $v_i^{(1)}$ e $v_i^{(2)}$ são coeficientes binários. Usando duas vezes a equação (4.9), obtemos

$$X^{\mathbf{V}} \mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)} = X^{\mathbf{V}+(n-1)\mathbf{V}_1} \prod_{j=1}^{n} X^{(n-1)v_j^{(2)} e_j} \prod_{i=1}^{n} \mathcal{X}^{(v_i^{(1)} e_i, v_j^{(2)} e_j)}. \tag{4.10}$$

Se $v_i^{(1)} \neq 0$ e $v_j^{(2)} \neq 0$, o termo $\mathcal{X}^{(v_i^{(1)} e_i, v_j^{(2)} e_j)} = \mathcal{X}^{(e_i,e_j)}$ é o operador de grover atuando nos qubits i e j. O circuito neste caso é conhecido. Se ambos $v_i^{(1)}$ e $v_j^{(2)}$ são zero, este termo é a identidade e se apenas um dos coeficientes é 0, o termo é a matriz de Pauli X atuando nos qubits i ou j. Em qualquer caso, podemos construir um circuito para $\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$.

Vamos calcular a complexidade do circuito de $\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$. O número de portas de $\mathcal{X}^{(v_i^{(1)} e_i, v_j^{(2)} e_j)}$ é, no pior caso, igual ao número de portas do operador de Grover, que é fixo. O número de portas no circuito de $X^{\mathbf{V}}$ é $O(n)$. Como i, j percorrem de 1 a n, a complexidade do circuito de $X^{\mathbf{V}}$ é $O(n)$. Como i, j percorrem de 1 até n, a complexidade do circuito de $X^{\mathbf{V}} \mathcal{X}^{(\mathbf{V}_1,\mathbf{V}_2)}$ é $O(n^2)$. A complexidade total do circuito para $\mathcal{U}$ também é $O(n^2)$ Cross et al. (2009). A complexidade total do circuito para $\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ é $O(n^2)$. A mesma análise de complexidade se aplica ao se medir com estes observáveis.

Para calcular a complexidade total do procedimento de decodificação, precisamos estimar o número de medidas necessárias para achar os erros. Uma estimativa para este número vem dos detalhes do Corolário 6 e procedimento 1.

Suponha que temos um conjunto completo de operadores de decodificação satisfazendo ao Corolário 6. Seja $\mathcal{S}^{\mathbf{V}} \mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ um destes observáveis. Seja s a síndrome de um erro E quando usamos o observável de Pauli $\mathcal{S}^{\mathbf{V}}$, isto é, $s = \pm 1$

se E e $\mathcal{S}^{\mathbf{V}}$ respectivamente comuta ou anti-comuta. Então temos

$$\mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}E = \mathcal{S}^{\mathbf{V}}E\,\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)} = s\,E\,\mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}.$$

Como $\mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ estabiliza o código, concluimos que a síndrome de $\mathcal{S}^{\mathbf{V}}$ $\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ é na realidade obtida da síndrome de $\mathcal{S}^{\mathbf{V}} \in S$. Como o número de geradores independentes de S é n, o número de medidas, tanto com operadores de Pauli quanto com operadores do tipo-4, não podem ser maiores que n, e a complexidade total das medidas no procedimento de decodificação é $O(n^3)$.

4.6 Exemplos

Nesta seção, empregamos o procedimento 1 para achar os observáveis para os códigos $((9, 12, 3))$ e $((10, 20, 3))$; o primeiro é baseado no grafo cíclico e o segundo no grafo bicíclico. Estes códigos foram descritos por Cross et al. (2009) e Hu et al. (2008).

Para o código $((10, 20, 3))$, temos os geradores

$$\begin{aligned} s_1 &= XZIIZZIIII & s_6 &= ZIIIIXZIIZ \\ s_2 &= ZXZIIIZIII & s_7 &= IZIIIZXZII \\ s_3 &= IZXZIIIZII & s_8 &= IIZIIIZXZI \\ s_4 &= IIZXZIIIZI & s_9 &= IIIZIIIZXZ \\ s_5 &= ZIIZXIIIIZ & s_{10} &= IIIIZZIIZX \end{aligned}$$

e palavras clássicas

0000000000	1001100100	1001101111	0101100000
0000101001	1100101101	0111011011	0111010000
1011011111	1110010110	1100000100	1101111110
1111000101	0101101011	0001111010	0010010010
0010111011	1011010100	0011000001	1110111111

No passo 1 do procedimento 1, temos que achar geradores para $N_S(W)$. Isto é feito achando uma base (O) para o núcleo da matriz C, descrita na equação (4.6). Neste exemplo, esta base é mostrada na Tabela 4.1. Então, os geradores de $N_S(W)$ são operadores de Pauli em $\mathcal{S}^{\mathbf{O}_1}$, $\mathcal{S}^{\mathbf{O}_2}$, $\mathcal{S}^{\mathbf{O}_3}$, $\mathcal{S}^{\mathbf{O}_4}$. No passo 2, são feitas as medidas com estes operadores. O resultado é mostrado nos sinais $\pm$ no topo das sub-tabelas da Figura 4.2, Por exemplo, se o resultado da medida é $+++-$, apenas dois erros de Pauli não foram detectados, Y_2 e Z_1. $\mathcal{E}'$ é $\{Y_2, Z_1\}$ neste caso.

Tabela 4.1: observáveis de Pauli ($\mathcal{S}^{\mathbf{O}_i}$) para o código ((10,20,3)).

