Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica

Departamento de Matemática Aplicada

Uma Álgebra de Clifford de Assinatura (n,3n) e os Operadores Densidade da Teoria da Informação Quântica

Autor: Nolmar Melo

Orientador: Carlile Campos Lavor

19 de Janeiro de 2011

Este trabalho teve o apoio financeiro da Fapesp. Processo 2006/58413-5.

Uma Álgebra de Clifford de Assinatura (n,3n) e os Operadores Densidade da Teoria da Informação Quântica

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Nolmar Melo de Souza e aprovada pela comissão julgadora.

Campinas, 19 de Janeiro de 2011

Carlile Campos Lavor

Prof. Dr. Carlile Campos Lavor
Orientador

Banca Examinadora:

1. Prof. Dr. Carlile Campos Lavor
2. Profa. Dra. Sueli Irene Rodrigues Costa
3. Prof. Dr. Ricardo Antônio Mosna
4. Prof. Dr. Renato Portugal
5. Prof. Dr. Nelson Maculan Filho

Tese de Doutorado apresentada ao Instituto de Matemática, Estatística e Computação Cientifica como parte dos requisitos para obtenção do título de **Doutor em Matemática Aplicada**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Melo, Nolmar

M491a Uma álgebra de Clifford de assinatura (n,3n) e os operadores densidade da teoria da informação quântica/Nolmar Melo de Souza-- Campinas, [S.P. : s.n.], 2011.

Orientador : Carlile Campos Lavor

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Clifford, Álgebra de. 2.Informação quântica. 3.Computação quântica. 4.Álgebra geométrica. 5.Operador densidade. I. Lavor, Carlile Campos. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: A Clifford algebra of signature (n,3n) and the density operators of quantum information theory

Palavras-chave em inglês (Keywords): 1.Clifford algebras. 2.Quantum information. 3.Quantum computation. 4.Geometric algebra. 5.Density operator.

Titulação: Doutor em Matemática Aplicada

Banca examinadora: Prof. Dr. Carlile Campos Lavor (IMECC – UNICAMP)
Profª. Drª. Sueli Irene Rodrigues Costa (IMECC – UNICAMP)
Prof. Dr. Ricardo Antônio Mosna (IMECC – UNICAMP)
Prof. Dr.Renato Portugal (LNCC)
Prof. Dr. Nelson Maculan Filho (UFRJ)

Data da defesa: 19/01/2011

Programa de Pós-Graduação: Doutorado em Matemática Aplicada

Tese de Doutorado defendida em 19 de janeiro de 2011 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). CARLILE CAMPOS LAVOR

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). RICARDO ANTONIO MOSNA

Prof(a). Dr(a). NELSON MACULAN FILHO

Prof(a). Dr(a). RENATO PORTUGAL

Resumo

Este trabalho apresenta uma linguagem algébrica para dois elementos básicos da teoria da informação quântica (os bits quânticos e os operadores densidade), baseada nas propriedades de uma álgebra de Clifford de assinatura (n,3n). Demonstramos que a nova descrição desses elementos preserva as mesmas propriedades matemáticas obtidas com a descrição clássica. Com isso, estendemos alguns resultados apresentados na literatura que relaciona Álgebra de Clifford e Informação Quântica.

Abstract

This work presents an algebraic language for two basic elements of quantum information theory (the quantum bits and density operators), based in the properties of a Clifford algebra of signature (n,3n). We prove that the new description of these elements preserves the same mathematical properties obtained with the classical description. We also extend some results presented in the literature that relate Clifford algebra and quantum information.

Dedico esse trabalho àqueles que me apoiaram incondicionalmente: meus pais, João Ferreira de Souza e Maria de Fátima Mello de Souza.

Agradecimentos

É difícil escrever a parte de agradecimentos desse trabalho e contemplar todos aqueles que merecem ser agradecidos, isso pelo fato de muitas pessoas terem contribuído de alguma forma para a conclusão desse trabalho, seja com dicas de como resolver um problema ou mesmo apoiando-me em momentos difíceis ou ainda gerando momentos alegres durante esse período de reclusão e pesquisa.

Começo agradecendo àquele que com muita paciência suportou-me e incentivou-me durante todo esse tempo. Carlile, sua orientação foi de fundamental importância para a conclusão desse trabalho.

Ainda com os docentes do IMECC, não posso deixar de agradecer à professora Sueli Costa, aos professores Plínio, Engler e Brumatti os quais de um modo ou outro também contribuíram no caminhar desse etapa.

Os amigos que comigo entraram nessa barca, Eduardo e Maurício, sempre serão lembrados em todos os momentos.

Retornando ao IMECC, não posso esquecer dos colegas do grupo de pesquisa, João, Cristiano, Carina, Grasiele, Agnaldo, Allan, Campello e outros que ficarei devendo.

Também agradeço aos amigos que suportaram-me por todo esse tempo: Lais, Taia, Renata, Gustavo, Estevão, Márcio, Bruna, Willian e aos demais sem os quais esse tempo aqui seria insuportável.

O mais importante, agradeço aos meus pais, irmãos e familiares que me apoiaram em todos os momentos da vida.

Para terminar, agradeço à FAPESP pelo apoio financeiro.

lance de dados
(gessinger)

daqui não tem mais volta, pra frente é sem saber
pequenos paraísos e riscos a correr
os deuses jogam pôquer
e bebem no saloon doses generosas de br 101
tá escrito há 6.000 anos em parachoques de caminhão
atalhos perigosos feito frases feitas
os deuses dão as cartas... o resto é com você

no fundo tudo é ritmo
a dança foge do salão
invade a autoestrada do átomo ao caminhão
o fim é puro ritmo
o último suspiro é purificação
os deuses dão as costas... agora é só você

os deuses dão as costas... agora é só você... querer

Sumário

Introdução

Neste texto, formalizamos e generalizamos a álgebra de Clifford usada nos trabalhos de Havel, Doran, Lasenby e outros [DLG93, SLD99, DLG+96, HD02]. De forma particular, estudamos o conceito de operadores densidade os quais são de grande importância na teoria de informação quântica.

As álgebras de Clifford, que têm esse nome em homenagem ao matemático inglês do século 19, William Kingdon Clifford, são uma classe de álgebras associativas relacionadas à teoria de formas quadráticas. Tal classe de álgebras generaliza os conjuntos dos números complexos e dos quatérnios.

Muito usadas na física-matemática, as álgebras de Clifford são ótimas ferramentas para o estudo de algumas áreas da mesma. Neste trabalho, usamos uma classe dessas álgebras com o intuito de estudar algumas propriedades da mecânica quântica utilizadas na teoria da informação e computação quântica.

A "Lei de Moore", de 1965, diz que a cada 18 meses a capacidade de processamento dos computadores duplica, isso com um custo constante. Dessa previsão, acredita-se que tal fenômeno tenha um limite de tempo, estimado entre os primeiros 20 anos do século atual.

Com essa limitação, alguns pesquisadores começaram a pensar em como superar esse problema e uma das possíveis soluções apresentadas foi a utilização das propriedades da mecânica quântica para tratar os problemas de computação e informação.

Ainda no século passado, David Hestenes começou a reescrever os fundamentos da física (mecânica clássica e quântica) usando as ferramentas da álgebra geométrica e algumas outras álgebras de Clifford. Com base em seus trabalhos, muito foi desenvolvido nos últimos anos chegando até o artigo [HD02] "Geometric Algebra in Quantum Information Processing" de Havel e Doran, o qual serviu de inspiração para este trabalho.

Iremos nos concentrar em um conceito fundamental da teoria da informação quântica, os operadores densidade. Tal conceito é muito útil quando queremos provar matematicamente que certas estruturas usadas realmente funcionam.

Analisaremos, formalmente, como uma álgebra de Clifford, mais precisamente a álgebra de assinatura $(n, 3n)$, pode ser usada para descrever os elementos principais da teoria de informação quântica.

O texto está dividido em três capítulos e tenta ser o mais auto-suficiente possível. No primeiro capítulo, fazemos uma breve revisão das estruturas algébricas tais como anéis, grupos e álgebras, e finalizamos com a apresentação das álgebras de Clifford e alguns exemplos das mesmas.

No segundo capítulo, "Álgebra de Clifford e a Teoria Quântica", apresentamos os conceitos básicos da teoria de informação quântica que tratamos no trabalho, q-bits e operadores densidade, e mostramos as álgebras de assinatura (n,3n) que passam a ser usadas até o fim do texto.

Já o terceiro e último capítulo, "Positividade", começamos mostrando como definir elementos definidos positivos na álgebra de Clifford em questão, com o intuito de definir os operadores densidade sem usar elementos da álgebra das matrizes. Finalizamos o trabalho apresentando definições equivalentes de operadores densidade.

Capítulo 1

Álgebras de Clifford

Neste capítulo, falaremos sobre álgebras dando um enfoque às álgebras de Clifford, formalizando-as e mostrando algumas propriedades básicas. A linguagem algébrica será utilizada em todo decorrer deste texto.

1.1 Noções Básicas de Álgebra - Anéis e Grupos

Um dos objetos básicos que usamos no decorrer deste texto é o que chamamos de anel. Um anel é uma tripla composta de um conjunto, A, e duas operações binárias, $+$ e $\cdot$, que damos o nome de adição e multiplicação, respectivamente.

Definição 1.1.1. *A uma tripla,* $(A, +, \cdot)$*, damos o nome de anel se para todos* $a, b, c \in A$ *as seguintes propriedades são válidas:*

1. *As operações* $+$ *e* $\cdot$ *são fechadas, ou seja,* $a + b \in A$ *e* $a \cdot b \in A$*;*
2. *Existe* 0 *e* $e \in A$ *tais que* $0 + a = a + 0 = a$ *e* $e \cdot a = a \cdot e = a$*;*
3. *Vale a propriedade distributiva,* $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c$*;*

4. *A operação soma é comutativa,* $a + b = b + a$*;*

5. *Para todo* $a \in A$ *existe* $b \in A$ *tal que* $a + b = 0$*, tal* b *é denotado por* $-a$*;*

6. *As operações são associativas,* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *e* $a + (b + c) = (a + b) + c$.

- *Se a multiplicação também for comutativa, chamamos o anel de comutativo.*

Como definimos, todo anel tem um elemento neutro referente à operação de multiplicação, chamado de unidade. Vale observar que o termo anel também é usado para uma estrutura um pouco mais geral, a qual difere dessa pela existência da unidade. Alguns autores chamam a estrutura aqui definida de "anel com unidade".

Definição 1.1.2. *Sejam* $(A, +, \cdot)$ *um anel e* I *um subconjunto de* A*. Falamos que* I *é um ideal à direita de* A *se:*

1. *Para todos* $a, b \in I$*, temos que* $a + b \in I$*;*

2. *Para todo* $a \in A$*, temos que* $aI \subset I$*, onde* $aI = \{a \cdot x; x \in I\}$.

Analogamente, definimos ideal à esquerda de A *impondo que* $Ia \subset I$.

Quando o anel A é comutativo, chamamos simplesmente de ideal.

Exemplo 1.1.3. *No anel dos números inteiros, se tomarmos o conjunto dos números pares perceberemos com facilidade que esse é um ideal, pois a soma de qualquer número par é um número par e a multiplicação de qualquer número inteiro por um número par também é par.*

Exemplo 1.1.4. *Sejam* A *um anel e* $S \subset A$ *não vazio. O conjunto:*

$$(S) = \left\{ \sum_{s \in S} \alpha_s s; \alpha_s \in A \textit{ e } \alpha_s = 0 \textit{ a menos de um numero finito de vezes} \right\},$$

é um ideal à direita de A. *Falamos que* (S) *é o ideal à direita de* A *gerado por* S. *Quando o contexto for claro falaremos apenas que este é o ideal gerado por* S.

Se um ideal I *for tal que existe um elemento* $a \in I$ *de tal modo que* $(a) = I$, *então damos a esse o nome de ideal principal.*

Definição 1.1.5 (Anel Quociente)**.** *Seja* $(A, +, \cdot)$ *um anel e* m *um ideal (à direita ou à esquerda) de* A. *Definimos o anel quociente* A/m *com as operações induzidas de* A *da seguinte forma:*

1. $(a+m)+(b+m) = (a+b)+m$, $\forall a, b \in A$, *onde* $(a+m) = \{a+c; c \in m\}$*;*

2. $(a + m) \cdot (b + m) = a \cdot b + m$, $\forall a, b \in A$.

Falamos que o anel quociente é o anel das classes de equivalências de A, onde a classe de $a \in A$, $a + m$, é equivalente à classe de $b \in A$, $b + m$, se tem-se que $a - b \in m$ e denotamos por: $a \equiv b$.

Definição 1.1.6. *Sejam* A *e* B *anéis. Chamamos de homomorfismo de anéis uma função* $f : A \to B$ *tal que:*

1. $f(a + b) = f(a) + f(b)$

2. $f(a \cdot b) = f(a) \cdot f(b)$.

Um homomorfismo injetivo e sobrejetivo ao mesmo tempo é dito um isomorfismo de anéis.

Exemplo 1.1.7. *Sejam* A *um anel e* m *um ideal de* A, *a função* π *definida abaixo é um homomorfismo sobrejetor de anéis, a essa função damos o nome de projeção canônica.*

$$\begin{array}{rccc} \pi: & A & \to & A/m \\ & a & \mapsto & a + m. \end{array}$$

Outro objeto básico utilizado neste texto é o que chamamos de grupo. Assim como um anel, um grupo é um conjunto munido com uma operação binária que segue algumas propriedades.

Definição 1.1.8. *Ao par formado por um conjunto não vazio* G *e uma operação binária* $+ : G \times G \to G$ *damos o nome de grupo se para todos* $a, b, c \in G$ *vale que:*

1. *Existe* $0 \in G$ *de modo que* $a + 0 = 0 + a = a$*;*
2. *Dado* $a \in G$ *existe* $-a \in G$ *tal que* $a + -a = -a + a = 0$*;*
3. *A operação é associativa, ou seja,* $(a + b) + c = a + (b + c)$*;*

- *Quando a operação é comutativa, ou seja* $a + b = b + a$*, falamos que o grupo é comutativo ou abeliano.*

Assim como acontece com os anéis, definimos homomorfismos e isomorfismos entre grupos.

Definição 1.1.9. *Sejam* G *e* F *grupos. Chamamos de homomorfismo de grupos uma função* $f : G \to F$ *tal que:*

$$f(a + b) = f(a) + f(b), \quad \forall a, b \in G.$$

Damos o nome de isomorfismo de grupos a um homomorfismo bijetor.

1.2 Módulos

O conceito de módulo é uma generalização dos conhecidos espaços vetoriais.

Definição 1.2.1. *Seja* A *um anel. Um módulo à esquerda sobre* A *(*$A-$*módulo à esquerda),* M*, é um grupo abeliano com uma operação de* $A \times M$ *em* M *tal que* *para todos* $a, b \in A$ *e* $x, y \in M$ *temos:*

$$(a + b)x = ax + bx \text{ e } a(x + y) = ax + ay.$$

Analogamente, definimos módulo à direita sobre A*. Quando* A *é comutativo, chamamos apenas de módulo e quando* A *é um corpo, temos que o módulo é exatamente um espaço vetorial.*

Sendo M um módulo e N um subconjunto que tem estrutura de módulo, N é chamado submódulo de M.

