Construção de Novos Códigos Quânticos Tóricos

Clarice Dias de Albuquerque Reginaldo Palazzo Jr. Eduardo Brandani da Silva

***Resumo*— Este artigo apresenta um método para obter códigos quânticos tóricos através de uma abordagem de teoria de grupos, usando tesselações no reticulado quadrado do toro. Com essa construção é possível reproduzir códigos já conhecidos e gerar outras inúmeras classes de códigos quânticos tóricos, dentre os quais destaca-se a classe $[[d^2, 2, d]]$ que fornece a melhor taxa de codificação até então encontrada para esses tipos de códigos.**

***Palavras-Chave*— Códigos quânticos, códigos tóricos, códigos quânticos topológicos, códigos reticulados.**

***Abstract*— In this paper we present a construction procedure of toric quantum error-correcting codes, via a group theory approach, by tiling the flat torus with polyominoes. This construction reproduces already known codes and generates countless new classes of toric quantum codes, among which the class $[[d^2, 2, d]]$ provides the best encoding rate known so far.**

***Keywords*— Quantum codes, toric codes, topological quantum codes, lattice codes.**

I. Introdução

Teoricamente, o uso de propriedades da mecânica quântica torna a computação quântica muito mais rápida que a computação clássica para obter soluções de certos problemas computacionais, incluindo fatoração prima, [1]. Porém, a construção de um computador quântico é um grande desafio. Uma das razões para essa dificuldade é a *decoerência*, fenômeno de decaimento de estados em superposições que se deve a interação entre os sistemas e o ambiente que o cerca.

Em teoria esse problema pode ser solucionado através dos *códigos quânticos corretores de erros* (QECC). A construção de tais códigos está fortemente baseada nas propriedades de códigos lineares clássicos. A maioria dos códigos quânticos disponíveis na literatura são baseados em códigos simpléticos ou *CSS*, [2], [3], [4], [5], subclasses dos códigos estabilizadores, [6]. Os códigos estabilizadores se baseiam em teoria de grupos, um código nesta classe é um subespaço invariante por um subgrupo Abeliano do grupo de Pauli, chamado *subgrupo estabilizador* cujos elementos são operadores unitários chamados *operadores estabilizadores*.

Kitaev propôs a classe de *códigos tóricos*, uma subclasse dos códigos estabilizadores, associada ao reticulado $\mathbb{Z}^2$, [7]. Por dependerem da topologia da superfície, são conhecidos como *códigos quânticos topológicos*. Nesta proposta, os qubits correspondem às arestas do reticulado enquanto os operadores estabilizadores estão associados aos vértices e às faces. Esses operadores estabilizadores juntos formam um Hamiltoniano com interação local cujo estado base coincide com o espaço protegido do código. As operações descritas pelo Hamiltoniano controlam um mecanismo intrínseco de proteção dos estados quânticos codificados. Os operadores que compõem esse Hamiltoniano são locais, e essa localidade é muito importante pois facilita a implementação física potencial desses sistemas reticulados. Ao contrário dos códigos topológicos, os operadores estabilizadores em códigos não-topológicos são geralmente não-locais. Apesar de não atingirem o limitante de Hamming, esses códigos proporcionam algumas vantagens diante de problemas como decoerência.

Bombin e Martin-Delgado, [8], apresentam uma abordagem diferente na construção dos códigos tóricos. Esta abordagem baseia-se no conceito de região fundamental de um reticulado, neste caso a esfera de Lee, usada para tesselar o reticulado quadrado do toro. Neste processo, as propriedades dos códigos de Kitaev são mantidas.

A partir disso, entendemos que é possível gerar um método para obter outros códigos quânticos tóricos de acordo com a possibilidade de tesselar, por determinados formatos, o reticulado quadrado do toro. Esses formatos são conhecidos como *poliminós*, [9]. Classicamente, os poliminós já foram usados para determinar códigos perfeitos em reticulados, [10] e [11].

Nossa proposta usa a estrutura algébrica de grupos para determinar tais tesselações. Dentre esses códigos é possível identificar diversas classes de códigos tóricos, inclusive reproduzir os códigos de Kitaev e Bombin e Martin-Delgado. Com respeito ao comprimento do código e à taxa de codificação, apresentamos uma classe de códigos cujos parâmetros $[[d^2, 2, d]]$ são os melhores encontrados até o presente momento.