$\mathbf{O}_1$	$\mathbf{O}_2$	$\mathbf{O}_3$	$\mathbf{O}_4$
0001110011	0010011001	0100111110	1000000100

Seguindo o passo 3 do procedimento 1, nós obtemos os primeiros observáveis do tipo-4, A_1 na Tabela 4.2, quando $\mathcal{E}' = \{Y_2, Z_1\}$. Estes são descritos por $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$ (veja Eq. (4.2)). Neste caso, a etapa (a) do passo 3 é usada apenas uma vez, porque o observável A_1 distingue todos os erros em em $\mathcal{E}'$. Note então que podemos verificar se A_1 pode ser usado para outros conjuntos $\mathcal{E}'$. Neste exemplo, A_1 pôde ser usado 4 vezes, como pode ser observado na Figura 4.2. O próximo conjunto será $\mathcal{E}' = \{X_4, Z_3\}$.

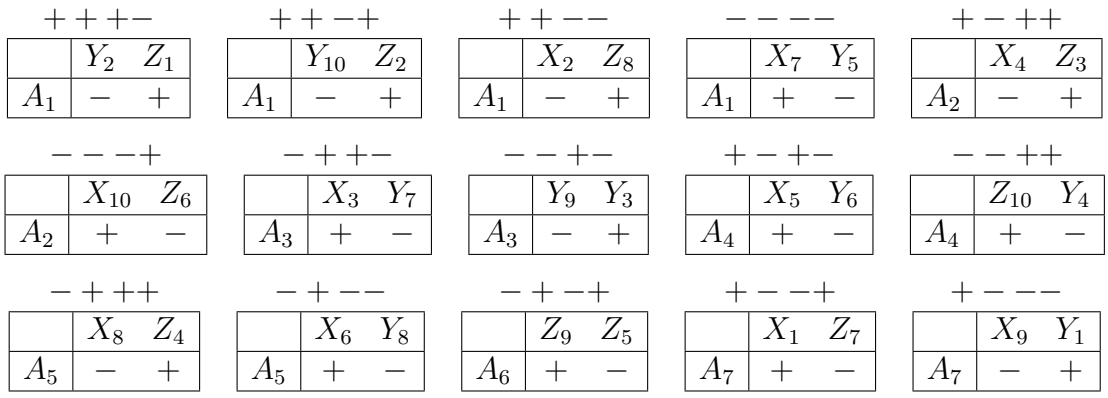
Tabela 4.2: Observáveis do tipo-4 para o código ((10,20,3)).

	$\mathbf{V}$	$\mathbf{V}_1$	$\mathbf{V}_2$
A_1	0000111001	0000100001	0001000011
A_2	0000111001	0000100010	0001000000
A_3	0000010001	0000000011	0000010010
A_4	0000110000	0000011000	0000100010
A_5	0000111001	0000011011	0000101011
A_6	0000111001	0000011000	0001000000
A_7	0000111001	0000110000	0010000010

No final, obtemos 7 observáveis do tipo-4 que estão listados na Tabela 4.2. A forma destes observáveis é dada pela expressão $\mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{V}_1,\mathbf{V}_2)}$, explicada na equação (4.2). Para decidir qual observável deve ser usado como medida, basta analisar a Figura 4.2. Note que para este código, é suficiente medir com apenas mais um observável do tipo-4. A síndrome $++++$ não foi considerada porque neste exemplo,

não existem erros associados a ela, apenas o operador identidade. A seguir, temos os resultados das medidas dos observáveis. Os sinais no topo de cada sub-tabela descrevem das medidas dos observáveis de Pauli da Tabela 4.1. As medidas dos operadores do tipo-4 estão condicionadas pelos resultados das medidas de Pauli.

Figura 4.1: Resultados das medidas dos observáveis para o código $((10, 20, 3))$.



O código $((9, 12, 3))$ tem seu grupo estabilizador S baseado num grafo cíclico com geradores $s_i = Z_{i-1}X_iZ_{i+1}$. As palavras clássicas são

000000000 100100100 010001100 110101000
000110001 100010101 011001010 111101110
001010011 101110111 011111111 111011011

De acordo com o procedimento já discutido, primeiramente medimos com três observáveis de Pauli

Tabela 4.3: Observáveis de Pauli ($\mathcal{S}^{\mathbf{O}_i}$) para o código ((9,12,3)).

O_1	O_2	O_3
000010001	001000010	010001000

Depois, achamos nove observáveis do tipo-4. Estes são descritos por $A = \mathcal{S}^{\mathbf{V}}\mathcal{S}^{(\mathbf{v}_1,\mathbf{v}_2)}$ (veja Eq. (4.2)).

O procedimento de medida está descrito na Tabela 4.2. Os sinais no topo de cada sub-tabela descrevem das medidas dos observáveis de Pauli da Tabela 4.4. As

Tabela 4.4: Observáveis do tipo-4 para o código ((9,12,3)).

$\mathbf{V}$	$\mathbf{V}_1$	$\mathbf{V}_2$
100000111	000000011	000001000
000100110	000000010	000011000
100101001	000000010	000001000
100101010	000000001	000001010
000100110	000000001	000001000
100001101	000000001	000000010
000100110	000001000	000010000
100001101	000000001	001000000
000100110	000000001	010000000

medidas dos operadores do tipo-4 estão condicionadas pelos resultados das medidas de Pauli.