Definição 1.2.2. *Sendo* M *e* N $A-$*módulos e* $f : M \to N$ *um homomorfismo de grupos tal que* $f(ax) = af(x)$*, para todo* $a \in A$*, chamamos* f *de homomorfismo de módulos .*

Definição 1.2.3. *Sejam* M *um* $A-$*módulo e* $\beta = \{b_1, b_2, \ldots\} \subset M$*. Falamos que* β *é um conjunto de geradores de* M *se para qualquer* $m \in M$ *tem-se que* $m = \sum_{b \in \beta} \lambda_b b$*, com* $\lambda_b \in A$ *e* $\lambda_b = 0$ *a menos de um número finito de vezes. Quando existe* β *finito, falamos que* M *é um módulo finitamente gerado.*

Definição 1.2.4. *Sejam* M *um* $A-$*módulo e* $\beta = \{b_1, b_2, \ldots\} \subset M$*. Falamos que* β *é um conjunto linearmente independente se a combinação linear* $\sum_{b \in \beta} \lambda_b b = 0$, $\lambda_b \in A$ *e* $\lambda_b = 0$ *quase sempre, é verdade apenas se todos os* λ_b *forem nulos.*

Definição 1.2.5. *A um conjunto de geradores linearmente independente damos o nome de base.*

Definição 1.2.6. *Sejam* M *um* $A-$*módulo e* N_1, N_2 *submódulos de* M*. Se* $B = N_1 \cup N_2$ *e* N *é o submódulo de* M *gerado por* B*, falamos que* N *é soma direta de* N_1 *e* N_2 *se dado* $n \in N$ *existem únicos* $n_1 \in N_1$ *e* $n_2 \in N_2$ *de modo que* $n = n_1 + n_2$ *e denotamos* $N = N_1 \oplus N_2$*.*

1.3 Álgebra

O conceito de álgebra é uma das principais estruturas que estudaremos nesse trabalho.

Definição 1.3.1. *Seja* M *um* $A-$*módulo. Se existe em* M *uma operação binária* $A-$*bilinear*[1]

$$\begin{array}{rccc} \cdot: & M\times M & \to & M \\ & (m_1, m_2) & \mapsto & m_1\cdot m_2 \end{array},$$

que seja associativa, distributiva em relação à soma e se M *tem unidade, chamamos* M *de* $A-$*álgebra.*

É importante destacar que uma álgebra tem estrutura de anel. Como temos um elemento unidade $1\in M$, podemos usar o "mergulho" $a\mapsto a\cdot 1$ e identificar A como subconjunto $A\cdot 1$ de M.

1.4 Álgebras Graduadas

Sejam F uma $A-$álgebra com um conjunto de geradores $\{x_i; i\in I\}$ e $y_\sigma = x_{i_1}x_{i_2}\dots x_{i_h}$, onde $\sigma = (i_1, \cdots, i_h)$ e I é um conjunto de índices. Podemos classificar os elementos y_σ pelo comprimento de σ.

Seja F_h o módulo gerado pelos y_σ de comprimento h. Pode-se provar que F é a soma direta dos módulos $F_0, F_1, \cdots$, ou seja:

$$F = F_0\oplus F_1\oplus F_2\oplus\cdots.$$

[1]Falamos que uma função $f: M\times M\to N$, onde M e N são $A-$módulos, é $A-$bilinear se para todos $a, b\in A$ e todos $w_1, w_2, w_3, w_4\in M$ tem-se que: $f(aw_1+w_2, bw_3+w_4) = abf(w_1,w_3)+af(w_1,w_4)+bf(w_2,w_3)+f(w_2,w_4)$.

Também temos que $F_i F_j \subset F_{i+j}$[2].

Definição 1.4.1. *Seja* $(\Gamma, +)$ *um grupo. Uma álgebra* $\Gamma-$*graduada é uma álgebra* E *que pode ser decomposta em soma direta de módulos na forma:*

$$\bigoplus_{\gamma \in \Gamma} E_\gamma,$$

onde os E_γ *são submódulos de* E *tais que*

$$E_\gamma E_{\gamma'} \subset E_{\gamma+\gamma'}.$$

Numa álgebra $\Gamma-$graduada E, um elemento, $x \in E_\gamma$, é dito elemento homogêneo de grau γ.

Casos especiais:

1)Quando $\Gamma = \mathbb{Z}$, chamamos a álgebra simplesmente de graduada;

2)Quando Γ é um grupo binário, $\{0, 1\}$, chamamos a álgebra de semi-graduada e escrevemos $E = E^+ \oplus E^-$, no lugar de $E_0 \oplus E_1$. Observe que E^+, com as operações induzidas de E é uma subálgebra de E, chamada de álgebra par.

1.5 Álgebra Tensorial

O produto tensorial é de grande valia para a mecânica quântica. Iremos tratá-lo nesta seção.

Definição 1.5.1. *Seja* M *um* $A-$*módulo. Uma álgebra,* T*, é dita álgebra tensorial sobre* M *se satisfaz as condições:*

1. T *é uma álgebra contendo* M *como submódulo e é gerada por* M *e* 1_T*;*

[2]Em um anel A, o produto de dois subconjuntos $B, C \subset A$ é o conjunto dado por: $BC = \{bc; b \in B, c \in C\}$.

2. *Para qualquer transformação linear, $\lambda : M \to E$, onde E é uma $A-$álgebra, existe um homomorfismo, $\theta : T \to E$, estendendo λ tal que o diagrama abaixo comuta, ou seja, $\lambda(x) = \theta(i(x))$, onde i é a inclusão de M em T.*

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[dr, "\lambda"'] & T \arrow[d, "\theta"] \\ & E \end{tikzcd}$$

Teorema 1.5.2. *Para um $A-$módulo M existe uma única álgebra tensorial, a menos de isomorfismo.*

Demonstração. [Che96] □

Definição 1.5.3. *Sejam M e N $A-$módulos, $P = N \oplus M$ e T a álgebra tensorial de P. O submódulo, Q de T_2,*[3] *formado por todos os produtos $\{xy; x \in N \text{ e } y \in M\}$ é chamado produto tensorial de N por M e é denotado por $N \otimes M$, seus elementos são denotados por $x \otimes y$, $x \in N$ e $y \in M$.*

Teorema 1.5.4. *Dada uma transformação bilinear, $\beta : M \times N \to R$, onde M, N e R são $A-$módulos, existe uma transformação linear, $\phi : M \otimes N \to R$, tal que $\phi(x \otimes y) = \beta(x, y)$ e o diagrama abaixo comuta.*

$$\begin{tikzcd} M \times N \arrow[r, "i"] \arrow[dr, "\beta"'] & M \otimes N \arrow[d, "\phi"] \\ & R \end{tikzcd}$$

Demonstração. [Che96] □

Quando M e N são espaços de matrizes, um exemplo de produto tensorial entre elementos desses espaços, $m \otimes n$, também conhecido como produto de Kronecker, é dado a seguir.

[3] T_2 é o módulo gerado pelo produto de quaisquer 2 elementos de P.

Se $m = (m_{ij})_{p\times q} \in M$ e $n = (n_{ij})_{k\times t} \in N$, então $m \otimes n = l \in M \otimes N$, onde $l = (l_{ij})_{pk\times qt}$, dado por

$$l = \left(\begin{array}{c|c|c|c} m_{11}n & m_{12}n & \cdots & m_{1q}n \\ \hline m_{21}n & m_{22}n & \cdots & m_{2q}n \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline m_{p1}n & m_{p2}n & \cdots & m_{pq}n \end{array}\right).$$

Assim, temos que $M \otimes N$ é o espaço das matrizes de dimensão $pk \times qt$.

Algumas propriedades interessantes, válidas para qualquer produto tensorial, são dadas abaixo (ver [Lan97], para mais detalhes).

Sendo $a \in A$, $w, m \in M$ e $n, t \in N$, onde A é um anel e M e N são $A-$módulos, então:

- $an \otimes m = n \otimes am$;
- $n \otimes (m + w) = n \otimes m + n \otimes w$;
- $(t + n) \otimes w = t \otimes w + n \otimes w$.

1.6 Álgebra de Clifford

Finalmente, com os conceitos já apresentados, poderemos tratar das álgebras de Clifford. Antes, precisamos definir uma forma quadrática.

Definição 1.6.1. *Seja* M *um* $A-$*módulo. Uma função* $f : M \to A$ *é uma forma quadrática se:*

1. $f(\alpha x) = \alpha^2 f(x)$, $\forall \alpha \in A$ *e* $x \in M$;
2. $\beta : M \times M \to A$, *definida por* $\beta(x, y) = f(x + y) - f(x) - f(y)$, *é bilinear.*

A função β *é dita forma bilinear associada a* f*.*

Definição 1.6.2. *Sejam* T *uma álgebra tensorial sobre um* $A-$*módulo* M *e* c *o ideal à direita de* T *gerado por elementos da forma* $x \otimes x - f(x) \cdot 1_T$, $x \in M$, *onde* f *é uma forma quadrática em* M *e* 1_T *é a unidade de* T*. A álgebra quociente* $\mathcal{C}\ell = T/c$ *é chamada álgebra de Clifford associada a* M *e* f*.*

Como antes, denotamos por π a projeção canônica de T na álgebra quociente

$$\begin{array}{rccc} \pi: & T & \rightarrow & \mathcal{C}\ell \\ & t & \mapsto & t+c \end{array}.$$

Assim $\pi(M)$ é o submódulo de $\mathcal{C}\ell$ que o gera como álgebra.

1.7 Casos Especiais de Álgebras de Clifford

Mostramos aqui alguns casos particulares de álgebras de Clifford, um dos quais serve como base para boa parte do que é feito no texto.

1.7.1 Primeiro Caso - Os Complexos

Consideremos M como um $A-$módulo gerado por $\{x\}$, ou seja, $M = Ax$. Temos aqui que $T = A[x]$, anel de polinômios, é a álgebra tensorial de M, tomando c como o ideal gerado por $x \otimes x - f(x) \cdot 1$, fazendo $\pi(x) = \xi$ e $\mathcal{C}\ell = T/c$.

Temos que $\mathcal{C}\ell$ é da forma $A \oplus A\xi$, onde $\xi^2 = f(\xi) \cdot 1$, fazendo $\varphi : M \rightarrow A\xi$, $ax \mapsto a\xi$, mergulhamos M em $\mathcal{C}\ell$ e podemos escrever $\mathcal{C}\ell = A \oplus M$, isto devido ao fato de φ ser um isomorfismo.

Agora se $A = \mathbb{R}$, o corpo dos números reais, e f é tal que $f(x) = -1$, temos que a álgebra aqui gerada é o corpo dos números complexos ($\mathbb{C}$).

1.7.2 Segundo Caso - Álgebra de Grassmann

Seja M um espaço vetorial sobre um corpo K, M é um módulo sobre K visto que K é um anel e todas as propriedades de módulo são satisfeitas por um espaço vetorial. Tome $f : M \to K$ identicamente nula.

Sejam T a álgebra tensorial de M e c o ideal gerado pelos elementos da forma $x \otimes x - f(x) \cdot 1_T = x \otimes x$. A álgebra de Clifford associada a M e f é chamada de álgebra de Grassmann associada a M ou álgebra exterior de M e denotada por $\Lambda(M)$.

O produto na álgebra exterior é denotado por $\wedge$ e é tal que $x \wedge y = -y \wedge x$. De fato, $0 = (x + y) \wedge (x + y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = x \wedge y + y \wedge x$. Assim a álgebra exterior é anti-comutativa.

1.7.3 Terceiro Caso - A Álgebra $\mathcal{C}\ell_3$ e as Matrizes de Pauli

Existem 3 matrizes especiais, chamadas de matrizes de Pauli, na teoria de informação quântica:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

onde i é o número complexo tal que $i^2 = -1$. Temos aqui que $\sigma_1\sigma_2 = i\sigma_3$ e $\sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{ij}I$, onde I é a matriz identidade. Também usaremos a notação σ_0 para a matriz identidade de ordem 2.

Analisaremos o caso da álgebra de Clifford do espaço vetorial $\mathbb{R}^3$ com a forma quadrática $f(x) = x_1^2 + x_2^2 + x_3^2$, denotada por $\mathcal{C}\ell_3$.

Considerando o conjunto $\{e_1, e_2, e_3\}$ como uma $\mathbb{R}-$base do espaço vetorial $\mathbb{R}^3$, temos que o conjunto $\{1, e_1, e_2, e_3, e_1 \otimes e_2, e_1 \otimes e_3, e_2 \otimes e_3, e_1 \otimes e_2 \otimes e_3\}$ é uma $\mathbb{R}-$base para a álgebra $\mathcal{C}\ell_3$. Observe que essa última base tem 8 elementos.

Na álgebra das matrizes $\mathrm{Mat}(2,\mathbb{C})$, podemos tomar como uma $\mathbb{R}-$base o conjunto $\{I, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_2\sigma_3, \sigma_1\sigma_3, \sigma_1\sigma_2\sigma_3\}$ e esse também contém 8 elementos.

Obtemos um isomorfismo de álgebras entre $\mathrm{Mat}(2,\mathbb{C})$ e $\mathcal{C}\ell_3$ pela função $\varphi : \mathrm{Mat}(2,\mathbb{C}) \to \mathcal{C}\ell_3$ dada por $\varphi(I) = 1$, $\varphi(\sigma_i) = e_i$ e estendendo linearmente para o resto do espaço.

A função φ leva base em base e tais bases têm a mesma cardinalidade. Fica provado assim que ela é um isomorfismo de espaços vetoriais. Agora é preciso mostrar que $\varphi(ab) = \varphi(a)\varphi(b)$.

Para provar que $\varphi(ab) = \varphi(a)\varphi(b)$, basta observar as tabelas de operações referentes às operações de multiplicação de cada álgebra comparando assim os resultados. Vale observar que só é preciso montar as tabelas para os elementos $1, e_1, e_2, e_2$ para a álgebra $\mathcal{C}\ell_3$ e $I, \sigma_1, \sigma_2, \sigma_3$ para a álgebra das matrizes em questão e lembrar que ambas as álgebras são associativas.

1	e_1	e_2	e_3
e_1	1	$e_1 \otimes e_2$	$e_1 \otimes e_3$
e_2	$-e_1 \otimes e_2$	1	$e_2 \otimes e_3$
e_3	$-e_1 \otimes e_3$	$-e_2 \otimes e_3$	1

I	σ_1	σ_2	σ_3
σ_1	I	$\sigma_1\sigma_2$	$\sigma_1\sigma_3$
σ_2	$-\sigma_1\sigma_2$	I	$\sigma_2\sigma_3$
σ_3	$-\sigma_1\sigma_3$	$-\sigma_2\sigma_3$	I

Referências do Capítulo

Recomendamos as seguintes referências para uma melhor compreensão sobre álgebras e especificamente as de Clifford. [Lan97, Lou97, Gar03, AM69, Knu88, Che96, Sch85]

◊♣♠♡

"Mathematicians practice absolute freedom"

Henry Adams

Capítulo 2

Álgebra de Clifford e a Mecânica Quântica

Neste capítulo, veremos a relação entre uma álgebra de Clifford e a mecânica quântica. As idéias básicas aqui são encontradas em artigos [SLD99, DLG$^+$96, DLG93, HD02, HCST01, SCH98, HD01, Hav03], sendo que a principal fonte é [HCST01].

2.1 Conceitos Básicos de Informação Quântica

Esta seção é dedicada a introduzir a linguagem matemática utilizada na teoria da informação quântica. Tal linguagem é encontrada na maioria dos textos básicos sobre informação e computação quântica.