Este artigo está organizado da seguinte maneira. Na Seção 2, revisamos os códigos tóricos de Kitaev e Bombin e Martin-Delgado. Na Seção 3, apresentamos a relação entre formas quadráticas, reticulados, e poliminós. A Seção 4, é dedicada ao problema de determinar a nova tesselação através de poliminós usando teoria de grupos. Além disso, reproduzimos classes de códigos quânticos tóricos conhecidas e apresentamos novas classes. Finalmente, na Seção 5, analisamos e discutimos os principais resultados obtidos.

II. Códigos Quânticos Tóricos Conhecidos

Um código corretor de erros quânticos é uma função de um espaço de Hilbert 2^k-dimensional em um espaço de Hilbert 2^n-dimensional, onde $k < n$. As palavras-código são os vetores no espaço 2^n-dimensional. A *distância mínima* d de um código QEC $\mathcal{C}$ é a menor distância de Hamming entre duas palavras-código distintas, ou ainda, é o menor peso de uma palavra-código não-nula. Um código QEC $\mathcal{C}$ com comprimento n, dimensão k, e distância mínima d é chamado código $[[n, k, d]]$.

Clarice Dias de Albuquerque, Departamento de Telemática, Universidade Estadual de Campinas, São Paulo, Brasil, E-mail: clarice@dt.fee.unicamp.br

Reginaldo Palazzo Jr., Departamento de Telemática, Universidade Estadual de Campinas, São Paulo, Brasil, E-mail: palazzo@dt.fee.unicamp.br.

Eduardo Brandani da Silva, Departamento de Matemática, Universidade Estadual de Maringá, Paraná, Brasil, E-mail: ebsilva@wnet.com.br. Este trabalho foi financiado pela Fapesp 2007/56052-8 e 2009/50837-9, CNPq 303364/2004-1, e CAPES-PROCAD 0121/01-0.

Um código com distância mínima d pode corrigir t erros ocorridos nos qubits de uma palavra-código, onde $t = \lfloor \frac{d-1}{2} \rfloor$. Em suma, códigos QEC codificam k qubits em n qubits para proteger os dados se erros ocorrerem em quaisquer t desses n qubits, onde n, k e t são valores que dependem do código usado, [12].

Um código estabilizador $\mathcal{C}$ é o autoespaço simultâneo, com autovalor 1, de todos os elementos de um subgrupo Abeliano $\mathcal{S}$ do grupo de Pauli P_n, chamado *grupo estabilizador*. Lembramos que $P_n = \pm\{I, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n}$, onde

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Portanto, $\mathcal{C} = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle \ \forall \ M \in \mathcal{S}\}$, [6].

A classe dos códigos tóricos de Kitaev é uma subclasse dos códigos estabilizadores e são definidos em um reticulado quadrado $m \times m$ do toro (veja Fig. 1). Os qubits estão em correspondência um a um com as arestas do reticulado. Os parâmetros desta classe de códigos são $[[2m^2, 2, m]]$, onde o comprimento do código é o número de arestas do reticulado $n = |E| = 2m^2$, o número de qubits codificados depende do gênero da superfície segundo a regra $k = 2g$ (no caso particular do toro, o gênero é $g = 1$) e a distância é o mínimo entre o número de arestas contidas no menor ciclo homologicamente não-trivial do reticulado e o número de arestas contidas no menor ciclo homologicamente não-trivial do reticulado dual, [13]. Lembrando que o reticulado quadrado é auto-dual, e uma vez que um ciclo homologicamente não-trivial é um caminho de arestas no reticulado que não pode ser contraído à uma face, segue que o menor desses caminhos corresponde aos eixos ortogonais do reticulado ou do reticulado dual, portanto $d = m$.

Os seus operadores estabilizadores estão associados a cada vértice e a cada face do reticulado (veja Fig. 1). Dado um vértice $v \in V$ o operador vértice A_v é definido como o produto tensorial de σ_x correspondendo a cada uma das quatro aresta que tem v como vértice comum e o operador identidade agindo nos qubits restantes. Analogamente, dada uma face $f \in F$, o operador face B_f é definido como o produto tensorial σ_z correspondendo a cada uma das quatro arestas que formam o bordo da face f e o operador identidade agindo nos demais qubits. Ou seja,

$$A_v = \bigotimes_{j \in E} \sigma_x^{\delta(j \in E_v)} \qquad B_f = \bigotimes_{j \in E} \sigma_z^{\delta(j \in E_f)},$$

onde δ é o delta de Kronecker.