Figura 4.2: Resultados das medidas dos observáveis para o código $((9, 12, 3))$

$+++$

	I	Z_7	Z_4	Z_1
A_1	$+$	$-$	$+$	$-$
A_3	$+$	$+$	$-$	$-$

$++-$

	X_5	X_3	Z_6	Z_2
A_6	$-$	$+$	$-$	$+$
A_7		$-$		$+$
A_9	$-$		$+$	

$+-+$

	X_9	X_2	Z_8	Z_3
A_5	$-$	$+$	$-$	$+$
A_6		$-$		$+$
A_8	$-$		$+$	

$+--$

	X_7	Y_7	Y_3	Y_2
A_4	$+$	$+$	$-$	$-$
A_5			$-$	$+$
A_8	$-$	$+$		

$-++$

	X_8	X_6	Z_9	Z_5
A_3	$-$	$+$	$-$	$+$
A_5		$-$		$+$
A_7	$-$		$+$	

$-++$

	X_1	Y_6	Y_5	Y_1
A_2	$+$	$-$	$-$	$+$
A_3	$-$			$+$
A_6		$+$	$-$	

$--+$

	X_4	Y_9	Y_8	Y_4
A_1	$+$	$-$	$-$	$+$
A_3	$+$			$-$
A_7		$-$	$+$	

Nem sempre conseguimos achar operadores do tipo-4 suficientes para efetuar a medida, por exemplo, para o código $((10, 18, 3))$ também presente em Cross et al. (2009), pode-se verificar que não há operadores deste tipo suficientes para se descobrir o erro.

4.7 Considerações finais

Na Seção 4.1, descrevemos tipos de observáveis que podemos usar para identificação dos erros em um código quântico geral e a complexidade do procedimento de medida com estes observáveis. Descrevemos também, especificamente para códigos CWS, o ganho em complexidade que os observáveis descritos em Li et al. (2010) possibilitam no procedimento de detecção e finalmente introduzimos algumas ideias a respeito do nosso conjunto de observáveis propostos para identificação dos erros.

Na Seção 4.2, definimos um operador que chamamos de observáveis do tipo-4 e caracterizamos algumas de suas propriedades.

Na Seção 4.3 apresentamos as principais contribuições, caracterizando, no Teorema 4.5 e no Corolário 6 quais as características que um observável do tipo-4 deve satisfazer para poder ser utilizado como observável de medida para códigos CWS.

Na Seção 4.4, descrevemos um algoritmo que busca observáveis para identificar os erros de um código CWS, tanto observáveis que são operadores de Pauli como observáveis do tipo-4.

Na Seção 4.5, descrevemos como funcionam as portas necessárias para implementar as medidas com os observáveis do tipo-4, mostrando que se o procedimento 1 encontra observáveis que são suficientes para determinar os erros, as medidas para que esta identificação seja feita são feitas de forma eficiente.

Na Seçao 4.6, descrevemos dois exemplos de códigos CWS explorando o uso dos observáveis do tipo-4. Nestes dois exemplos, apenas com operadores de Pauli e observáveis do tipo-4 foi possível identificar o erro.

Capítulo 5

Conclusão

Acreditamos que este trabalho contribuiu para o desenvolvimento da pesquisa na área de códigos quânticos de correção de erros de duas formas: a primeira foi no entendimento mais apurado da relação entre códigos quânticos do tipo CWS em sistemas de mais de um nível (qudits) e códigos estabilizadores; a segunda contribuição foi na eficiência na detecção dos erros em códigos CWS em sistemas de dois níveis (qubits).

Nos Capítulos 2 e 3 apresentamos as ferramentas necessárias para entender os resultados da tese. No Capítulo 4, apresentamos os códigos CWS. Neste capítulo, tratamos os códigos CWS em sua forma mais geral, sobre qudits, onde d pode assumir qualquer valor. Quando necessário, evidenciamos os resultados válidos apenas para qupits, quando d é primo, para qubits, quando $d = 2$ e quando o código CWS é baseado em um estado-grafo. Na literatura estes resultados não se encontram facilmente disponíveis, gerando as vezes confusão sobre quais resultados são válidos em cada caso. Além disto, apresentamos um novo resultado, contido no Teorema 10. Este resultado generaliza os resultados presentes na literatura que relacionam códigos estabilizadores com códigos CWS, que neste trabalho foram apresentados como Corolários do Teorema 10, respectivamente, o Corolário 4 e o Corolário 5. O resultado contido no Teorema 10 surge ao se explorar propriedades dos *operadores-palavras* $W = \{w_1, \ldots, w_K\}$de um código CWS, mais especificamente, surge ao se enxergar estes *operadores-palavras* através da estrutura de uma

matriz verificadora $R(W)$, como definido na Definição 3 e analisar a matriz $R(W)\Lambda$ como um homomorfismo entre $\mathbb{Z}_d$-módulos.

No Capítulo 5, apresentamos outro resultado desta tese. Baseado-nos principalmente nas ideias contidas em Yu et al. (2008) desenvolvemos uma caracterização geral de um tipo de operador que pode ser usado para detecção dos erros em um código CWS. Chamamos este operador de tipo-4, devido ao fato de ser a combinação linear de 4 operadores de Pauli presentes no grupo estabilizador S do código CWS. O Teorema 13 e o Corolário 6 caracterizam, dado um código CWS, quando um operador deste tipo pode ser usado como operador de medida para a detecção dos erros. Nem sempre é possível usar operadores deste tipo para identificar todos os erros que um código CWS é capaz de corrigir, mas segundo a caracterização contida no Corolário 6, quando isto é possível, sabendo quais operadores do tipo-4 usar, esta identificação é feita de forma eficiente. Portanto, dado um código CWS, é interessante descobrir se é possível ou não usar estes tipos de operadores para identificação de todos os erros que este código promete corrigir. A busca por estes operadores é descrita no procedimento 1. Este procedimento de busca em si não é eficiente, sendo também interessante descobrir formas de torná-lo mais eficiente em trabalhos futuros.

Referências Bibliográficas

D. Aharonov e M. Ben-or. Fault-tolerant quantum computation with constant error. páginas 176–188, 1997.

V. Arvind, P. P. Kurur, e K. R. Parthasarathy. Nonstabilizer quantum codes from abelian subgroups of the error group. 2002.

S. Beigi, I. Chuang, M. Grassl, P. Shor, e B. Zeng. Graph concatenation for quantum codes. **Journal of Mathematical Physics**, 52(2):022201, Fevereiro 2011.

P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. **Journal of Statistical Physics**, 22(5):563–591, Maio 1980. ISSN 0022-4715.