2.1.1 Espaços de Hilbert

Um espaço de Hilbert é um espaço vetorial real ou complexo, munido de um produto interno e completo[1] com a norma induzida pelo produto interno.

Como iremos utilizar a mecânica quântica, os espaços de Hilbert aqui considerados sempre serão complexos. Além disso, por estarmos interessados na teoria da informação quântica, tais espaços sempre terão dimensão finita. Vale observar que todo espaço vetorial complexo de dimensão finita é um espaço de Hilbert.

Definição 2.1.1. *Sendo V um espaço de Hilbert, definimos um estado como sendo um vetor unitário do mesmo, onde usaremos a notação de Dirac, $|\phi\rangle$ para denotar o estado.*

Observe que quando V é um espaço de dimensão finita, o estado $|\phi\rangle$ é um vetor coluna, enquanto que $\langle\phi| = |\phi\rangle^*$ é o vetor linha conjugado, ou seja o adjunto. Na literatura é dado o nome de "ket" para o vetor $|\phi\rangle$ e $\langle\phi|$ recebe o nome de "bra".

Definição 2.1.2. *A um estado no espaço vetorial $\mathbb{C}^2$, damos o nome de estado de 1 q-bit. Quando o estado pertence ao espaço vetorial $\bigotimes_{i=1}^{n} \mathbb{C}^2$, temos um estado de n q-bits.*

Os q-bits são usados na mecânica quântica para descrever um sistema quântico [NC00, Pre98], mas como descrever o sistema quando o seu estado não é completamente conhecido? Tal descrição é feita com um conjunto de estados puros com probabilidades associadas a esses estados.

Definição 2.1.3. *Damos o nome de "ensemble" a um conjunto $\{(p_i, |\rho_i\rangle)\}$ de pares formados por estados $|\rho_i\rangle$ e probabilidades, p_i, do estado ocorrer no sistema quântico.*

[1] Um espaço com uma norma $|\cdot|$ é dito completo se toda sequência de Cauchy é convergente, ou seja, se (x_n) é uma sequência onde dado $\varepsilon > 0$ existe n_0 natural de modo que para todos naturais $n, m > n_0$ é verdade que $|x_n - x_m| < \varepsilon$, então a sequência converge.

2.1.2 A Ligação Entre os Estados e os Operadores Densidade

Na seção anterior, definimos o objeto básico da teoria da informação quântica, o q-bit. Agora, veremos um outro objeto que pode ser usado em substituição ao q-bit, que tem propriedades matemáticas interessantes, de tal modo que os postulados da mecânica quântica que a principio são descritos com q-bits passam a ser descritos via operadores densidade.

Definição 2.1.4. *Seja* $A \in \mathrm{Mat}(2^n, \mathbb{C})$ *uma matriz complexa de ordem* 2^n*. Se* A *é semidefinida positiva e tem traço 1, dizemos que* A *é uma matriz densidade ou um operador densidade.*

Existe uma ligação entre os operadores densidade e os q-bits, tal ligação é dada pelo seguinte teorema.

Teorema 2.1.5. *Dados um estado* $|\rho\rangle$ *e um "ensemble"* $\{(p_i, |\rho_i\rangle)\}$*, as matrizes definidas por* $A = |\rho\rangle\langle\rho|$ *e* $B = \sum_i p_i |\rho_i\rangle\langle\rho_i|$ *são operadores densidade. Falamos que* A *e* B*, respectivamente, são os operadores associados ao estado e ao ensemble.*

Demonstração. Não é difícil notar que A e B são semidefinidas positivas, visto que elas são somas de projetores multiplicados por um número não negativo e tais projetores são semidefinidas positivos.

Já para o traço temos que

$$\mathrm{tr}(A) = \mathrm{tr}(|\rho\rangle\langle\rho|) = \langle\rho||\rho\rangle = 1$$

e

$$\mathrm{tr}(B) = \mathrm{tr}\left(\sum_i p_i |\rho_i\rangle\langle\rho_i|\right) = \sum_i \mathrm{tr}(p_i |\rho_i\rangle\langle\rho_i|) =$$

$$\sum_i p_i \mathrm{tr}(|\rho_i\rangle\langle\rho_i|) = \sum_i p_i \mathrm{tr}(\langle\rho_i||\rho_i\rangle) = \sum_i p_i = 1.$$

□

Teorema 2.1.6. *Se A é um operador densidade, então existe um ensemble de modo que A é o seu operador densidade associado.*

Demonstração. Pelo fato de A ser uma matriz semidefinida positiva, existe uma base ortonormal de autovetores. A soma dos autovalores de A é 1, pois tal soma é igual ao traço da matriz, além disso seus autovalores são não negativos.

Se $\{(\lambda_i, |\phi_i\rangle)\}$ é tal que λ_i é o autovalor associado ao autovetor $|\phi_i\rangle$ de A, então tal conjunto é um ensemble. □

Vimos aqui dois elementos associados que são usados para descrever os postulados da mecânica quântica [NC00]. No que segue, veremos novamente esses conceitos em uma álgebra não usual.

2.2 Álgebra de Assinatura (1,3)

Álgebra de assinatura (1,3) é a álgebra de Clifford associada ao $\mathbb{R}-$espaço vetorial $\mathbb{R}^4$ e à forma quadrática $f : \mathbb{R}^4 \to \mathbb{R}$, $f(x_0, x_1, x_2, x_3) = x_0^2 - (x_1^2 + x_2^2 + x_3^2)$. Tomaremos aqui $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ como uma $\mathbb{R}-$base $\beta-$ortonormal para $\mathbb{R}^4$, onde β é a forma bilinear associada a f. Por abuso de notação a álgebra de Clifford, $\mathcal{C}\ell(\mathbb{R}^4, f)$, será denotada por $\mathcal{C}\ell_{1,3}$. Além disso, omitiremos a notação $\otimes$ quando se tratar de produto entre os elementos dessa álgebra, ou seja, $a \otimes b = ab$. Tem-se aqui que $\gamma_0^2 = 1$ e $\gamma_1^2 = \gamma_2^2 = \gamma_3^2 = -1$.

Proposição 2.2.1. *Em $\mathcal{C}\ell_{1,3}$, tem-se que $\gamma_i\gamma_j = -\gamma_j\gamma_i$ para $i \neq j$.*

Demonstração. Lembrando que $\mathcal{C}\ell_{1,3} = T/c$, onde T é a álgebra tensorial de $\mathbb{R}^4$ e c é o ideal gerado por elementos da forma $x \otimes x - f(x)1_T$. Para $i = 1,\ 2,\ 3$, tem-se que $\gamma_i \otimes \gamma_i - f(\gamma_i)1_T = \gamma_i \otimes \gamma_i + 1_T$, e para γ_0, tem-se que $\gamma_0 \otimes \gamma_0 - f(\gamma_0)1_T =$

$\gamma_0 \otimes \gamma_0 - 1_T$. Como c é um ideal, segue que $\gamma_0 \otimes \gamma_0 - 1_T + \gamma_i \otimes \gamma_i + 1_T = \gamma_0 \otimes \gamma_0 + \gamma_i \otimes \gamma_i \in c$.

Observe agora que $\gamma_0 \otimes \gamma_i + \gamma_i \otimes \gamma_0 + \gamma_i \otimes \gamma_i + \gamma_0 \otimes \gamma_0 = (\gamma_i + \gamma_0) \otimes (\gamma_i + \gamma_0) \in c$, pois $f(\gamma_i + \gamma_0) = 1 - 1 = 0$.

Para $j = 1,\ 2,\ 3$ e $j \neq i$, tem-se que $\gamma_j \otimes \gamma_j + 1_T + \gamma_i \otimes \gamma_i + 1_T = \gamma_j \otimes \gamma_j + \gamma_i \otimes \gamma_i + 2 \cdot 1_T \in c$. Como anteriormente, $\gamma_j \otimes \gamma_i + \gamma_i \otimes \gamma_j + \gamma_i \otimes \gamma_i + \gamma_j \otimes \gamma_j + 2 \cdot 1_T = (\gamma_i + \gamma_j) \otimes (\gamma_i + \gamma_j) + 2 \cdot 1_T \in c$, visto que $f(\gamma_i + \gamma_j) = -2$. □

Adiante, serão usadas as seguintes notações:

$$\dot{\sigma}_i = \gamma_i \gamma_0, \ \ i = 1,\ 2,\ 3, \text{ e } \mathcal{I} = \gamma_0 \gamma_1 \gamma_2 \gamma_3.$$

Queremos, agora, fazer uma ligação entre os estados de q-bits e a álgebra de Clifford. Para isso, lembremos que um estado de um q-bit, $|\psi\rangle$, é um vetor unitário do espaço vetorial complexo $\mathbb{C}^2$, e quando visto como um $\mathbb{R}-$espaço vetorial, tem dimensão 4. Assim, podemos tomar $\{e_0 = (1,0)^t,\ e_1 = (0,i)^t,\ e_2 = (0,1)^t, e_3 = (i,0)^t\}$ como uma $\mathbb{R}-$base de $\mathbb{C}^2$.

Como visto na seção 1.4, podemos ver a álgebra $\mathcal{C}\ell_{1,3}$ como uma álgebra semi-graduada e escrevê-la como $\mathcal{C}\ell_{1,3} = \mathcal{C}\ell_{1,3}^+ \oplus \mathcal{C}\ell_{1,3}^-$, onde $\mathcal{C}\ell_{1,3}^+$ é chamada de álgebra par.

Proposição 2.2.2. *A função*

$$\begin{array}{rccl} \dot{\pi}: & \mathbb{C}^2 & \rightarrow & \mathcal{C}\ell_{1,3}^+ \\ & a = (a_0, a_1, a_2, a_3) & \mapsto & a_0 + \displaystyle\sum_{k=1}^{3} (-1)^{k+1} a_k \mathcal{I} \dot{\sigma}_k \end{array},$$

onde a está escrito na base acima dada, é uma injeção de $\mathbb{C}^2$ em $\mathcal{C}\ell_{1,3}$.

Demonstração. Sejam $a, b \in \mathbb{C}^2$ tais que $\dot{\pi}(a) = \dot{\pi}(b)$ queremos mostrar que $a = b$. Se $a = (a_0, a_1, a_2, a_3)$ e $b = (b_0, b_1, b_2, b_3)$ temos que $0 = \dot{\pi}(a) - \dot{\pi}(b) = a_0 +$

$$\sum_{k=1}^{3}(-1)^{k+1}a_k\mathcal{I}\dot{\sigma}_k - b_0 - \sum_{k=1}^{3}(-1)^{k+1}b_k\mathcal{I}\dot{\sigma}_k = a_0 - b_0 + \sum_{k=1}^{3}(-1)^{k+1}(a_k - b_k)\mathcal{I}\dot{\sigma}_k,$$

logo $a_i = b_i$ para todo i, ou seja, $a = b$. □

Essa função nos dá a ligação entre a álgebra de Clifford em questão e o espaço dos estados quânticos de um q-bit.

Definição 2.2.3 (Reversão). *Dado um elemento ψ na álgebra de Clifford $\mathcal{C}\ell_{1,3}$, definimos sua reversão, denotada por $\breve{\psi}$, como sendo a inversão da ordem dos produtos dos elementos da base no qual ψ está escrito, ou seja, se $\psi = \prod_{i=1}^{n}\gamma_i$, então $\breve{\psi} = \prod_{i=0}^{n-1}\gamma_{n-i}$. Por exemplo, se $\psi = \gamma_1\gamma_3\gamma_2$, então $\breve{\psi} = \gamma_2\gamma_3\gamma_1$.*

A reversão é útil para definirmos o elemento adjunto em $\mathcal{C}\ell_{1,3}$, o qual também está incluso no mesmo espaço.

Definição 2.2.4 (Adjunto). *Dado um elemento $\psi \in \mathcal{C}\ell_{1,3}$, definimos o seu adjunto, ψ^*, como sendo:*

$$\psi^* = \gamma_0\breve{\psi}\gamma_0.$$

Outra função importante é a função escalar definida a seguir.

Definição 2.2.5. *Definimos a função $\langle\cdot\rangle_0 : \mathcal{C}\ell_{1,3} \to \mathbb{R}$ da álgebra de Clifford no corpo de escalares, como sendo o escalar que multiplica o elemento neutro da multiplicação da álgebra.*

Observe que a álgebra que construímos neste capítulo é real, logo a função escalar retorna um número real. Mais adiante, transformaremos tal álgebra em complexa, mas manteremos a função escalar com valores no corpo dos números reais.

Nossa idéia é construir um produto interno na álgebra de assinatura (1,3).

Na proposição a seguir, usaremos a função $\dot{\pi}$ (proposição 2.2.2) para relacionar $\mathbb{C}^2$ com $\mathcal{C}\ell_{1,3}^{+}$.

Proposição 2.2.6. *Dados dois elementos, $|\varphi\rangle$, $|\psi\rangle$, do espaço de estados quânticos de 1 q-bit, a parte real de $\langle\psi||\varphi\rangle$, $\mathfrak{R}(\langle\psi||\varphi\rangle)$, é dada por $\langle\psi^*\varphi\rangle_0$, onde $\psi = \dot{\pi}(|\psi\rangle)$ e $\varphi = \dot{\pi}(|\varphi\rangle)$. E mais, a parte "complexa", $\mathfrak{R}(-i\langle\psi||\varphi\rangle)$, é dada por $\langle-\psi^*\varphi\mathfrak{I}\dot{\sigma}_3\rangle_0$.*

Demonstração. Sejam $|\varphi\rangle = a_1e_0 + b_1e_3 + a_2e_2 + b_2e_1 = (a_1 + ib_1, a_2 + ib_2)^t$ e $|\psi\rangle = c_1e_0 + d_1e_3 + c_2e_2 + d_2e_1 = (c_1 + id_1, c_2 + id_2)^t$ dois vetores complexos, onde $\{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2\} \subset \mathbb{R}$.

Temos que a parte real do produto interno entre $|\psi\rangle$ e $|\varphi\rangle$ é dada por:

$$\mathfrak{R}(\langle\psi||\varphi\rangle) = \mathfrak{R}((a_1 + ib_1)(c_1 - id_1) + (a_2 + ib_2)(c_2 - id_2)) =$$

$$= a_1c_1 + b_1d_1 + a_2c_2 + b_2d_2.$$

Temos também que $\dot{\pi}(|\psi\rangle) = \psi = c_1 + d_1\mathfrak{I}\dot{\sigma}_3 - c_2\mathfrak{I}\dot{\sigma}_2 + d_2\mathfrak{I}\dot{\sigma}_1$, $\dot{\pi}(|\varphi\rangle) = \varphi = a_1 + b_1\mathfrak{I}\dot{\sigma}_3 - a_2\mathfrak{I}\dot{\sigma}_2 + b_2\mathfrak{I}\dot{\sigma}_1$ e $\psi^* = c_1 - d_1\mathfrak{I}\dot{\sigma}_3 + c_2\mathfrak{I}\dot{\sigma}_2 - d_2\mathfrak{I}\dot{\sigma}_1$.