O código tórico consiste do espaço fixado pelos operadores A_v e B_f, $\mathcal{C} = \{|\psi\rangle : A_v|\psi\rangle = |\psi\rangle, \ B_f|\psi\rangle = |\psi\rangle \ \ \forall \ v, f\}$. A dimensão de $\mathcal{C}$ é 4, ou seja, $\mathcal{C}$ codifica $k = 2$ qubits.

Algebricamente, podemos caracterizar o código de Kitaev como o conjunto das classes laterais do grupo quociente $\mathbb{Z}^2/m\mathbb{Z}^2 \cong \mathbb{Z}_m \times \mathbb{Z}_m$. As identificações dos lados opostos da região delimitada por $\mathbb{Z}_m \times \mathbb{Z}_m$ resulta na identificação com o toro plano. A área associada com o reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$ é m^2. Logo, como cada aresta pertence simultaneamente à duas faces quadradas do reticulado temos $2m^2$ arestas, ou seja, constata-se que $n = 2m^2$ qubits. Os qubits a serem codificados estão relacionados aos ciclos essenciais da superfície, no caso do toro há dois ciclos (meridiano e paralelo), portanto $k = 2$. Assim como no caso clássico, podemos definir a distância mínima do código observando seu reticulado dual. A distância mínima do código corresponde ao menor número de arestas no reticulado dual a serem percorridas entre os representantes de cada classe lateral ($d = m$).

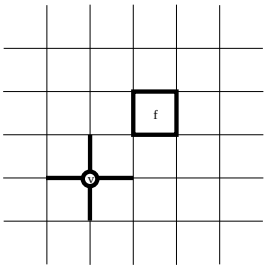

Fig. 1. Reticulado quadrado do toro.

Em [8], Bombin e Martin-Delgado consideram o código de Kitaev $\mathbb{Z}_m \times \mathbb{Z}_m$ como a *região fundamental* de um reticulado do toro, que chamaremos de subreticulado para não confundir. Translações dessa região fundamental resultam no reticulado quadrado do toro $\mathbb{Z}^2$, veja Fig. 2. Os parâmetros e propriedades do código tórico permanecem os mesmos. Além disso, podemos entender a distância mínima do código como sendo o menor número de arestas do reticulado dual entre duas regiões fundamentais distintas. Na Fig. 2 essas regiões são demarcadas pelas retas em negrito e têm a marcação X como um representante de cada região.

Para definir seus códigos, Bombin e Martin-Delgado utilizam outro subreticulado regular para tesselar o toro $\mathbb{Z}^2$, veja Fig. 2. Esse novo subreticulado tem esferas de Lee de raio r como região fundamental. É possível mostrar que m esferas de Lee de raio r, em duas dimensões, podem ser usadas para tesselar o toro $\mathbb{Z}_m \times \mathbb{Z}_m$, onde $m = 2r^2 + 2r + 1$ e $r = 1, 2, \ldots$, [10]. Este sistema de reticulados usado em [8] fornece códigos com parâmetros $[[d^2+1, 2, d]]$ que demandam um pouco mais da metade do número de qubits e mantém as mesmas propriedades do código original de Kitaev, como por exemplo, os operadores vértice e face agindo em quatro qubits.

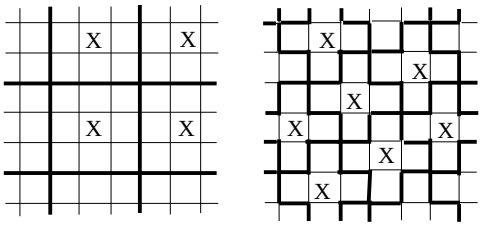

Fig. 2. Reticulados do código de Kitaev e do código de Bombin e Martin-Delgado com $d = 3$.

III. Formas Quadráticas, Reticulados e Poliminós

Em geral, qualquer tesselação de um toro $\mathbb{Z}_m \times \mathbb{Z}_m$ por translações de um dado formato corresponde classicamente a um código perfeito, conhecido também como *close-packed*, [10]. Quanticamente, podemos considerar esses formatos como regiões fundamentais de um subreticulado do toro onde definimos um código quântico tórico similarmente ao que foi feito em [8]. Portanto, estamos interessados em regiões com área m que tesselam reticulados $\mathbb{Z}_m \times \mathbb{Z}_m$. Encontrar esses formatos é um problema combinatorial.

Antes, porém, faremos uma breve revisão de conceitos relacionados a esse problema, a saber formas quadráticas, reticulados e poliminós.