C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, e W. K. Wootters. Mixed-state entanglement and quantum error correction. **Phys. Rev. A**, 54(5):3824–3851, Nov 1996.

I. Burda. **Introduction to Quantum Computation**. Lightning Source Incorporated, 2005. ISBN 9781581124668.

A. R Calderbank, E. M. Rains, P. W. Shor, e N. J. A. Sloane. Quantum error correction via codes over gf(4), 1997.

A. R. Calderbank e P. W. Shor. Good quantum error-correcting codes exist. **Phys. Rev. A**, 54:1098–1105, Aug 1996.

X. Chen, B. Zeng, e I. L. Chuang. Nonbinary codeword-stabilized quantum codes. **Phys. Rev. A**, 78:062315, Dec 2008.

A. M. Childs e W. van Dam. Quantum algorithms for algebraic problems. **Rev. Mod. Phys.**, 82:1–52, Jan 2010.

I. Chuang, A. Cross, G. Smith, J. Smolin, e B. Zeng. Codeword stabilized quantum codes: Algorithm and structure. **Journal of Mathematical Physics**, 50(4): 042109, 2009.

C. M. M Cosme. **Algoritmos Quânticos para o Problema do Subgrupo Oculto não Abeliano**. Tese de Doutorado, Laboratório Nacional de Computação Científica, 2008.

A. Cross, G. Smith, J. A. Smolin, e B. Zeng. Codeword stabilized quantum codes. **IEEE Trans. Inf. Theor.**, 55(1):433–438, Janeiro 2009. ISSN 0018-9448.

D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. 400:97–117, 1985.

M. B. Elliott, B. Eastin, e C. M. Caves. Graphical description of the action of Clifford operators on stabilizer states. 2007.

R. Feynman. Simulating Physics with Computers. **International Journal of Theoretical Physics**, 21(6/7), 1982.

A. Gonçalves. **Introdução à álgebra**. Projeto Euclides. Instituto de Matemática Pura e Aplicada, CNPq, 1979.

D. Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. **Phys. Rev. A**, 54:1862–1868, Sep 1996.

D. Gottesman. **Stabilizer codes and quantum error correction**. Tese de Doutorado, California Institute of Technology, 1997.

M. Grassl e T. Beth. A note on non-additive quantum codes. **eprint arXiv:quant-ph/9703016**, Marçø1997.

M. Grassl e M. Rötteler. Non-additive quantum codes from goethals and preparata codes. In: **Information Theory Workshop, 2008. ITW '08. IEEE**, páginas 396 –400, may 2008a.

M. Grassl e M. Rötteler. Quantum goethals-preparata codes. In: **Information Theory, 2008. ISIT 2008. IEEE International Symposium on**, páginas 300 –304, july 2008b.

M. Grassl e M. Rötteler. Graphs, quadratic forms and quantum codes. In: **In Proc. IEEE Int. Symp. Inf. Th. 2002. IEEE Inf. Th. Soc**, página 45, 2002.

M. Grassl, P. Shor, G. Smith, J. Smolin, e B. Zeng. Generalized concatenated quantum codes. **Physical Review A**, 79(5):050306, Maio 2009.

L. K. Grover. A fast quantum mechanical algorithm for database search. In: **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**, STOC '96, páginas 212–219, New York, NY, USA, 1996. ACM. ISBN 0-89791-785-5.

I.N. Herstein. **Abstract algebra**. Macmillan Pub., 1990. ISBN 9780023538223.

E. Hostens, J. Dehaene, e B. De Moor. Stabilizer states and Clifford operations for systems of arbitrary dimensions, and modular arithmetic. Fevereiro 2005.

D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, e C. H. Oh. Graphical nonbinary quantum error-correcting codes. **Phys. Rev. A**, 78:012306, Jul 2008.

P. Kaye, R. Laflamme, e M. Mosca. **An Introduction to Quantum Computing**. Oxford University Press, 2007. ISBN 9780198570493.

A. Ketkar, A. Klappenecker, S. Kumar, e P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. **Information Theory, IEEE Transactions on**, 52 (11):4892 –4914, nov. 2006. ISSN 0018-9448.

E. Knill e R. Laflamme. Theory of quantum error-correcting codes. **Phys. Rev. A**, 55:900–911, Feb 1997.

Y. Lequain e A. Garcia. **Álgebra: uma introdução**. Monografias de Matemática. Instituto de Matemática Pura e Aplicada, 1983.

Y. Li, I. Dumer, M. Grassl, e L. P. Pryadko. Structured error recovery for code-word-stabilized quantum codes. **Phys. Rev. A**, 81:052337, May 2010.

S. Y. Looi, L. Yu, V. Gheorghiu, e R. B Griffiths. Quantum error correcting codes using qudit graph states. (arXiv:0712.1979), Dec 2007. Comments: Any comments are welcome.

F. J. MacWilliams e N. J. A. Sloane. **The theory of error correcting codes / F.J. MacWilliams, N.J.A. Sloane**. North-Holland Pub. Co. ; sole distributors for the U.S.A. and Canada, Elsevier/North-Holland, Amsterdam ; New York : New York :, 1977. ISBN 0444850090 0444850104 0444850090.

N. Melo, R. Portugal, e D. F. G. Santiago. Decoder for nonbinary cws quantum codes. **arXiv:1204.2218v1 [cs.IT]**, april 2012.

F.C.P. Milies. **Anéis e módulos**. Publicaçoes do Instituto de matemática e estatística da universidade de Sao Paulo. Instituto de Matemática e Estatística da Universidade de Sao Paulo, 1972.