Assim:

$$\psi^*\varphi = (c_1 - d_1\mathfrak{I}\dot{\sigma}_3 + c_2\mathfrak{I}\dot{\sigma}_2 - d_2\mathfrak{I}\dot{\sigma}_1)(a_1 + b_1\mathfrak{I}\dot{\sigma}_3 - a_2\mathfrak{I}\dot{\sigma}_2 + b_2\mathfrak{I}\dot{\sigma}_1) =$$

$$\begin{gathered}(a_1c_1 + b_1d_1 + a_2c_2 + b_2d_2)\\ +c_1(b_1\mathfrak{I}\dot{\sigma}_3 - a_2\mathfrak{I}\dot{\sigma}_2 + b_2\mathfrak{I}\dot{\sigma}_1)\\ -d_1\mathfrak{I}\dot{\sigma}_3(a_1 - a_2\mathfrak{I}\dot{\sigma}_2 + b_2\mathfrak{I}\dot{\sigma}_1)\\ +c_2\mathfrak{I}\dot{\sigma}_2(a_1 + b_1\mathfrak{I}\dot{\sigma}_3 + b_2\mathfrak{I}\dot{\sigma}_1)\\ -d_2\mathfrak{I}\dot{\sigma}_1(a_1 + b_1\mathfrak{I}\dot{\sigma}_3 - a_2\mathfrak{I}\dot{\sigma}_2).\end{gathered}$$

Logo $\langle \psi^* \varphi \rangle_0 = a_1 c_1 + b_1 d_1 + a_2 c_2 + b_2 d_2$, o que completa a demonstração da primeira parte.

A demonstração é análoga para encontrar a parte complexa. $\square$

Da proposição acima e como $\langle \psi | | \varphi \rangle = \Re(\langle \psi | | \varphi \rangle) - i\Re(\langle \psi | | i\varphi \rangle)$, podemos definir um produto interno entre os elementos da álgebra $\mathcal{C}\ell_{1,3}^+$ como sendo:

$$\langle \psi, \varphi \rangle_0 = \langle \psi^* \varphi \rangle_0 - \langle \psi^* \varphi \mathcal{I} \dot{\sigma}_3 \rangle_0 \mathcal{I} \dot{\sigma}_3.$$

Observe que aqui fazemos uma analogia entre o número complexo i e o elemento $\mathcal{I}\dot{\sigma}_3$ da álgebra $\mathcal{C}\ell_{1,3}$. Assim como o número complexo i, $\mathcal{I}\dot{\sigma}_3$ é tal que seu quadrado é -1, dando sentido à analogia.

Retornando à função $\dot{\pi}$ e com a analogia acima, podemos considerar a função apenas na base $\{e_0 = (1, 0)^t, e_2 = (0, 1)^t\}$ e fazer $\dot{\pi}(i\,|\phi\rangle) = \dot{\pi}(|\phi\rangle)\mathcal{I}\dot{\sigma}_3$.

Na subseção 1.7.3, descrevemos as matrizes de Pauli e mostramos que elas geram o espaço das matrizes de ordem 2, com entradas no corpo dos números complexos e como corpo de escalares o conjunto dos números reais. Esse espaço gerado tem dimensão 8. Além disso concluímos que tal álgebra é isomorfa à álgebra de Clifford $\mathcal{C}\ell_3$.

Proposição 2.2.7. *A álgebra de Clifford $\mathcal{C}\ell_3$ é isomorfa à álgebra par $\mathcal{C}\ell_{1,3}^+$.*

Demonstração. O primeiro fato a observar é que ambas as álgebras são reais, ou seja, o anel de escalares é o corpo dos números reais. Também temos que $\{\dot{\sigma}_1, \dot{\sigma}_2, \dot{\sigma}_3\}$ gera $\mathcal{C}\ell_{1,3}^+$ como álgebra. De fato, como $\gamma_i \gamma_j = -\dot{\sigma}_i \dot{\sigma}_j$, qualquer elemento de comprimento par pode ser gerado por esses elementos.

Lembrando que $\mathcal{C}\ell_3$ tem como base o conjunto $\{1, e_1, e_2, e_3, e_i \otimes e_j, e_1 \otimes e_2 \otimes e_3\}$, considerando a transformação T dada por:

$$\begin{array}{rccl} \mathsf{T}: & \mathcal{C}\ell_3 & \rightarrow & \mathcal{C}\ell_{1,3}^{+} \\ & \displaystyle\sum_i \bigotimes_j a_{ij} e_j & \mapsto & \displaystyle\sum_i \prod_j a_{ij}\gamma_j\gamma_0 = \sum_i \prod_j a_{ij}\dot{\sigma}_j \,, \end{array}$$

encontramos o isomorfismo entre às álgebras. De fato, primeiro observamos que a transformação leva base em base (como espaço vetorial) e ambas bases têm cardinalidade 8. Logo, já tem-se um isomorfismo de espaços vetoriais, bastando apenas montar a tabela de multiplicação, como foi feito em 1.7.3, para concluir o resultado. □

2.3 Aumentando a Dimensão

Como queremos trabalhar com estados quânticos de dimensões maiores, ou seja, estados de n q-bits, vamos generalizar a forma quadrática vista na seção 2.2. Anteriormente, usamos o espaço vetorial real de dimensão 4. Consideraremos agora espaços vetoriais de dimensão $4n$, com $n \in \mathbb{N}$.

Definição 2.3.1. *Sejam* V *um espaço vetorial real de dimensão* $4n$*, com* $n \in \mathbb{N}$*, e* $B = \{e_{ji}\}$*, com* $i \in \{0, 1, 2, 3\}$ *e* $j \in \{1, \ldots, n\}$*, uma base para* V*. Definimos a forma quadrática* $f : V \to \mathbb{R}$ *a ser utilizada como sendo:*

$$f(x) = \sum_{j=1}^{n} \left(x_{j0}^2 - \sum_{1=1}^{3} x_{ji}^2 \right),$$

onde $x = \sum_{i,j} x_{ji} e_{ji}$.

Podemos tomar B *como uma base* β*-ortonormal, onde* β *é a função bilinear associada a* f.

Denotaremos por $\mathcal{C}\ell_{n,3n}$, a álgebra de Clifford $\mathcal{C}\ell(V, f)$, e por $\{\gamma_{ji}\}$, a sua base referente à base B. Vejamos agora algumas propriedades dessa álgebra.

Proposição 2.3.2. *Em $\mathcal{C}\ell_{n,3n}$, tem-se que $\gamma_{ji}^2 = -1$, para $i \neq 0$, e $\gamma_{j0}^2 = 1$. Além disso, $\gamma_{ji}\gamma_{kl} = -\gamma_{kl}\gamma_{ji}$ para $j \neq k$ ou $i \neq l$.*

Demonstração. Temos que $f(\gamma_{j0}) = 1$ para todo j, e como $\gamma_{j0} \otimes \gamma_{j0} - f(\gamma_{j0})1 = 0$, $\gamma_{j0}^2 = 1$. Para $i \neq 0$, $f(\gamma_{ji}) = -1$, logo $\gamma_{ji}^2 = -1$.

Sejam T a álgebra tensorial de V e c o ideal tal que $\mathcal{C}\ell_{n,3n} = T/c$. Temos que $\gamma_{j0} \otimes \gamma_{j0} - 1 \in c$ e para $i \neq 0$, $\gamma_{ki} \otimes \gamma_{ki} + 1 \in c$, segue que $\gamma_{j0} \otimes \gamma_{j0} + \gamma_{ki} \otimes \gamma_{ki} \in c$.

Vemos que $\gamma_{j0} \otimes \gamma_{ki} + \gamma_{ki} \otimes \gamma_{j0} + \gamma_{j0} \otimes \gamma_{j0} + \gamma_{ki} \otimes \gamma_{ki} = (\gamma_{j0} + \gamma_{ki}) \otimes (\gamma_{j0} + \gamma_{ki}) \in c$, pois $f(\gamma_{j0} + \gamma_{ki}) \in c) = 0$.

Agora sejam $j \neq k$ ou $l \neq i$ e $l, i \neq 0$. $\gamma_{ki} \otimes \gamma_{ki} + f(\gamma_{ki}) + \gamma_{jl} \otimes \gamma_{jl} + f(\gamma_{jl}) = \gamma_{ki} \otimes \gamma_{ki} + \gamma_{jl} \otimes \gamma_{jl} + 2 \in c$. Por outro lado temos que $\gamma_{ki} \otimes \gamma_{ki} + \gamma_{ki} \otimes \gamma_{jl} + \gamma_{jl} \otimes \gamma_{ki} + \gamma_{jl} \otimes \gamma_{jl} + 2 = (\gamma_{ki} + \gamma_{jl}) \otimes (\gamma_{ki} + \gamma_{jl}) + 2 \in c$, pois $f(\gamma_{ki} + \gamma_{ki}) = -2$. □

De maneira similar ao que foi feito anteriormente, denotamos aqui $\dot{\sigma}_{ji} = \gamma_{ji}\gamma_{j0}$, onde $i \in \{1, 2, 3\}$ e $j \in \{1, \ldots, n\}$.

Introduziremos agora a noção de correlator quântico na álgebra de Clifford $\mathcal{C}\ell_{n,3n}$, o que nos permitirá considerar o ideal gerado por esse correlator como uma álgebra complexa.

Definimos o correlator quântico E_n como:

$$E_n = \prod_{k=2}^{n} \frac{1}{2} \left(1 - \mathcal{J}_1 \dot{\sigma}_{13} \mathcal{J}_k \dot{\sigma}_{k3}\right),$$

onde $\mathcal{J}_t = \gamma_{t0}\gamma_{t1}\gamma_{t2}\gamma_{t3}$, $t = 1, \ldots, n$.

Proposição 2.3.3. *O correlator quântico é um elemento idempotente, ou seja, $E_n^2 = E_n$.*

Demonstração. Observemos que

$$\left(\frac{1}{2}(1 - \mathcal{J}_1 \dot{\sigma}_{13} \mathcal{J}_k \dot{\sigma}_{k3})\right)^2 = \frac{1}{4}\left(1 + (\mathcal{J}_1 \dot{\sigma}_{13} \mathcal{J}_k \dot{\sigma}_{k3})^2 - 2\mathcal{J}_1 \dot{\sigma}_{13} \mathcal{J}_k \dot{\sigma}_{k3}\right) =$$

$$= \frac{1}{4}(1 + 1 - 2\mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3}) = \frac{1}{2}(1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3}).$$

Logo, o quadrado de cada termo é o próprio termo. Como cada elemento da multiplicação está dentro da álgebra par, $\mathcal{C}\ell^+_{n,3n}$, e os elementos de um termo são distintos dos do outro termo, a menos do 1, eles comutam entre si. Ou seja, concluímos que E_n é idempotente. □

Proposição 2.3.4. *A multiplicação à esquerda de* E_n *por* $\mathcal{I}_k\dot{\sigma}_{k3}$ *independe do índice* k.

Demonstração. Novamente, lembremos que cada elemento envolvido na multiplicação faz parte da álgebra par $\mathcal{C}\ell^+_{n,3n}$ e tem as mesmas características da demonstração acima. Logo, também comutam entre si. Para cada k fixo, temos:

$$(1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3})\,\mathcal{I}_k\dot{\sigma}_{k3} = \mathcal{I}_k\dot{\sigma}_{k3} - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3}\mathcal{I}_k\dot{\sigma}_{k3} = \mathcal{I}_k\dot{\sigma}_{k3} + \mathcal{I}_1\dot{\sigma}_{13}$$

e

$$(1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3})\,\mathcal{I}_1\dot{\sigma}_{13} = \mathcal{I}_1\dot{\sigma}_{13} - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3}\mathcal{I}_1\dot{\sigma}_{13} = \mathcal{I}_k\dot{\sigma}_{k3} + \mathcal{I}_1\dot{\sigma}_{13}.$$

Ou seja, multiplicar por $\mathcal{I}_k\dot{\sigma}_{k3}$ é o mesmo que multiplicar por $\mathcal{I}_1\dot{\sigma}_{13}$. Como o resultado é válido para qualquer k, segue que $E_n\mathcal{I}_k\dot{\sigma}_{k3} = E_n\mathcal{I}_t\dot{\sigma}_{t3}$. □

Para obtermos uma “estrutura complexa” em $\mathcal{C}\ell^+_{n,3n}$ notemos que $J_n^2 = -E_n$, onde $J_n = E_n\mathcal{I}_k\dot{\sigma}_{k3}$.

Queremos agora projetar o espaço $\mathbb{C}^{2n}$ na álgebra de Clifford $\mathcal{C}\ell_{n,3n}$. Para isso, vamos generalizar a função $\dot{\pi}$. Usaremos as notações $|+\rangle = (1, 0)^t$ e $|-\rangle = (0, 1)^t$. Além disso quando estiver escrito $|\pm\rangle$, $|+\rangle$ ou $|-\rangle$ podem ocorrer.

Proposição 2.3.5. *Considere a função*

$$\begin{array}{rccc} \dot{\pi}: & \mathbb{C}^{2^n} & \rightarrow & \mathcal{C}\ell^+_{n,3n} \\ & |\phi\rangle = \displaystyle\sum_{j=1}^{2^n} \alpha_{\lambda_j} \bigotimes_{i=1}^{n} |i_j\rangle & \mapsto & \displaystyle\sum_{j=1}^{2^n} \alpha_{\lambda_j} \left(\prod_{i=1}^{n} \varphi(|i_j\rangle, i) \right) E_n, \end{array}$$

onde $\alpha_{\lambda_j} \in \mathbb{R}$, $\lambda_j = (1_j, \cdots, n_j)$, $i_j \in \{+,-\}$, $\varphi(|-\rangle, i) = -\mathcal{J}_i \dot{\sigma}_{i2}$, $\varphi(|+\rangle, i) = 1$ *e a estrutura complexa é completada fazendo* $\dot{\pi}(i\,|\psi\rangle) = \dot{\pi}(|\psi\rangle)J_n$. *Essa função é uma injeção do espaço dos estados de* n *q-bits na álgebra de Clifford* $\mathcal{C}\ell_{n,3n}$.

Demonstração. Fazendo a identificação $\mathcal{J}_k \dot{\sigma}_{k3} = \mathcal{J}_j \dot{\sigma}_{j3}$ temos que $E_n = 1$. Queremos mostrar que a função é injetiva, então seja $|a\rangle = \sum_{j=1}^{2^n} \alpha_{\lambda_j} \bigotimes_{i=1}^{n} |i_j\rangle$ e $|b\rangle = \sum_{j=1}^{2^n} \beta_{\lambda_j} \bigotimes_{i=1}^{n} |i_j\rangle$. Supondo que $\dot{\pi}(|a\rangle) = \dot{\pi}(|b\rangle)$ teremos que

$$\sum_{j=1}^{2^n} \alpha_{\lambda_j} \left(\prod_{i=1}^{n} \varphi(|i_j\rangle, i) \right) = \sum_{j=1}^{2^n} \beta_{\lambda_j} \left(\prod_{i=1}^{n} \varphi(|i_j\rangle, i) \right)$$

implicando que

$$\sum_{j=1}^{2^n} (\alpha_{\lambda_j} - \beta_{\lambda_j}) \left(\prod_{i=1}^{n} \varphi(|i_j\rangle, i) \right) = 0.$$

Cada produto do tipo $\prod_{i=1}^{n} \varphi(|i_j\rangle, i)$ forma um elemento da base de $\mathcal{C}\ell_{n,3n}$, logo encontramos que $\alpha_{\lambda_j} - \beta_{\lambda_j} = 0$ para todo j, assim temos que $|a\rangle = |b\rangle$, ou seja, a função é injetiva. □

Caminharemos agora para a construção do produto interno associado a essa álgebra. Inicialmente, temos que definir o adjunto de um elemento em $\mathcal{C}\ell_{n,3n}$.

Lembremos que definimos o adjunto de um elemento ψ em $\mathcal{C}\ell_{1,3}$ por $\psi^* = \gamma_0 \breve{\psi} \gamma_0$.

Na verdade, definiremos o adjunto apenas dos elementos da álgebra par $\mathcal{C}\ell^+_{n,3n}$, pois esse é o espaço que nos interessa.

Definição 2.3.6. *Dado um elemento* $\psi \in \mathcal{C}\ell^+_{n,3n}$, *definimos o seu adjunto como sendo* $\psi^* = \left(\prod_{i=1}^{n} \gamma_{i0} \right) \breve{\psi} \left(\prod_{i=1}^{n} \gamma_{i0} \right)$.

Notemos que $E_n \in \mathcal{C}\ell^+_{n,3n}$, $En = \prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3})$, e que se $h = (1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3})$, então $h^* = h = (1 - \mathcal{I}_1\dot{\sigma}_{13}\mathcal{I}_k\dot{\sigma}_{k3})$. Assim, $E_n^* = E_n$ e $E_n^* E_n = E_n^2 = E_n$.

Estamos prontos para definir o produto interno na álgebra par $\mathcal{C}\ell^+_{n,3n}$.

Definição 2.3.7 (Produto Interno)**.** *Dados* $\psi, \phi \in \mathcal{C}\ell^+_{n,3n}$, *com* $\psi = \dot{\pi}(|\psi\rangle)$ *e* $\phi = \dot{\pi}(|\phi\rangle)$, $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2n}$, *o produto interno entre* ψ *e* ϕ *é dado por*

$$\langle \psi, \phi \rangle = \langle E_n \rangle_0^{-1} \left[\langle \psi^* \phi \rangle_0 - \langle \psi^* \phi J_n \rangle_0 J_n \right],$$

onde $\langle E_n \rangle_0 = \dfrac{1}{2^{n-1}}$.

Lembramos que aqui $\mathcal{I}\dot{\sigma}_{k3}$ faz referência à unidade imaginária dos elementos no ideal (E_n) e que o produto interno foi definido apenas para elementos desse ideal. Posteriormente, veremos outra forma de ver a unidade imaginária, relacionada a outro ideal, e com outras finalidades.

Proposição 2.3.8. *Sejam* $|\varphi\rangle, |\phi\rangle \in \mathbb{C}^{2n}$ *e* $\varphi, \psi \in \mathcal{C}\ell^+_{n,3n}$, *com* $\varphi = \dot{\pi}(|\varphi\rangle)$ *e* $\psi = \dot{\pi}(|\psi\rangle)$, *então o produto interno entre* $|\varphi\rangle$ *e* $|\phi\rangle$ *tem o mesmo valor que o produto interno entre* φ *e* ψ, *a menos da unidade imaginária que muda de* i *para* J_n.

Demonstração. Inicialmente, consideraremos o caso mais simples, em $\mathcal{C}\ell_{1,3}$. Sejam $|\varphi\rangle = (a_1 + b_1 i, c_1 + d_1 i)^t$ e $|\psi\rangle = (a_2 + b_2 i, c_2 + d_2 i)^t$ dois vetores em $\mathbb{C}^2$. Temos que:

$$\dot{\pi}(|\varphi\rangle) = \varphi = a_1 + d_1\mathcal{I}\dot{\sigma}_1 - c_1\mathcal{I}\dot{\sigma}_2 + b_1\mathcal{I}\dot{\sigma}_3,$$

$$\dot{\pi}(|\psi\rangle) = \psi = a_2 + d_2\mathcal{I}\dot{\sigma}_1 - c_2\mathcal{I}\dot{\sigma}_2 + b_2\mathcal{I}\dot{\sigma}_3$$

e

$$\psi^* = a_2 - d_2\mathcal{I}\dot{\sigma}_1 + c_2\mathcal{I}\dot{\sigma}_2 - b_2\mathcal{I}\dot{\sigma}_3.$$

Continuando, verificamos que:

$$\langle \psi^* \varphi \rangle_0 = a_1 a_2 + d_1 d_2 + c_1 c_2 + b_1 b_2$$

e

$$\langle \psi^* \varphi \mathcal{J} \dot{\sigma}_3 \rangle_0 = a_1 + b_2 - d_1 c_2 + c_1 d_2 - b_1 a_2.$$

Assim, $\langle \psi, \varphi \rangle = a_1 a_2 + d_1 d_2 + c_1 c_2 + b_1 b_2 - (a_1 + b_2 - d_1 c_2 + c_1 d_2 - b_1 a_2) \mathcal{J} \dot{\sigma}_3$ que é o mesmo valor de $\langle \psi | | \varphi \rangle$ com a substituição de i por $J_n = \mathcal{J} \dot{\sigma}_3$.

Lembramos agora que se v_1, v_2, w_1 e w_2 são vetores, então $(v_1^t \otimes w_1^t)(v_2 \otimes w_2) = (v_1^t v_2) \otimes (w_1^t w_2)$. Assim podemos perceber que o produto interno em um espaço que é formado por produtos tensoriais de espaços componentes é o mesmo que o produto dos resultados de cada um desses espaços componentes.

Observamos que se $\langle \alpha_k \rangle_0 = 0$ e $\langle \alpha_j \rangle_0 = 0$ com α_j e α_k não nulos pertencentes a parte j e k, respectivamente, $j \neq k$, então $\langle \alpha_j \alpha_k \rangle_0 = 0$. Assim, calcular o produto interno em E_n é o mesmo que calcular em cada parte e depois multiplicar os resultados, o que conclui a demonstração. $\square$

2.4 O Espaço dos Operadores Densidade

Como observamos anteriormente, os estados quânticos são levados em um ideal na álgebra par $\mathcal{C}\ell^+_{n,3n}$, gerado por $E_n = \displaystyle\prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{J}_1 \dot{\sigma}_{13} \mathcal{J}_k \dot{\sigma}_{k3})$.

Criaremos agora outro ideal, onde poderemos identificar todos os $\mathcal{J}_k = \gamma_{k0}\gamma_{k1}\gamma_{k2}\gamma_{k3}$. Tal ideal também é principal, gerado pelo elemento $C_n = \displaystyle\prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{J}_1 \mathcal{J}_k)$.

Proposição 2.4.1. *Seja* $\mathrm{ann}(C_n)$[2] *o anulador do ideal* $(C_n) = \{aC_n; a \in \mathcal{C}\ell^+_{n,3n}\}$. *Então* $\mathcal{C}\ell^+_{n,3n}/\mathrm{ann}(C_n)$ *é isomorfo à* (C_n).

[2]Denotamos por $\mathrm{ann}(A)$ o conjunto anulador de $A \in M$, onde M é uma álgebra, $\mathrm{ann}(A) = \{m \in M; mA = 0\}$.

Demonstração. [Lan97]. □

O ideal $\mathfrak{ann}(C_n)$ é gerado pelos elementos da forma $(\mathcal{J}_1 - \mathcal{J}_k)$, pois $(1 - \mathcal{J}_1\mathcal{J}_k)(\mathcal{J}_1 - \mathcal{J}_k) = 0$, onde $(1 - \mathcal{J}_1\mathcal{J}_k)$ é divisor de C_n . Observado isso, temos que as projeções dos $\mathcal{J}_k$ em (C_n) são identificadas[3], pois $\mathcal{J}_k - \mathcal{J}_j \in \mathfrak{ann}(C_n)$ implicando que $\mathcal{J}_k \equiv \mathcal{J}_j$ em (C_n) . Tal identificação é importante, pois a princípio, $\mathcal{C}\ell_{n,3n}$ é uma álgebra real. Entretanto, quando identificamos os pseudoescalares de cada parte[4] como sendo o mesmo, transformamos o ideal (C_n) em uma $\mathbb{C}-$ álgebra. Com esse outro ideal, estamos prontos para construir a versão dos operadores densidade na álgebra de Clifford em questão.

Lembrando que os operadores densidade são da forma $\sum_i a_i |i\rangle\langle i|$, consideraremos inicialmente o termo $|i\rangle\langle i|$.

O elemento idempotente $H_+ = \prod_{k=1}^{n} \frac{1}{2}(1 + \dot{\sigma}_{k3})$ é útil na definição dos operadores densidade na álgebra de Clifford. H_+ é equivalente à matriz diagonal cujo único elemento não nulo está na posição (1,1) e tem valor 1. Tal matriz é dada por:

$$\bigotimes_{i=1}^{n} \frac{(I + \sigma_3)}{2}$$

onde σ_3 é uma matriz de Pauli.

Definição 2.4.2. *Seja* $|i\rangle \in \mathbb{C}^{2^n}$*, associado ao operador densidade* $P = |i\rangle\langle i|$*. Definimos o operador densidade equivalente a* P *na álgebra de assinatura* $(n, 3n)$ *como* $\rho = \dot{\pi}(|i\rangle)H_+(\dot{\pi}(|i\rangle))^* C_n$*. Ou seja, consideramos os operadores densidade como elementos do ideal* (C_n)*.*

Na definição acima, levamos o estado para a álgebra, multiplicamos pelo seu

[3]Falamos que identificamos $\mathcal{J}_k$ com $\mathcal{J}_j$ pois no anel quociente $\mathcal{C}\ell_{n,3n}/\mathfrak{ann}(C_n)$, $\mathcal{J}_k$ e $\mathcal{J}_j$ representam a mesma classe de equivalência e assim denotamos $\mathcal{J}_k \equiv \mathcal{J}_j$.

[4] Estamos chamando de parte k ao conjunto gerado por elementos da forma γ_{kj}, onde $j \in \{0, 1, 2, 3\}$.

conjugado e fazemos sua projeção no ideal gerado por C_n.

Novamente, ressaltamos que os elementos C_n, H_+ e E_n são idempotentes e $E_n^* = E_n$.

No caso geral temos que os operadores densidade são da forma:

Definição 2.4.3. *Seja* $P = \sum_j \alpha_j |j\rangle\langle j|$, *o operador densidade associado ao ensemble* $\{(\alpha_j, |j\rangle)\}$. *Definimos o operador densidade equivalente a* P *em* $\mathcal{C}\ell^+_{n,3n}$ *como* $\rho = \sum_j (a_j + b_j\mathcal{I})\rho_j$, *onde* $\alpha_j = a_j + b_j i$ *e* ρ_j *é o operador densidade equivalente a* $|j\rangle\langle j|$.

Veremos agora como ficam os operadores da forma $|\psi\rangle\langle\phi|$.

Definição 2.4.4. *Seja* P *um operador da forma* $P = |\psi\rangle\langle\phi|$, *onde* $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2n}$. *Definimos o seu associado na álgebra de assinatura* $(n, 3n)$ *como:*

$$\rho = \dot{\pi}(|\psi\rangle)H_+\dot{\pi}(|\phi\rangle)^*C_n.$$

Vimos acima como levar qualquer matriz de $\mathrm{Mat}(2n, \mathbb{C})$ na álgebra de assinatura $(n, 3n)$. Veremos agora uma proposição que nos dá um outro modo de de fazer isso. Mais adiante, concluiremos que ambos são equivalentes.

Proposição 2.4.5. *Identificando* $a + bi \in \mathbb{C}$ *com* $a + b\mathcal{I} \in \mathcal{C}\ell^+_{1,3}$, *as álgebras* $\mathrm{Mat}(2, \mathbb{C})$ *e* $\mathcal{C}\ell^+_{1,3}$ *são isomorfas.*

Demonstração. $\mathrm{Mat}(2, \mathbb{C})$ tem dimensão 4 sobre $\mathbb{C}$ e o conjunto $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ é uma $\mathbb{C}$-base, como espaço vetorial, para esse espaço. Notemos também que $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3, i\sigma_0, i\sigma_1, i\sigma_2, i\sigma_3\}$ é uma $\mathbb{R}-$ base para esse mesmo espaço.

Sejam $v = \sum_{j=0}^{3}(a_j + b_j i)\sigma_j$ e

$$\begin{array}{rccl} \ddot{\pi}: & \mathsf{Mat}(2,\mathbb{C}) & \to & \mathcal{C}\ell_{1,3}^{+} \\ & v & \mapsto & \sum_{j=0}^{3}(a_j + b_j \mathcal{I})\dot{\sigma}_j. \end{array}$$

Mostraremos que $\ddot{\pi}$ é um isomorfismo.

Primeiro notemos que com a troca do número complexo i por $\mathcal{I}$ a função $\ddot{\pi}$ é linear, se $v = \sum_{j=0}^{3}(a_j + b_j i)\sigma_j$ e $w = \sum_{j=0}^{3}(c_j + d_j i)\sigma_j$, segue que $v + w = \sum_{j=0}^{3}(a_j + c_j + (b_j + d_j)i)\sigma_j$, implicando que $\ddot{\pi}(v + w) = \sum_{j=0}^{3}(a_j + c_j + (b_j + d_j)\mathcal{I})\dot{\sigma}_j = \sum_{j=0}^{3}(a_j + b_j\mathcal{I})\dot{\sigma}_j + \sum_{j=0}^{3}(c_j + d_j\mathcal{I})\dot{\sigma}_j = \ddot{\pi}(v) + \ddot{\pi}(w)$. Também é fácil ver que $\ddot{\pi}(\alpha v) = \alpha\ddot{\pi}(v)$ com $\alpha \in \mathbb{C}$ e as devidas alterações no número complexo. Assim a linearidade é comprovada.

Se $v \in \mathsf{Ker}(\ddot{\pi})$, temos que

$$\ddot{\pi}(v) = 0 \Leftrightarrow \sum_{j=0}^{3}(a_j + b_j\mathcal{I})\dot{\sigma}_j = 0 \Leftrightarrow (a_j + b_j\mathcal{I}) = 0 \ \forall j \Leftrightarrow a_j = b_j = 0 \ \forall j \Leftrightarrow v = 0.$$

Segue que $\ddot{\pi}$ é injetiva.

É fácil observar que $\ddot{\pi}$ também é sobrejetiva. Falta então mostrar que $\ddot{\pi}(vw) = \ddot{\pi}(v)\ddot{\pi}(w)$.