M. Mosca. Quantum algorithms. In: **Encyclopedia of Complexity and Systems Science**, páginas 7088–7118. 2009.

M. A. Nielsen e I. Chuang. **Quantum Computation and Quantum Information**, volume 70. Cambridge University Press, 2000.

M. Ricou e R. L. Fernandes. **Introdução á Álgebra**. Instituto Superior Técnico, 2004. ISBN 9789728469276.

D. F. G. Santiago, R. Portugal, e N. Melo. Non-pauli observables for cws codes. **Quantum Information Processing**, october 2012a. ISSN 1573-1332.

D. F. G. Santiago, R. Portugal, e N. Melo. Non-pauli observables for cws codes. In: **WECIQ 2012 - Workshop-school on Quantum Computation and Information**, páginas 17 –22, October 2012b.

D. Schlingemann. Stabilizer codes can be realized as graph codes. **Quantum Info. Comput.**, 2(4):307–323, Junho 2002. ISSN 1533-7146.

P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In: **Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on**, páginas 124 –134, nov 1994.

J. A. Smolin, G. Smith, e S. Wehner. Simple family of nonadditive quantum codes. **Phys. Rev. Lett.**, 99:130505, Sep 2007.

G. F. Staff. **Quantum Error Correction and Fault Tolerant Quantum Computing - S**. Taylor & Francis Group, 2008. ISBN 0849371996.

A. M. Steane. Simple quantum error-correcting codes. **Phys. Rev. A**, 54:4741–4751, Dec 1996.

M. Van den Nest, J. Dehaene, e B. De Moor. Graphical description of the action of local clifford transformations on graph states. **Phys. Rev. A 69, 022316 (2004). Arxiv preprint quant-ph/0308151**, 2004.

L.R. Vermani. **Elements of Algebraic Coding Theory**. Chapman and Hall Mathematics Series. Taylor & Francis, 1996. ISBN 9780412573804.

S. Yu, Q. Chen, C. H. Lai, e C. H. Oh. Nonadditive quantum error-correcting code. **Phys. Rev. Lett.**, 101:090501, Aug 2008.

S. Yu, Q. Chen, e C. H. Oh. Graphical quantum error-correcting codes. Relatório Técnico arXiv:0709.1780, Sep 2007. Comments: 7 pages and 3 figures.

S. Yu, Q. Chen, e C. H. Oh. Two infinite families of nonadditive quantum error-correcting codes. **ArXiv e-prints**, Janeiro 2009.

Capítulo 6

Apêndice A: Grupos e Anéis

Neste capítulo, faremos uma revisão sore a teoria de grupos. A estrutura de grupos é importante para entender alguns aspectos da computação quântica e de forma mais específica, dos códigos quânticos de correção de erros. Neste trabalho usamos grupos sobre operadores lineares, especificamente sobre os operadores de Pauli para entender o grupo estabilizador S dos códigos estabilizadores. Como os códigos CWS são uma generalização dos códigos estabilizadores, eles também usam a estrutura de um grupo estabilizador. Para estudar a estrutura algébrica dos grupos, usamos principalmente as referências, Nielsen e Chuang (2000), Gonçalves (1979), Herstein (1990), Lequain e Garcia (1983) e Milies (1972).

Definição 7. *Um conjunto não vazio G com uma operação*

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

é um grupo se as seguintes condições são satisfeitas:

(1) A operação é associativa, isto é,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(2) Existe um elemento neutro, isto é,

$$\exists e \in G \; tal \; que \, e \cdot a = a \cdot e = a, \; \forall a \in G$$

(3) Todo elemento possui um elemento inverso, isto é,

$$\forall a \in G, \; \exists b \in G \; tal \; que \, a \cdot b = b \cdot a = e.$$

A ordem de um grupo G é o seu número de elementos e é denotado por $|G|$. O grupo é dito **Abeliano** se todos os seus elementos comutam. Neste caso é comum também expressar a operação do grupo pelo símbolo de adição "+". Um subgrupo H de um grupo G é um subconjunto de G que satisfaz todas as propriedades de grupo. Denotamos então $H \leq G$. Um teorema que relaciona a ordem de um subgrupo com a ordem do grupo é o teorema de Lagrange.

Teorema 14. *Seja G um grupo e H um subgrupo de G. então a ordem de H divide a ordem de G, isto é $|H|$ divide $|G|$.*

Dado $H \leq G$ e $g \in G$ então uma classe lateral à esquerda de H em G com representante g é o conjunto

$$gH = \{gh | h \in H\}$$

Uma classe lateral à direita é definido de forma similar como $Hg = \{hg | h \in H\}$.

Um subgrupo $N \leq G$ é dito normal se

$$g^{-1}ng = \overline{n} \in N \; \forall \; n \in N \text{ e } g \in G$$

em outras palavras, se $g^{-1}Ng \subset N$. Neste caso, denota-se $H \triangleleft G$.

Quando $H \triangleleft G$, então o conjunto das classes laterais $G/H = \{H, g_1H, \ldots, g_tH\}$ também forma um grupo com a operação $(g_1H)(g_2H) = (g_1g_2H)$. Este grupo é chamado de grupo quociente de H em G.

seguem duas definições importantes para o trabalho. Dados os grupos $H \leq G$, podemos definir o centralizador de H em G ($C_G(H)$) e o normalizador de H em G ($N_G(H)$).

Definição 8. *Sejam $H \leq G$. O Normalizador de H em G, denotado por $N_G(H)$ é o grupo definido por*

$$N_G(H) = \{g \in G | g^{-1}Hg \in H\}.$$

Definição 9. *Sejam $H \leq G$. O Centralizador de H em G, denotado por $C_G(H)$ é o grupo definido por*

$$C_G(H) = \{g \in G | g^{-1}hg = h \; \forall \; h \in H\}.$$

Uma outra estrutura algébrica que será usada é a de anel. Daremos aqui apenas sua definição.

Definição 10. *O conjunto A munido de duas operações $(+)$ e $(.)$ (denotamos $(A, +, .)$) é um anel se*

(1) $(A, +)$ é um grupo abeliano.

(2) a operação $(.)$ é associativa, isto é

$$\forall a, b, c \in A, \; (a.b).c = a.(b.c)$$

(3) As operações $(.)$ e $(+)$ são distributivas, isto é

$$\forall a, b, c \in A, \; a.(b + c) = a.b + a.c \text{ e } (b + c).a = b.a + c.a.$$

Capítulo 7

Apêndice B: Módulos e Álgebra de Grupos

Neste capítulo, faremos uma revisão sore a teoria de módulos. A estrutura algébrica de módulos generaliza o conceito de espaço vetorial. Definimos espaço vetorial como um conjunto que sofre ação de um corpo que normalmente é $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{C}$. Um módulo é um conjunto (um grupo abeliano, como nos espaços vetoriais) que sofre a ação de um anel, uma estrutura algébrica mais geral que a de um corpo. Neste trabalho consideramos os módulos $\mathbb{Z}_d^n$.Este conjunto sofre a ação do anel $\mathbb{Z}_d$, o anel dos inteiros módulo d. Usamos esta estrutura de módulos principalmente no Teorema 10 que é um resultado novo que relaciona códigos estabilizadores com códigos CWS. Para estudar a estrutura algébrica dos módulos, usamos principalmente a referência, Ricou e Fernandes (2004), mas também usamos Gonçalves (1979), Herstein (1990), Lequain e Garcia (1983) e Milies (1972).

Definição 11. *Um módulo M sobre um anel unitário A (um A-módulo) é um grupo abeliano $(M, +)$ que sofre a ação dos elementos de A. Isto é, dados $a \in A$ e $v \in M$, existe uma operação $(a, v) \mapsto av \in M$ satisfazendo as seguintes propriedades:*

(1) $a(v_1 + v_2) = av_1 + av_2$, $a \in A$, $v_1, v_2 \in M$

(2) $(a_1 + a_2)v = a_1v + a_2v$, $a_1, a_2 \in A$, $v \in M$

(3) $a_1(a_2v) = (a_1a_2)v$, $a_1, a_2 \in A$, $v \in M$

(4) $1v = v$, $v \in M$

Um submódulo N de um A-módulo M é um subgrupo de $(M, +)$ que é fechado pela ação do elementos de A. Como exemplo de módulo, tome o anel $A = \mathbb{Z}_d$ e o grupo abeliano $(M, +) = \mathbb{Z}_d^n$ onde a operação do anel em M é a operação no anel $\mathbb{Z}_d$ aplicada em cada entrada dos elementos em $\mathbb{Z}_d^n$. Todos os módulos considerados neste trabalho serão módulos e submódulos deste tipo. Quando d é primo, o anel A é um corpo e o módulo M é na verdade um espaço vetorial. Assim como uma transformação linear é uma operação entre espaços vetoriais que preservam as operações entre os espaços, um homomorfismo entre módulos é definido da seguinte forma.

Definição 12. *Um homomorfismo de A-módulos,* $\phi : M_1 \to M_2$ *é uma aplicação entre A-módulos que satisfaz:*

(1) $\phi(v_2 + v_2) = \phi v_1 + \phi v_2$, $v_1, v_2 \in M$

(2) $\phi(av) = a\phi(v)$, $a \in A$, $v \in V$

Assim como uma matriz representa uma transformação linear entre espaços vetoriais, uma matriz $T_{(n\times m)}$ com entradas em $\mathbb{Z}_d$ representa, com a operação usual de matriz por vetor, um homomorfismo entre módulos $T : \mathbb{Z}_d^m \to \mathbb{Z}_d^n$. Dado então o homomorfismo representado por esta matriz $T_{(n\times m)}$, podemos facilmente verificar que os seguintes três conjuntos na verdade são submódulos:

(1) O núcleo de T, $(Ker(T))$ é um submódulo de $\mathbb{Z}_d^m$.

(2) A imagem de T, $(Im(T))$ é um submódulo de $\mathbb{Z}_d^n$. $Im(T)$ é na verdade o submódulo gerado pelas colunas de T e será também designado (**Módulo coluna de** T).

(3) $(\langle T \rangle)$ designará o submódulo de $\mathbb{Z}_d^m$ gerado pelas linhas de T e será chamado de (**Módulo linha de** T).

Seguem então os teoremas do isomorfismo de módulos, que serão usados futuramente em algumas demonstrações sobre os códigos CWS.

Teorema 15. *(Teoremas do Isomorfismo)*

(1) Se $\phi : M_1 \to M_2$ é um homomorfismo de A-módulos, então existe um isomorfismo de A-módulos:

$$Im(\phi) \simeq \frac{M_1}{Ker(\phi)}.$$

(2) Se N_1, N_2 são submódulos de um A-módulo M, então existe um isomorfismo de A-módulos:

$$\frac{N_1 + N_2}{N_2} \simeq \frac{N_1}{N_1 \cap N_2}.$$

(3) Se N, P são submódulos dum A-módulo M e $P \subset N \subset M$ então P é um submódulo de N e existe um isomorfismo de A-módulos:

$$M/N \simeq \frac{M/P}{N/P}.$$

Nosso objetivo é mostrar que, de forma equivalente para uma matriz T, representando uma transformação linear entre dois espaços vetoriais, onde a dimensão do espaço linha é igual à dimensão do espaço coluna, em uma matriz T representando um homomorfismo de módulos temos que a cardinalidade do módulo linha, $\#\langle T\rangle$ é igual à cardinalidade do módulo coluna, $\#Im(T)$. Para mostrar este resultado vamos introduzir o conceito de operação elementar.