Sejam $v = \sum_{j=0}^{3} x_j\sigma_j$ e $w = \sum_{j=0}^{3} y_j\sigma_j$, onde $x_j = (a_j + b_j i)$ e $y_j = (c_j + d_j i)$

para todo j. Calculando o produto vw temos:

$$\begin{aligned}
\left(\sum_{j=0}^{3} x_j\sigma_j\right)\left(\sum_{j=0}^{3} y_j\sigma_j\right) &= \\
&(x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3)\sigma_0 + (x_0y_1 + a_1y_0)\sigma_1 \\
&+(x_0y_2 + x_2y_0)\sigma_2 + (x_0y_3 + x_3y_0)\sigma_3 \\
&+(x_2y_3 - x_3y_2)\sigma_2\sigma_3 + (x_1y_2 - x_2y_1)\sigma_1\sigma_2 \\
&+(x_1y_3 - x_3y_1)\sigma_1\sigma_3 \\
&= (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3)\sigma_0 \\
&+(x_0y_1 + x_1y_0 + x_2y_3 i - x_3y_2 i)\sigma_1 \\
&+(x_0y_2 + x_2y_0 + x_1y_3 i - x_3y_1 i)\sigma_2 \\
&+(x_0y_3 + x_3y_0 + x_1y_2 i - x_1y_2 i)\sigma_3.
\end{aligned}$$

Assim:

$$\begin{aligned}
\ddot{\pi}(vw) &= (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3)\dot{\sigma}_0 + \\
&(x_0y_1 + x_1y_0 + x_2y_3\mathcal{I} - x_3y_2\mathcal{I})\dot{\sigma}_1 + \\
&(x_0y_2 + x_2y_0 + x_1y_3\mathcal{I} - x_3y_1\mathcal{I})\dot{\sigma}_2 + \\
&(x_0y_3 + x_3y_0 + x_1y_2\mathcal{I} - x_1y_2\mathcal{I})\dot{\sigma}_3 \\
&= (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3)\dot{\sigma}_0 + (x_0y_1 + a_1y_0)\dot{\sigma}_1 + \\
&(x_0y_2 + x_2y_0)\dot{\sigma}_2 + (x_0y_3 + x_3y_0)\dot{\sigma}_3 + \\
&(x_2y_3 - x_3y_2)\dot{\sigma}_2\dot{\sigma}_3 + (x_1y_2 - x_2y_1)\dot{\sigma}_1\dot{\sigma}_2 + \\
&(x_1y_3 - x_3y_1)\dot{\sigma}_1\dot{\sigma}_3 \\
&= \left(\sum_{j=0}^{3} x_j\dot{\sigma}_j\right)\left(\sum_{j=0}^{3} y_j\dot{\sigma}_j\right) \\
&= \ddot{\pi}(v)\ddot{\pi}(w).
\end{aligned}$$

Ou seja, de fato, $\ddot{\pi}$ é um isomorfismo de álgebras. $\square$

$\Diamond\clubsuit\spadesuit\heartsuit$

"In mathematics you don't understand things. You just get used to them"

John Von Neumann

Capítulo 3

Positividade

Este capítulo é dedicado à construção formal dos operadores densidade na álgebra de Clifford de assinatura $(n, 3n)$. Além disso, mostraremos a equivalência entre tais operadores e o que já foi feito no capítulo anterior. A principal contribuição desta tese encontra-se neste capítulo quando damos uma definição para elementos positivos definidos e como consequência para operadores densidade na álgebra de Clifford.

3.1 O Ideal (C_n)

O objetivo dessa seção é mostrar que o ideal (C_n) é isomorfo à álgebra de matrizes $\mathrm{Mat}(2^n, \mathbb{C})$. Lembramos que $C_n = \prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{J}_1\mathcal{J}_k)$ e que estamos vendo (C_n) como um ideal de $\mathcal{C}\ell^+_{n,3n}$.

O primeiro fato a observar é que como $(\mathcal{J}_1 - \mathcal{J}_k)C_n = 0$, $(\mathcal{J}_1 - \mathcal{J}_k) \in \mathrm{ann}(C_n)$. Ou seja, multiplicar C_n por $\mathcal{J}_1$ é o mesmo que multiplicar por $\mathcal{J}_k$. Isto permite identificar todos os $\mathcal{J}_k$ e assim passar a denotá-los por $\mathcal{J}$.

Teorema 3.1.1. *O conjunto* $\{\underline{\dot{\sigma}}_i C_n\}$*, onde* $\underline{\dot{\sigma}}_i = \prod_{k=1}^{n} \dot{\sigma}_{k i_k}$ *e* $i_k \in \{0, 1, 2, 3\}$*, é linearmente independente em* (C_n)*.*

Demonstração. Expandindo $\prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{I}_1 \mathcal{I}_k)$, obtemos:

$$\begin{aligned} C_n &= \frac{1}{2^n} \Bigg(1 - \sum_{i_1, i_2} \mathcal{I}_{i_1} \mathcal{I}_{i_2} + \sum_{i_1, i_2, i_3, i_4} \mathcal{I}_{i_1} \mathcal{I}_{i_2} \mathcal{I}_{i_3} \mathcal{I}_{i_4} \\ &+ \cdots + (-1)^{\lfloor \frac{n}{2} \rfloor} \sum_{i_1, \ldots, i_{2\lfloor \frac{n}{2} \rfloor}} \mathcal{I}_{i_1} \cdots \mathcal{I}_{i_{2\lfloor \frac{n}{2} \rfloor}} \Bigg), \end{aligned}$$

onde $\lfloor \cdot \rfloor$ é a função que retorna o maior inteiro menor ou igual ao valor dado.

Temos que provar que $\sum (a_i + b_i \mathcal{I}) \underline{\dot{\sigma}}_i C_n = 0 \Rightarrow a_i + b_i \mathcal{I} = 0 \ \forall i$. Reescrevendo somatório, temos:

$$\sum_i (a_i + b_i \mathcal{I}) \underline{\dot{\sigma}}_i C_n = 0 \Leftrightarrow \underbrace{\sum_i a_i \underline{\dot{\sigma}}_i}_{(1)} + \underbrace{\sum_{i,j} \mathcal{I}_j b_i \underline{\dot{\sigma}}_i}_{(2)} + H = 0,$$

onde H é a soma dos termos de C_n que contém o produto de pelo menos dois termos da forma $\mathcal{I}_k$.

Observemos que (1) é o único termo da expressão acima que não envolve qualquer tipo de $\mathcal{I}_k$, implicando que nenhum outro termo que apareça em (2) ou H pode anular (1). Logo, devemos ter $a_i = 0$ para todo i.

Em (2), aparecem apenas somas de $\mathcal{I}_k$ e não produtos deles, implicando que nenhum termo em H pode anular (2). Portanto, $b_i = 0$ para todo i, o que conclui a demonstração.

□

Veremos agora que o ideal (C_n) é isomorfo à álgebra de matrizes $Mat(2^n, \mathbb{C})$.

Para isso precisamos generalizar a função $\ddot{\pi}$, dada na demonstração da proposição 2.4.5. Ou seja,

Teorema 3.1.2. *A transformação linear*

$$\begin{array}{rccc} \ddot{\pi}: & Mat(2^n, \mathbb{C}) & \longrightarrow & \mathcal{C}\ell^+_{n,3n} \\ & \displaystyle\sum_\theta (a_\theta + b_\theta i) \bigotimes_{j=1}^{n} \sigma_{k_j} & \longmapsto & \displaystyle\left(\sum_\theta (a_\theta + b_\theta \mathcal{J}) \prod_{j=1}^{n} \dot{\sigma}_{jk_j} \right) c_n, \end{array}$$

é sobrejetiva sobre (C_n) *e* $\ddot{\pi}(AB) = \ddot{\pi}(A)\ddot{\pi}(B)$.

Demonstração. Começamos a demonstração observando que cada parte[1] k de $\mathcal{C}\ell^+_{n,3n}$ é gerada como uma $\mathbb{R}-$álgebra pelo conjunto $B_k = \{\dot{\sigma}_{kj}, \mathcal{J}_k\dot{\sigma}_{kj}\}$, que tem 8 elementos.

Se $A \in \mathcal{C}\ell^+_{n,3n}$, temos que $A = \displaystyle\sum_\sigma c_\sigma \prod_{k=1}^{n} \beta_{k_j}$, onde $\beta_{k_j} \in B_k$. Também temos que se $\dot{A} \in (C_n)$, então $\dot{A} = AC_n$, para algum $A \in \mathcal{C}\ell^+_{n,3n}$. Lembrando que identificamos todos os $\mathcal{J}_k$, temos que:

$$\dot{A} = \left(\sum_\sigma c_\sigma \prod_{k=1}^{n} \beta_{k_j} \right) C_n = \sum_\theta (a_\theta + b_\theta \mathcal{J}) \prod_{l=1}^{n} \dot{\sigma}_{lj_l}.$$

Assim, se tomarmos $H = \displaystyle\sum_\theta (a_\theta + b_\theta i) \bigotimes_{l=1}^{n} \sigma_{j_l}$, temos que $\ddot{\pi}(H) = \dot{A}$. Ou seja, $\ddot{\pi}$ é sobrejetiva.

Mostraremos agora a segunda parte do teorema.

A tabela de multiplicação da parte k no ideal C_n é dada por:

C_n	$\dot{\sigma}_{k1}C_n$	$\dot{\sigma}_{k2}C_n$	$\dot{\sigma}_{k3}C_n$
$\dot{\sigma}_{k1}C_n$	$-C_n$	$\dot{\sigma}_{k1}\dot{\sigma}_{k2}C_n$	$\dot{\sigma}_{k1}\dot{\sigma}_{k3}C_n$
$\dot{\sigma}_{k2}C_n$	$-\dot{\sigma}_{k1}\dot{\sigma}_{k2}C_n$	$-C_n$	$\dot{\sigma}_{k2}\dot{\sigma}_{k3}C_n$
$\dot{\sigma}_{k3}C_n$	$-\dot{\sigma}_{k1}\dot{\sigma}_{k3}C_n$	$-\dot{\sigma}_{k2}\dot{\sigma}_{k3}C_n$	$-C_n$

[1] Estamos chamando de parte k ao conjunto gerado por elementos da forma γ_{kj}, onde $j \in \{0, 1, 2, 3\}$.

Por outro lado a tabela de multiplicações de $\mathsf{Mat}(2,\mathbb{C})$ em relação à base das matrizes de Pauli é:

I	σ_1	σ_2	σ_3
σ_1	$-I$	$\sigma_1\sigma_2$	$\sigma_1\sigma_3$
σ_2	$-\sigma_1\sigma_2$	$-I$	$\sigma_2\sigma_3$
σ_3	$-\sigma_1\sigma_3$	$-\sigma_2\sigma_3$	$-I$

Dos fatos $(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$ e $\dot{\sigma}_{kj}\dot{\sigma}_{li} = \dot{\sigma}_{li}\dot{\sigma}_{kj}$ para $k \neq l$, concluímos que a tabela de multiplicações da base de (C_n) equivale a tabela de multiplicações da base de $\bigotimes^n \mathsf{Mat}(2,\mathbb{C})$ e assim terminamos a demostração deste teorema. $\square$

Dos teoremas 3.1.1 e 3.1.2 temos o seguinte corolário:

Corolário 3.1.3. *O ideal (C_n) é isomorfo à álgebra de matrizes $\mathsf{Mat}(2^n,\mathbb{C})$.*

3.1.1 O Traço

Começaremos aqui analisando o caso mais simples e lembramos que o traço de uma matriz é a soma dos elementos de sua diagonal. Manteremos o conjunto das matrizes de Pauli, $\{\sigma_0,\ \sigma_1,\ \sigma_2,\ \sigma_3\}$, como uma base para o espaço das matrizes $\mathsf{Mat}(2,\mathbb{C})$.

Seja $A \in \mathsf{Mat}(2,\mathbb{C})$. Como $A = \sum_i \alpha_i\sigma_i$, segue que $\mathrm{tr}(A) = \mathrm{tr}\left(\sum_i \alpha_i\sigma_i\right) = \sum_i \mathrm{tr}(\alpha_i\sigma_i) = \sum_i \alpha_i \mathrm{tr}(\sigma_i) = \alpha_0 \mathrm{tr}(\sigma_0) = 2\alpha_0$. Ou seja, o traço da matriz A é dado por duas vezes o escalar que multiplica o primeiro elemento da base acima dada: a matriz identidade.

Visto isso, podemos definir:

Definição 3.1.4. *Dado* $\rho \in \mathcal{C}\ell^+_{1,3}$*, definimos o traço de* ρ *como:*

$$\dot{\mathrm{tr}}(\rho) = 2(\langle\rho\rangle_0 - \langle\rho\mathcal{J}\rangle_0\, i).$$

Como foi definido, o traço retorna um número complexo. Contudo podemos trocar i por $\mathcal{J}$ na definição passando assim a retornar um valor na álgebra, pelo fato de podermos mergulhar o corpo dos números complexos na álgebra $\mathcal{C}\ell^+_{n,3n}$ levando $a + bi$ em $a + b\mathcal{J}$.

Com essa definição, segue o teorema:

Teorema 3.1.5. *Dado* $A \in \mathrm{Mat}(2, \mathbb{C})$*,* $\mathrm{tr}(A) = \alpha$ *se, e somente se,* $\dot{\mathrm{tr}}(\ddot{\pi}(A)) = \alpha$*.*

Demonstração. De fato, basta observar que $\ddot{\pi}(2\alpha\sigma_0) = 2(a + b\mathcal{J})$ onde $\alpha = a + bi$ e que se $\mathrm{tr}(A) = \alpha$, então $A = \dfrac{\alpha}{2}\sigma_0 + \displaystyle\sum_{i=1}^{3} a_i\sigma_i$. Isso nos dá que $\dot{\mathrm{tr}}(\ddot{\pi}(A)) = \alpha$.

O outro lado da demonstração segue os mesmos princípios. □

Passemos agora a descrever o que ocorre no caso geral. Ou seja, o espaço de matrizes envolvido é o $\mathrm{Mat}(2^n, \mathbb{C})$ e a álgebra de Clifford é o $\mathcal{C}\ell^+_{n,3n}$.

Como anteriormente, analisaremos o que acontece com o traço no espaço das matrizes. Para isso, vamos escolher uma base conveniente usando os produtos tensoriais das matrizes de Pauli, n vezes, obtendo uma base com 4^n elementos.

Para o cálculo do traço, somente os elementos que são tensoriais entre σ_0 e σ_3, sem incluir os outros, é que são importantes, pois nos demais elementos, a diagonal é nula. Na realidade, apenas σ_0 é levado em conta, pois $\mathrm{tr}(A \otimes \sigma_3) = \mathrm{tr}(A) - \mathrm{tr}(A) = 0$.

Como feito antes, seja $B = \{\omega_i\}$ a base formada pelos tensoriais mencionados acima, onde $\omega_0 = \bigotimes^n \sigma_0$, ou seja, ω_0 é a matriz identidade. Dado

$A \in \mathrm{Mat}(2^n, \mathbb{C})$, obtemos:

Se $A = \sum_i \alpha_i \omega_i$, temos que

$$\mathrm{tr}(A) = \mathrm{tr}\left(\sum_i \alpha_i \omega_i\right) = \sum_i \mathrm{tr}(\alpha_i \omega_i) = \sum_i \alpha_i \mathrm{tr}(\omega_i) = \alpha_0 \mathrm{tr}(\omega_0) = 2^n \alpha_0.$$

Assim, o traço da matriz A é dado por 2^n vezes o escalar que multiplica o primeiro elemento da base B.

Podemos então definir o traço em (C_n) da seguinte forma:

Definição 3.1.6. *Sendo* $\rho \in (C_n)$, *definimos o traço de* ρ *como:*

$$\dot{\mathrm{tr}}(\rho) = 2^n(\langle\rho\rangle_0 - \langle\rho\mathcal{I}\rangle_0\, i).$$

Também podemos generalizar o teorema 3.1.5.

Teorema 3.1.7. *Dado* $A \in \mathrm{Mat}(2^n, \mathbb{C})$, $\mathrm{tr}(A) = \alpha$ *se, e somente se,* $\dot{\mathrm{tr}}(\ddot{\pi}(A)) = \alpha$.

Demonstração. A demonstração desse teorema segue direto das definições do traço, da função $\ddot{\pi}$ e da decomposição de A em $\sum_i \alpha_i \omega_i$. □

3.2 Positividade em $\mathcal{C}\ell^+_{n,3n}$

Nesta seção apresentaremos uma definição para um elemento semidefinido positivo em $\mathcal{C}\ell^+_{n,3n}$.