Definição 13. *Uma operação elementar sobre um vetor $V = (v_1, \ldots, v_n)$ em $\mathbb{Z}_d^n$ consiste em uma das duas operações:*

(1) Adicionar um múltiplo em $\mathbb{Z}_d$ de uma entrada do vetor à uma outra entrada, isto é, em notação computacional, fazer $v_i = v_i + av_j$, onde $a \in \mathbb{Z}_d$.

(2) Trocar duas entradas do vetor.

Lema 5. *Dados dois números inteiros $0 \leq a, b \leq d-1$ e $a \neq 0$, então existem $\overline{q}, \overline{r} \in \mathbb{Z}_d$ tal que $0 \leq r < a$ e*

$$\overline{r} = \overline{a}\,\overline{q} + \overline{b}$$

Demonstração. Pelo algoritmo de divisão de Euclides sobre $\mathbb{Z}$, temos que existe q' e $0 \leq r < d-1$ tal que

$$b = a\,q' + r$$

logo

$$\overline{b} = \overline{a}\,\overline{q'} + \overline{r}$$

neste caso, como $0 \leq b < d$, temos também $0 \leq q' < d$. Tome $q = d - q'$ e temos

$$\overline{r} = \overline{b} + \overline{a}\,\overline{q}$$

completando a prova □

A próxima proposição diz que, através de operações elementares em um vetor com entradas em $\mathbb{Z}_d$, sempre é possível obter um resultado análogo à eliminação gaussiana.

Proposição 4. *Através de operações elementares, podemos transformar um vetor* $V = (\overline{v_1}, \ldots, \overline{v_n}) \in \mathbb{Z}_d^n$ *com* $0 \leq v_i < d$ *com pelo menos uma entrada não nula, em um vetor* $V' = (\overline{a}, \overline{0}, \ldots, \overline{0})$ *com apenas a primeira entrada assumindo um valor* $\overline{a}$ *não nulo enquanto os outras entradas assumem valores nulos.*

Demonstração. Repita o seguinte processo:

(1) Seja v_j um elemento que tem o menor valor absoluto positivo. Troque a $j$ésima entrada com a primeira. Renomeie as entradas do vetor para $V = (\overline{a_1}, \ldots, \overline{a_n})$.

(2) Para cada $j \neq 1$ aplique o Lema 5 para obter, na $j$ésima entrada,

$$\overline{r_j} = \overline{a_j} + \overline{q_j}\,\overline{a_1} \quad \text{onde} \quad 0 \leq r_j < a_1.$$

(3) Repita os procedimentos 1 e 2 até obter o resultado desejado.

□

Operações elementares sobre as colunas de uma matriz $T_{(m\times n)}$ em $\mathbb{Z}_d$ claramente não alteram o módulo coluna e portanto nem a cardinalidade deste módulo. Operações elementares sobre as linhas de T claramente não alteram o núcleo $Ker(T)$ e consequentemente pelo primeiro teorema do isomorfismo, não alteram a cardinalidade do módulo $Im(T)$ que é justamente o módulo coluna. De forma análoga podemos mostrar que estas operações também não alteram a cardinalidade do módulo linha.

Proposição 5. *Seja $T_{(m\times n)}$ uma matriz com entradas em $\mathbb{Z}_d$ representando um homomorfismo de módulos. então as cardinalidades dos módulos linha e coluna são iguais, $\#Im(T) = \#\langle T\rangle$.*

Demonstração. Usando o fato de que operações elementares nas linhas e colunas de T não alteram a cardinalidade do módulo linha nem do módulo coluna, podemos seguir o seguinte procedimento:

(1) Considere juntos todos os valores da primeira linha e primeira coluna de T. Tome o menor deles, e através de operações elementares de troca, coloque este na posição $(1, 1)$.

(2) Faça agora como na demonstração da Proposição 4, só que considerando todos os valores juntos da primeira linha e coluna. Após este procedimento, todos os valores da primeira linha e coluna, tirando possivelmente o valor na entrada $(1, 1)$ são nulos.

repetindo este procedimento para as outras linhas e colunas, obtemos no final uma matriz T' onde apenas os valores $T'_{i,i}$ com i variando de 1 até mín(n, m) podem assumir valores diferentes de 0. Claramente esta matriz satisfaz $\#Im(T') = \#\langle T'\rangle$ e como operações elementares não mudam a cardinalidade destes módulos, segue o resultado. □

Um conceito também importante para o entendimento do trabalho e que está relacionado ao conceito de módulos é o de **álgebra** e **álgebra de grupos**.

Definição 14. *Seja K um anel comutativo com unidade. Um anel A é chamado de K-Álgebra (ou álgebra sobre K) se*

(1) $(A, +)$ é um K-módulo unitário à esquerda.

(2) $K(ab) = (Ka)b = a(Kb)$ $\forall k \in K$ e $a, b \in A$.

Com esta definição podemos então entender o conceito de álgebra de grupos.

Definição 15. *Sejam K um anel comutativo com unidade e G um grupo. A álgebra de grupos $K[G]$ é uma K-álgebra em que o anel A da Definição 14 é o anel onde os elementos são dados por*

$$\alpha = \sum_{i=1}^{|G|} \alpha_i g_i$$

em que g_i percorre todos os elementos do grupo e $\alpha_i \in K$.