Inicialmente, consideramos o caso de 1 q-bit, ou seja, estaremos em $\mathcal{C}\ell^+_{1,3}$. Lembremos que esse espaço é isomorfo ao espaço das matrizes $\mathrm{Mat}(2, \mathbb{C})$.

Lema 3.2.1. *Sejam* $\rho \in (C_n)$ *e* $P = \ddot{\pi}^{-1}(\rho)$, *então a primeira coluna de* P *é não nula se, e só se,* $\dot{\mathrm{tr}}(\rho H_+ \rho^*) \neq 0$.

Demonstração. Suponha que $|\psi\rangle$ seja a primeira coluna de P e faça $H = \bigotimes^{n} \frac{I+\sigma_3}{2}$. Temos que $\dot{\mathrm{tr}}(\rho H_+ \rho^*) = \mathrm{tr}(PHP^*) = \mathrm{tr}(|\psi\rangle\langle\psi|) = \langle\psi||\psi\rangle$. Concluímos que $\dot{\mathrm{tr}}(\rho H_+ \rho^*) \neq 0$ se, e só se, $\langle\psi||\psi\rangle \neq 0$, ou seja, se, e só se, a primeira coluna de P é não nula. □

Definição 3.2.2. *Dizemos que $A \in \mathcal{C}\ell^+_{1,3}$ é definido positivo se, para todo $\beta \in \mathcal{C}\ell^+_{1,3}$, com $\dot{\mathrm{tr}}(\beta H_+ \beta^*) \neq 0$, temos que:*

$$\langle\beta^* A\beta\rangle_0 - \langle\beta^* A\beta\mathcal{I}\rangle_0\, i - \langle\beta^* A\beta\dot{\sigma}_3\rangle_0 + \langle\beta^* A\beta\dot{\sigma}_3\mathcal{I}\rangle_0\, i > 0.$$

Quando ocorre

$$\langle\beta^* A\beta\rangle_0 - \langle\beta^* A\beta\mathcal{I}\rangle_0\, i - \langle\beta^* A\beta\dot{\sigma}_3\rangle_0 + \langle\beta^* A\beta\dot{\sigma}_3\mathcal{I}\rangle_0\, i \geqslant 0,$$

dizemos que A é semidefinido positivo.

Teorema 3.2.3. *Uma matriz $A \in \mathrm{Mat}(2,\mathbb{C})$ é (semi) definida positiva se, e somente se, $\ddot{\pi}(A) \in \mathcal{C}\ell^+_{1,3}$ é (semi) definido positivo.*

Demonstração. Seja $0 \neq v \in \mathbb{C}^2$. Construímos a matriz $V = [v|w]$, onde V tem como colunas o vetor v dado e um outro vetor w qualquer. Se $A \in \mathrm{Mat}(2,\mathbb{C})$ é definida positiva, temos que $v^*Av > 0$. É fácil observar que, $C = V^*AV$ implica que $c_{11} = v^*Av > 0$. Além disso,

$$C = \frac{c_{11}+c_{22}}{2}\sigma_0 + \frac{c_{12}+c_{21}}{2}\sigma_1 + \frac{c_{12}-c_{21}}{2} i\sigma_2 + \frac{c_{11}-c_{22}}{2}\sigma_3.$$

Dado $\dot{\beta} \in \mathcal{C}\ell^+_{1,3}$, temos que $\dot{\beta} = \sum_i \dot{b}_j \dot{\sigma}_j$, onde $\dot{b}_j = b_{j1} + b_{j2}\mathcal{I}$ e $b_{jt} \in \mathbb{R}$. Observamos que $\beta = \sum_j b_j \sigma_j \in \mathrm{Mat}(2,\mathbb{C})$, onde $b_j = b_{j1} + b_{j2} i$, é tal que $\ddot{\pi}(\beta) = \dot{\beta}$.

Sejam $\dot{A} = \ddot{\pi}(A)$, $\dot{X} = \dot{\beta}^*\dot{A}\dot{\beta}$ e $X = \beta^*A\beta$, temos que $\ddot{\pi}(X) = \ddot{\pi}(\beta^*A\beta) = \dot{X}$, além disso $\left\langle\dot{\beta}^*\dot{A}\dot{\beta}\right\rangle_0 - \left\langle\dot{\beta}^*\dot{A}\dot{\beta}\mathcal{I}\right\rangle_0 i - \left\langle\dot{\beta}^*\dot{A}\dot{\beta}\dot{\sigma}_3\right\rangle_0 + \left\langle\dot{\beta}^*\dot{A}\dot{\beta}\dot{\sigma}_3\mathcal{I}\right\rangle_0 i = x_{11} > 0$, assim $\dot{A}$ é definido positivo.

O caso semidefinido positivo segue de maneira análoga.

$\square$

Queremos agora generalizar o que foi feito acima, ou seja, definir quando um elemento em $\mathcal{C}\ell^{+}_{n,3n}$ é definido positivo. Para isso, definimos duas funções auxiliares s e $\dot{s}$, dadas por:

$$\begin{array}{rccl} s: & \mathbb{N}\cup\{0\} & \to & \bigotimes^{n} Mat(2,\mathbb{C}) \\ & k & \mapsto & s(k) = \left(\bigotimes_{i}(\sigma_3)^{x_i}\right)\otimes I \end{array}$$

e

$$\begin{array}{rccl} \dot{s}: & \mathbb{N}\cup\{0\} & \to & \mathcal{C}\ell^{+}_{n,3n} \\ & k & \mapsto & \dot{s}(k) = \prod_{i}(\dot{\sigma}_{i3})^{x_i} \end{array}$$

onde $\sum x_i 2^i$ é a representação binária de k.

Definição 3.2.4. *Dada a função* P*,*

$$\begin{array}{rccl} P: & (C_n) & \to & \mathbb{C} \\ & A & \mapsto & P(A) = \sum_{k=0}^{2^n-1} \langle A\dot{s}(k)\rangle_0 - \sum_{k=0}^{2^n-1} \langle A\dot{s}(k)\mathcal{J}\rangle_0\, i \end{array},$$

dizemos que um elemento $\beta \in (C_n)$ *é definido positivo, se para todo* $\rho \in (C_n)$*,com com* $\dot{tr}(\rho H_+ \rho^*) \neq 0$*, temos que* $P(\rho^*\beta\rho) > 0$*. Quando temos* $P(\rho^*\beta\rho) \geqslant 0$*, falamos que* β *é semidefinido positivo.*

Lembramos que (C_n) é o ideal à direita gerado pelo idempotente $C_n \in \mathcal{C}\ell^{+}_{n,3n}$ e que os elementos $\mathcal{J}_k$ são identificados na multiplicação por C_n, fazendo sentido usar apenas $\mathcal{J}$.

A definição acima é justamente a generalização que queríamos. Enunciaremos agora um teorema que também generaliza o teorema 3.2.3.

Teorema 3.2.5. *Uma matriz* $A \in \mathrm{Mat}(2^n, \mathbb{C})$ *é (semi) definida positiva se, e somente se,* $\ddot{\pi}(A) \in (C_n)$ *é (semi) definido positivo.*

Demonstração. Sejam $X \in \mathrm{Mat}(2^n, \mathbb{C})$ e D a matriz diagonal que tem a mesma diagonal de X. Assim, podemos escrever D como:

$$D = \sum_{j=0}^{2^n-1} \alpha_j s(j),$$

com $\alpha_j = a_j + b_j i \in \mathbb{C}$. Além disso, $D_{11} = \sum_j \alpha_j = a + bi$. Seja $Y = X - D$. Temos que $\ddot{\pi}(Y)$ é tal que $\langle \ddot{\pi}(Y) \rangle_0 = 0$ e $\langle \ddot{\pi}(Y\mathcal{I}) \rangle_0 = 0$, assim encontramos que $\langle \ddot{\pi}(X) \rangle_0 = \langle \ddot{\pi}(D+Y) \rangle_0 = \langle \ddot{\pi}(D) \rangle_0 + \langle \ddot{\pi}(Y) \rangle_0 = \langle \ddot{\pi}(D) \rangle_0 = \left\langle \sum_j a_j \ddot{\pi}(s(j)) \right\rangle_0 = \left\langle \sum_j a_j \dot{s}(j) \right\rangle_0 = a$. Também vale que $\langle \ddot{\pi}(X)\mathcal{I} \rangle_0 = \langle \ddot{\pi}(D)\mathcal{I} \rangle_0 = \left\langle \sum_j b_j \mathcal{I}\dot{s}(j)\mathcal{I} \right\rangle_0 = \left\langle \sum_j -b_j \dot{s}(j) \right\rangle_0 = -b$. Disso concluímos que $P(X) = a + bi = \alpha$.

Para finalizar a demonstração vemos que A é (semi) definida positiva se, e só se, para todo $|\phi\rangle \in \mathbb{C}^{2^n}$ vale que $\langle \phi | A | \phi \rangle > 0$ que é equivalente a exigir que $X_{11} > 0$ onde $X = V^* A V$ e $V = [|\phi\rangle \, |0]$. Assim $P(\ddot{\pi}(V^* A V)) = P(\ddot{\pi}(V)^* \ddot{\pi}(A) \ddot{\pi}(V)) > 0$ se, e só se, $\ddot{\pi}(A)$ é (semi) definido positivo. $\square$

3.3 Operadores Densidade

Como caracterizados em 2.1.4, os operadores densidade são definidos como matrizes em $\mathrm{Mat}(2^n, \mathbb{C})$ semidefinidas positiva, com traço 1. Na seção anterior, vimos como definir positividade para elementos da álgebra de Clifford $\mathcal{C}\ell_{n,3n}$. Agora, veremos que elementos dessa álgebra podemos chamar de operadores densidade.

3.3.1 Operadores Densidade em $\mathcal{C}\ell_{n,3n}$

Chegamos ao ponto onde já é possível definir os operadores densidade em um álgebra de Clifford. Nas seções anteriores, definimos o que seria um elemento positivo e o que seria o traço em uma álgebra de Clifford. De posse dessas informações, podemos definir o seguinte:

Definição 3.3.1. *Chamamos de operadores densidade os elementos* $\rho \in \mathcal{C}\ell_{n,3n}$ *que satisfazem as seguintes condições:*

1. *O elemento pertence a álgebra par,* $\rho \in \mathcal{C}\ell^{+}_{n,3n}$*;*
2. *Esta no ideal* (C_n)*;*
3. ρ *é semidefinido positivo;*
4. *O traço de* ρ *é igual a* 1*;*
5. *Vale que* $\rho = \rho^*$.

3.3.2 Voltando a Falar de Adjunto

Definimos anteriormente que, dado $\beta \in \mathcal{C}\ell_{1,3}$, seu adjunto é dado por :

$$\beta^* = \gamma_0 \breve{\beta} \gamma_0.$$

Observaremos agora que, de fato, essa definição faz sentido.

Teorema 3.3.2. *Seja* $M \in Mat(2, \mathbb{C})$*. Se* T *é a matriz adjunta de* M*, então* $\ddot{\pi}(T) = \ddot{\pi}(M)^*$.

Demonstração. Escrevendo M como $M = \sum_i \alpha_i \sigma_i$, temos que $M^* = \sum_i \overline{\alpha_i} \sigma_i = T$ (lembramos que as matrizes de Pauli são auto-adjuntas). Temos também que

$\ddot{\pi}(M) = \sum_i (\Re(\alpha_i) + \Im(\alpha_i)\mathcal{I})\dot{\sigma}_i$, onde $\Re$ é a função parte real e $\Im$ é a função parte imaginária.

Vejamos agora que $\dot{\sigma}_i = \dot{\sigma}_i^*$ e que $\mathcal{I}^* = -\mathcal{I}$. Por definição, $\dot{\sigma}_i = \gamma_i\gamma_0$ e

$$\dot{\sigma}_i^* = \gamma_0\breve{\dot{\sigma}}_i\gamma_0 = \gamma_0\gamma_0\gamma_i\gamma_0 = \gamma_i\gamma_0 = \dot{\sigma}_i.$$

No mesmo caminho, temos que

$$\mathcal{I}^* = \gamma_0\gamma_3\gamma_2\gamma_1\gamma_0\gamma_0 = \gamma_0\gamma_3\gamma_2\gamma_1 = -\gamma_0\gamma_1\gamma_2\gamma_3 = -\mathcal{I}.$$

Ou seja:

$$\ddot{\pi}(M)^* = \sum_i (\Re(\alpha_i) - \Im(\alpha_i)\mathcal{I})\dot{\sigma}_i.$$

Por outro lado:

$$\ddot{\pi}(T) = \sum_i (\Re(\overline{\alpha}_i) + \Im(\overline{\alpha}_i)\mathcal{I})\dot{\sigma}_i = \sum_i (\Re(\alpha_i) - \Im(\alpha_i)\mathcal{I})\dot{\sigma}_i = \ddot{\pi}(M)^*,$$

o que conclui a demonstração.

□

Vimos então que em $\mathcal{C}\ell_{1,3}$, a definição de adjunto faz sentido. A definição que demos para o adjunto em $\mathcal{C}\ell_{n,3n}$ nada mais é que a definição em $\mathcal{C}\ell_{1,3}$, pensada em cada parte, $\psi^* = \left(\prod_{i=1}^{n}\gamma_{i0}\right)\breve{\psi}\left(\prod_{i=1}^{n}\gamma_{i0}\right)$. Portanto, podemos enunciar o teorema:

Teorema 3.3.3. *Seja* $M \in Mat(2^n, \mathbb{C})$. *Se* T *é a matriz adjunta de* M*, então* $\ddot{\pi}(H) = \ddot{\pi}(M)^*$.

Demonstração. Já sabemos que se α_k pertence a parte k do sistema e α_j pertence a parte j, com $k \neq j$, então $\alpha_k\alpha_j = \alpha_j\alpha_k$, ou seja, eles comutam. Assim quando calculamos o adjunto de um elemento podemos agrupar os termos por suas referentes partes e calcular o adjunto de cada uma dessas partes. Também usamos que $(A \otimes B)^* = A^* \otimes B^*$. Para finalizar usamos o mesmo passo da demonstração anterior e o teorema 3.3.2. $\square$

3.3.3 Relacionando as Definições de Operador Densidade

Vimos duas maneiras distintas de descrever um operador densidade: partindo da álgebra das matrizes, com um operador da forma $\sum_i \alpha_i |i\rangle \langle i|$, e definindo na própria álgebra de Clifford que estamos trabalhando. Fica a pergunta: essas duas definições são consistentes uma com a outra? Responderemos isso agora.

Lema 3.3.4. *Sejam* $|\psi\rangle \in \mathbb{C}^{2^n}$ *e* $\psi = [|\psi\rangle\, |X]\in \mathrm{Mat}(2^n, \mathbb{C})$*, onde a primeira coluna é* $|\psi\rangle$ *e as demais podem ser quaisquer vetores em* $\mathbb{C}^{2^n}$*. Então,* $\dot{\pi}(|\psi\rangle)H_+C_n = \ddot{\pi}(\psi)H_+$.

Demonstração. Primeiro, façamos algumas observações importantes para demonstrar o lema:

1. $\dot{\sigma}_{k0}H_+ = \dot{\sigma}_{k3}H_+ = H_+$;
2. $\dot{\sigma}_{k2}H_+ = \mathcal{J}\dot{\sigma}_{k1}H_+$;
3. $E_nC_n = \prod_{k=2}^{n} \frac{1}{2}(1 + \dot{\sigma}_{13}\dot{\sigma}_{k3})C_n$, ou seja, já estamos fazendo a identificação dos elementos $\mathcal{J}_k$;
4. $E_nH_+E_nC_n = H_+C_n$.

Se $A = \bigotimes^{n} \frac{1}{2}(I + \sigma_3)$, temos que $\ddot{\pi}(A) = H_+C_n$. Também é verdade que $\ddot{\pi}(\psi)H_+ = \ddot{\pi}(\psi A)$, onde $\psi A = [|\psi\rangle\, |0]$. Ou seja, como não importa a escolha de X, tomaremos um valor específico de modo a facilitar a demonstração.

Vamos analisar o que acontece em cada parte do sistema, pelo fato de que partes diferentes não influenciam uma na outra.

Temos que $\dot{\pi}$ age em cada parte k da seguinte maneira: $\dot{\pi}$ leva $(1,0)^t$ em E_n e $(0,1)^t$ em $-\mathfrak{I}_k\dot{\sigma}_{k2}E_n$. Além disso, o escalar complexo é levado em $\mathfrak{I}_k\dot{\sigma}_{k3}$.

Seja $|k\rangle = (a_k, b_k)^t$ a parte k de ψ. Se tomarmos $B_k = a_k\sigma_0 + b_k\sigma_1$, teremos que $|\psi\rangle = \bigotimes_{k=1}^{n} |k\rangle$ será a primeira coluna de $B = \bigotimes_{k=1}^{n} B_k$. Temos então que

$$\dot{\pi}(|k\rangle) = (\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I}_k\dot{\sigma}_{k3} - \mathfrak{R}(b_k)\mathfrak{I}\dot{\sigma}_{k2} + \mathfrak{I}(b_k)\mathfrak{I}_k\dot{\sigma}_{k1})E_n,$$

implicando em:

$$\begin{aligned}
\dot{\pi}(|k\rangle)H_+C_n &= \\
&= (\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I}_k\dot{\sigma}_{k3} - \mathfrak{R}(b_k)\mathfrak{I}\dot{\sigma}_{k2} + \mathfrak{I}(b_k)\mathfrak{I}_k\dot{\sigma}_{k1})H_+C_n \\
&= (\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I}\dot{\sigma}_{k3} - \mathfrak{R}(b_k)\mathfrak{I}\dot{\sigma}_{k2} \\
&+ \mathfrak{I}(b_k)\mathfrak{I}\dot{\sigma}_{k1})\frac{1}{2}(1 + \dot{\sigma}_{k3})H_+C_n \\
&= \frac{1}{2}(\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I}\dot{\sigma}_{k3} - \mathfrak{R}(b_k)\mathfrak{I}\dot{\sigma}_{k2} + \mathfrak{I}(b_k)\mathfrak{I}\dot{\sigma}_{k1} \\
&+ \mathfrak{R}(a_k)\dot{\sigma}_{k3} + \mathfrak{I}(a_k)\mathfrak{I} - \mathfrak{R}(b_k)\mathfrak{I}\dot{\sigma}_{k1} + \mathfrak{I}(b_k)\dot{\sigma}_{k2})H_+C_n \\
&= \frac{1}{2}((\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I})(1 + \dot{\sigma}_{k3}) + (\mathfrak{I}(b_k) \\
&- \mathfrak{R}(b_k)\mathfrak{I})(\dot{\sigma}_{k2} + \mathfrak{I}\dot{\sigma}_{k1}))H_+C_n.
\end{aligned}$$

Por outro lado, temos que $\ddot{\pi}(B_k)H_+$ é dado por:

$$\begin{aligned}
\ddot{\pi}(B_k)H_+ &= \\
&= (\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I} + (\mathfrak{R}(b_k) + \mathfrak{I}(b_k)\mathfrak{I})\dot{\sigma}_{k1})C_nH_+ \\
&= (\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I} + (\mathfrak{R}(b_k) + \mathfrak{I}(b_k)\mathfrak{I})\dot{\sigma}_{k1})\frac{1}{2}(1 + \dot{\sigma}_{k3})H_+C_n \\
&= \frac{1}{2}\left[(\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I})(1 + \dot{\sigma}_{k3}) + (\mathfrak{R}(b_k)\right. \\
&+ \left.\mathfrak{I}(b_k)\mathfrak{I})(-\mathfrak{I}\mathfrak{I})(\dot{\sigma}_{k1} + \mathfrak{I}\dot{\sigma}_{k2})\right] H_+C_n \\
&= \frac{1}{2}\left[(\mathfrak{R}(a_k) + \mathfrak{I}(a_k)\mathfrak{I})(1 + \dot{\sigma}_{k3})\right. \\
&+ \left.(\mathfrak{I}(b_k) - \mathfrak{R}(b_k)\mathfrak{I})(\mathfrak{I}\dot{\sigma}_{k1} - \dot{\sigma}_{k2})\right] H_+C_n.
\end{aligned}$$

Com isso encontramos a igualdade do teorema. □

Teorema 3.3.5. *A seguinte igualdade é verdadeira:*

$$\dot{\pi}(|\psi\rangle)H_+(\dot{\pi}(|\phi\rangle))^*C_n = \ddot{\pi}(|\psi\rangle\langle\phi|).$$

Demonstração. O primeiro fato a observar é que para ψ e $\phi \in \mathrm{Mat}(2^n, \mathbb{C})$, onde $\psi = [|\psi\rangle\, |X]$ e $\phi = [|\phi\rangle\, |X]$, temos que $|\psi\rangle\langle\phi| = \psi A \phi^*$, onde $A = \bigotimes^n \frac{1}{2}(I + \sigma_3)$.

Temos então que:

$$\ddot{\pi}(|\psi\rangle\langle\phi|) = \ddot{\pi}(\psi A \phi^*) =$$

$$\ddot{\pi}(\psi)\ddot{\pi}(A)\ddot{\pi}(\phi^*) = \ddot{\pi}(\psi)H_+\ddot{\pi}(\phi)^*.$$

Do lema 3.3.4 obtemos

$$\ddot{\pi}(\psi)H_+ = \dot{\pi}(|\psi\rangle)H_+C_n$$

e

$$H_+\ddot{\pi}(\phi)^* = (\ddot{\pi}(\phi)H_+)^* = (\dot{\pi}(|\phi\rangle)H_+C_n)^*.$$

Ou seja,

$$\ddot{\pi}(|\psi\rangle\langle\phi|) = \ddot{\pi}(\psi)H_+H_+\ddot{\pi}(\phi)^* = \dot{\pi}(|\psi\rangle)H_+C_n(\dot{\pi}(|\phi\rangle)H_+C_n)^* =$$

$$\dot{\pi}(|\psi\rangle)H_+(\dot{\pi}(|\phi\rangle))^*C_n,$$

o que completa a demonstração. □

Teorema 3.3.6. *Um operador densidade, segundo a definição 2.4.2, obedece as propriedades da definição 3.3.1.*

Demonstração. Seja $\rho = \dot{\pi}(|i\rangle)H_+(\dot{\pi}(|i\rangle))^*C_n$. Claramente, ρ satisfaz as propriedades 1 e 2.

Do teorema 3.1.7 e pelo fato de $|i\rangle\langle i|$ ser uma matriz densidade (equivalente a ρ), temos que o traço é unitário, pois o traço de $|i\rangle\langle i|$ é unitário.

Também é fácil observar que vale a propriedade 5, ou seja, $\rho = \rho^*$. Para isso basta usar que $H_+ = H_+^*$, $C_n^* = C_n$ e que C_n comuta com todos os elementos do ideal (C_n).

Pelos teoremas 3.2.5 e 3.3.5, temos que ρ é semidefinido positivo, pois $|i\rangle\langle i|$ é semidefinida positiva.

Assim, verifica-se a validade da proposição.

□

Teorema 3.3.7. *Um operador densidade, segundo 2.4.3, obedece as propriedades de 3.3.1.*

Demonstração. Em linhas gerais, repetiremos a demonstração do teorema anterior.

Por definição, as propriedades 1 e 2 são satisfeitas.

Se $P = \sum_j \alpha_j |j\rangle\langle j|$ é um operador densidade associado a um ensemble $\{(\alpha_j, |j\rangle)\}$, onde $\alpha_j = a_j + b_j i$, temos então que $\ddot{\pi}(P) = \ddot{\pi}\left(\sum_j \alpha_j |j\rangle\langle j|\right) = \sum_j (a_j + b_j \mathcal{J})\ddot{\pi}(|j\rangle\langle j|)$, segundo o teorema 3.3.5, e $\ddot{\pi}(P) = \sum_j (a_j + b_j \mathcal{J})\dot{\pi}(|j\rangle)H_+(\dot{\pi}(|j\rangle))^* C_n$. Ou seja, $\ddot{\pi}(P)$ também é o operador densidade equivalente a P em $\mathcal{C}\ell_{n,3n}^+$.

Agora usando os teoremas 3.2.5, 3.3.3 e 3.1.7 temos que o teorema é válido. □

Teorema 3.3.8. *Dado um operador densidade ρ, segundo 3.3.1, existe um ensemble com operador densidade associado P tal que P é equivalente a ρ (definição 2.4.3).*

Demonstração. Se ρ é um operador densidade em $\mathcal{C}\ell_{n,3n}$ segundo 3.3.1, então existe $P \in \mathrm{Mat}(2^n, \mathbb{C})$ de modo que $\ddot{\pi}(P) = \rho$ e P é um operador densidade clássico, logo por 2.1.6 existe um ensemble $\{(\alpha_j, |j\rangle)\}$ com $P = \sum_j \alpha_j |j\rangle \langle j|$.

Agora resta observar que o operador densidade equivalente a P segundo 2.4.3 é igual a ρ. De fato, se $\rho' = \sum_j (a_j + b_j \mathcal{I})\dot{\pi}(|j\rangle)H_+(\dot{\pi}(|j\rangle))^* C_n$, onde $\alpha_j = a_j + b_j i$, temos por 3.3.5 que $\rho' = \sum_j (a_j + b_j \mathcal{I})\ddot{\pi}(|j\rangle \langle j|) = \sum_j \ddot{\pi}(\alpha_j |j\rangle \langle j|) = \ddot{\pi}(P) = \rho$ e assim provamos que o teorema é verdadeiro. $\square$

◊♣♠♡

"Anyone who has never made a mistake has never tried anything new"

Albert Einstein

Considerações Finais

Vimos aqui que as álgebras de assinatura $(n, 3n)$, $\mathcal{C}\ell_{n,3n}$, contêm ideais com os quais podemos identificar tanto a álgebra das matrizes, onde se encontram os operadores densidade, quanto o espaço vetorial dos bits quânticos.

Mostramos como podemos considerar um elemento na álgebra par $\mathcal{C}\ell^+_{n,3n}$ e decidir se o mesmo é ou não equivalente a uma matriz semidefinida positiva. Também vimos como se comportam as "traduções" de operações básicas da álgebra de matrizes, tais como a função traço, adjunto e produto interno.

Como principal contribuição, construímos duas formas equivalentes de vermos os operadores densidade na álgebra de Clifford. Tais formas traduzem exatamente o que ocorre na teoria "tradicional" da informação quântica. Ou seja, mostramos como lidar com os q-bits que se transformam em elementos do ideal gerado pelo elemento $\mathsf{E}_n = \prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{J}_1\dot{\sigma}_{13}\mathcal{J}_k\dot{\sigma}_{k3})$ e também como tratar os seus equivalentes (operadores densidade) contidos no ideal principal de $\mathcal{C}\ell^+_{n,3m}$, gerado por $\mathsf{C}_n = \prod_{k=2}^{n} \frac{1}{2}(1 - \mathcal{J}_1\mathcal{J}_k)$.

Um dos pontos "delicados" foi a forma como "traduzimos" a unidade imaginária complexa para a álgebra de Clifford, onde apresentamos duas formas distintas de observar tal unidade, $\mathcal{J}_k$ e $\mathcal{J}_k\dot{\sigma}_{k3}$. A primeira, quando lidamos com os elementos do ideal (C_n) e a segunda, quando tratamos do ideal (E_n). Isso foi necessário, pois precisamos transformar a álgebra real $\mathcal{C}\ell^+_{n,3n}$ em uma álgebra complexa (escalares no corpo dos números complexos), já que a teoria da informação quântica é baseada em uma álgebra tensorial com base nos complexos.

Um ponto não considerado neste trabalho foi a descrição dos axiomas da mecânica quântica. Entretanto, como apresentamos um isomorfismo entre as álgebras, basta usá-lo para descrever como a evolução do sistema e as medidas são caracterizadas na álgebra de Clifford. Os dois outros axiomas são consequências diretas do texto.

Várias questões surgiram como consequência da conclusão desta tese, onde destacamos algumas delas:

1. Como fica o emaranhamento quântico na álgebra?
2. Existe alguma forma eficiente de saber se determinado elemento da álgebra par é (semi) definido positivo?
3. Como se comportam as operações quânticas?
4. Que aplicações práticas podemos obter com essa reformulação?

Referências Bibliográficas

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Massachusetts, 1969.

[Che96] Claude Chevalley. *Collected Works / Claude Chevalley v.2. The algebraic theory of spinors and Clifford algebras*. Springer, Berlin, 1996.

[DLG93] Chris Doran, Anthony Lasenby, and Stephen Gull. States and operators in the spacetime algebra. *Foundations of Physics*, 23:1239–1264, 1993.

[DLG+96] Chris Doran, Anthony Lasenby, Stephen Gull, Shyamal Somaroo, and Anthony Challinor. Spacetime algebra and electron physics. *Advances in Imaging and Electron Physics*, 95:271–386, 1996.

[Gar03] Yves Garcia, Arnaldo e Lequain. *Elementos de Álgebra*. Projeto Euclides. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2003.

[Hav03] Timothy F. Havel. The real density matrix. *Quantum Information Processing*, 1:511–538, 2003.

[HCST01] T. F. Havel, D. G. Cory, S. S. Somaroo, and C. Tseng. *Geometric Algebra with Applications in Science and Engeneering / Geometric Algebra in Quantum Information Processing by Nuclear Magnetic Resonance*. Birkäuser Boston, 2001.

[HD01] Timothy Havel and Chris J. L. Doran. Interaction and entanglement in the multiparticle spacetime algebra. *arXiv:quant-ph/0106063v1*, pages 81–100, 2001.

[HD02] T. F. Havel and C. J. L. Doran. *Geometric algebra in quantum information processing*. AMS Contemporary Mathematics Series, 2002.

[Knu88] Max-Albert Knus. *Quadratic Forms, Clifford Algebras and Spinors*. Seminários de Matemática. IMECC-Unicamp, Campinas, 1988.

[Lan97] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Massachusetts, third edition, 1997.

[Lou97] Pertti Lounesto. *Clifford algebras and spinors*. Number 239. Cambridge University Press, Cambridge, 1997.

[NC00] Michel A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[Pre98] John Preskill. Quantum information and computation. Lecture Notes for Physics 229 - California Institute of Technology, 1998.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian Forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1985.

[SCH98] Shyamal S. Somaroo, David G. Cory, and Timothy F. Havel. Expressing the operations of quantum computing in multiparticle geometric algebra. *Physics Letters A*, 240:1–7, 1998.

[SLD99] Shyamal Somaroo, Anthony Lasenby, and Chris Doran. Geometric algebra and the causal approach to multiparticle quantum mechanics. *J. Math. Phys.*, 40:3327–3340, 1999.

Índice de Notações

Índice Remissivo