Capítulo 8

Apêndice C: Projetores de um Código Estabilizador

Definição 16. *Sejam $S = \langle s_1, \ldots, s_m \rangle$ um subgrupo do do grupo de Pauli $\mathcal{G}_d^n$ e $\mathbf{x} \in \mathbb{Z}_d^m$. defina então o operador $P_S^{\mathbf{x}}$ como*

$$P_S^{\mathbf{x}} = \frac{1}{d^r} \prod_{i=1}^{r} (I + q_d^{d-x_i} s_i + (q_d^{d-x_i} s_i)^2 + \ldots + (q_d^{d-x_i} s_i)^{d-1})$$

Teorema 16. *Sejam $S = \langle s_1, \ldots, s_m \rangle$ um subgrupo abeliano do grupo de Pauli $\mathcal{G}_d^n$ que não contêm múltiplos da identidade que não a identidade propriamente dita, $\mathbf{x} \in \mathbb{Z}_d^m = (x_1, \ldots, x_r)$ e $V_S^{\mathbf{x}}$ o subespaço de $\mathcal{H}_d^n$ definido como a interseção dos auto-espaços associados aos autovalores $q_d^{x_i}$ de cada gerador s_i, então o projetor sobre $V_S^{\mathbf{x}}$ é o operador $P_S^{\mathbf{x}}$.*

Demonstração. Como os operadores de S são simultaneamente diagonalizáveis, considere $\beta = \{|\theta_j\rangle\}$ uma base comum de autovetores. Se $|\theta_j\rangle \in V_S^{\mathbf{x}}$ então:

$$\begin{aligned}
&\frac{1}{d^r}(I + q_d^{d-x_i} s_i + (q_d^{d-x_i} s_i)^2 + \ldots + (q_d^{d-x_i} s_i)^{d-1})|\theta_j\rangle \\
=&\frac{1}{d^r}(|\theta_j\rangle + q_d^{d-x_i} q_d^{x_i}|\theta_j\rangle + (q_d^{d-x_i})^2 (q_d^{x_i})^2 |\theta_j\rangle + \ldots + (q_d^{d-x_i})^{d-1} (q_d^{x_i})^{d-1})|\theta_j\rangle = \frac{1}{d^{r-1}}|\theta_j\rangle
\end{aligned}$$

segue então que $P_S^{\mathbf{x}}|\theta_j\rangle = |\theta_j\rangle$. Se $|\theta_j\rangle \notin V_S^{\mathbf{x}}$ então existe um s_i tal que $s_i|\theta_j\rangle =$

$q_d^{\overline{x_i}}|\theta_j\rangle$ para algum $\overline{x_i} \neq x_i$, logo para este s_i temos:

$$\begin{aligned}
&\frac{1}{d^r}(I + q_d^{d-x_i}s_i + (q_d^{d-x_i}s_i)^2 + \ldots + (q_d^{d-x_i}s_i)^{d-1})|\theta_j\rangle \\
=&\frac{1}{d^r}(|\theta_j\rangle + q_d^{d-x_i+\overline{x_i}}|\theta_j\rangle + (q_d^{d-x_i+\overline{x_i}})^2|\theta_j\rangle + \ldots + (q_d^{d-x_i+\overline{x_i}})^{d-1}|\theta_j\rangle) \\
=&\frac{1}{d^r}(\sum_{l=1}^{d-1}(q_d^{d-x_i+\overline{x_i}})^l|\theta_j\rangle)
\end{aligned}$$

e como $q_d^{d-x_i+\overline{x_i}}$ é uma raiz d-ésima da unidade não trivial, o somatório acima é 0 e portanto $P_S^{\mathbf{x}}|\theta_j\rangle = \overline{0}$. Daí segue também que $(P_S^{\mathbf{x}})^2 = P_S^{\mathbf{x}}$ e portanto $P_S^{\mathbf{x}}$ é o projetor sobre $V_S^{\mathbf{x}}$. □

Provamos então que $P_S^{\mathbf{x}}$ é o projetor de $\mathcal{H}_d^n$ no subespaço $V_S^{\mathbf{x}}$ que é a interseção dos auto-espaços associados aos autovalores $q_d^{x_i}$ de cada gerador s_i. Pode-se verificar que a soma destes projetores é igual a I e que a interseção de quaisquer dois subespaços $V_S^{\mathbf{x}} \bigcap V_S^{\overline{\mathbf{x}}}$ tem apenas o vetor nulo em comum. Os subespaços $V_S^{\mathbf{x}}$ podem ser alguns deles triviais, contendo apenas o vetor nulo. Isto ocorre por exemplo, quando existir um gerador s_i que não possui um autovetor associado a algum autovalor $q_d^{x_i}$. Para calcular a dimensão de $V_S^{\mathbf{x}}$ basta calcular o traço do projetor $tr(P_S^{\mathbf{x}})$. O próximo teorema mostra como então saber a dimensão do auto-espaço associado ao autovalor 1 de todos os geradores s_i.

Demonstração. A expressão do projetor é dada por

$$P_S^{\overline{0}} = \prod_{i=1}^{r}\left(\frac{I + s_i + s_i^2 + \ldots + s_i^{d-1}}{d}\right)$$

considere $o(s_i)$ a ordem de s_i. Como $o(s_i)$ divide d podemos reescrever a expressão como

$$P_S^{\overline{0}} = \prod_{i=1}^{r}\left(\frac{d}{o(s_i)}\frac{I + s_i + s_i^2 + \ldots + s_i^{o(s_i)-1}}{d}\right) = \prod_{i=1}^{r}\left(\frac{I + s_i + s_i^2 + \ldots + s_i^{o(s_i)-1}}{o(s_i)}\right)$$

usando o fato de S ser abeliano e a distributividade, obtemos

$$P_S^{\overline{0}} = \frac{1}{o(s_1)\dots o(s_r)} \sum_{v_1=0,\dots,v_r=0}^{o(s_1)-1,\dots,o(s_r)-1} s_1^{v_1}\dots s_r^{v_r}$$

Temos que $tr(I) = d^n$ e $tr(s_1^{v_1}\dots s_r^{v_r}) = 0$ se $s_1^{v_1}\dots s_r^{v_r} \neq q_d^k I$. usando o fato de que S não possui múltiplos da identidade além dela própria e a linearidade do traço, temos

$$dim(V_S^{\overline{0}}) = tr(P_S^{\overline{0}}) = \frac{tr(I)}{|S|} = \frac{d^n}{|S|}$$

□