A. Formas Quadráticas e Reticulados

Fermat introduziu o estudo de inteiros representados pela forma quadrática $x^2 + y^2$. Um de seus principais resultados é que somente os primos da forma $p \equiv 1(mod 4)$ podem ser escritos como somas de quadrados, $x^2+y^2 = p$, onde x, y são inteiros. Em seu estudo sobre a forma quadrática mais geral $\mathbf{A}x^2+\mathbf{B}xy+\mathbf{C}y^2$, onde $\mathbf{A}, \mathbf{B}$ e $\mathbf{C}$ são inteiros fixos, Lagrange deu início a classificação de formas quadráticas relacionando-as a geometria de certos pontos regularmente espaçados no plano, conhecidos como *reticulados*, [14].

Os reticulados têm sido bastante utilizados na teoria das comunicações. Sua principal aplicação está relacionada ao problema de codificação de canal. Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular. Formalmente, um reticulado Λ é definido como um subconjunto discreto infinito de $\mathbb{R}^n$ que forma um grupo aditivo sob adição usual de vetores.

Se Λ é um reticulado em um espaço N-dimensional, então existem vetores linearmente independentes $\nu_1, \nu_2, \ldots, \nu_{\mathrm{M}}$, com $\mathrm{M} < \mathrm{N}$, tal que Λ consiste de todos os pontos da forma $x = \sum_{i=1}^{\mathrm{M}} \xi_i \nu_i, \xi_i \in \mathbb{Z}$. Tal conjunto de vetores $\beta = \{\nu_1, \nu_2, \ldots, \nu_{\mathrm{M}}\}$ é chamado uma *base* de Λ, e M é a *dimensão* do reticulado, [14].

Uma *região fundamental* para um reticulado Λ é um bloco de construção que quando repetido muitas vezes preenche o espaço completo com apenas um ponto do reticulado em cada cópia. Existem diferentes formas de escolher uma base e uma região fundamental para um reticulado Λ, mas o volume da região fundamental é unicamente determinado por Λ, [15]. O volume da região fundamental é $|det(B)|$, onde B é a matriz quadrada formada pelos vetores da base β de um reticulado.

Por exemplo, o reticulado $\Lambda = \mathbb{Z}^2$ é gerado pelos vetores $\nu_1 = (1, 0)$ e $\nu_2 = (0, 1)$ com região fundamental descrita como um quadrado, e $B = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Então $det(B) = 1$. Ou seja, a área da região fundamental do reticulado $\mathbb{Z}^2$ é 1.

Formas quadráticas fornecem uma linguagem alternativa para estudos de reticulados, especialmente útil para investigar propriedades aritméticas, [15]. Em particular, a forma quadrática correspondente ao reticulado quadrado bidimensional $\mathbb{Z}^2$ é $\xi_1^2+\xi_2^2$, resultante de $(\xi_1\ \xi_2)B(\xi_1\ \xi_2)^{tr}$. Usaremos as coordenadas (ξ_1, ξ_2) para vetores reticulados.

B. Poliminós

Já sabemos que o reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$ está associado a forma quadrática $\xi_1^2 + \xi_2^2$, e a sua região fundamental é o quadrado com área 1. Nesta subseção definimos os poliminós que serão usados posteriormente como regiões fundamentais com área m (ou seja, composta de m quadrados) de um subreticulado que tessela o reticulado original.

O termo poliminó é uma generalização de "dominó" o formato que inclui dois quadrados com tamanhos iguais e um lado em comum. Um dominó tem somente o formato de retângulo. Um trominó é um poliminó formado por três quadrados e existem dois formatos de trominós, assim como existem quatro formatos de tetrominós, doze pentominós, e asism por diante, [9].

Padrões poliminós são exemplos de geometria combinatorial, e foram usados em codificação clássica para obtenção de códigos *close-packed*. Um código *close-packed* corresponde a qualquer tesselação de um toro $m \times m$ por translações de um dado formato poliminó, [10]. Esse formato determina o padrão de correção de erros de um tal código, ou seja, a diferença entre a palavra-código recebida e a palavra-código enviada.

IV. Códigos Quânticos Tóricos - Uma Abordagem Algébrica

Como mencionado anteriormente, estamos interessados em construir códigos quânticos tóricos através de tesselações regulares do toro $m \times m$ por meio de translações de um determinado poliminó com área m. Na verdade, a área do poliminó pode ser qualquer valor que divida a área do reticulado, m^2, porém o caso mais geral é obtido ao considerar poliminós com área m. Por exemplo, para $m = 5$ a Fig. 3 mostra dois modelos de regiões que tesselam o reticulado $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Antes de determinar as regiões fundamentais da tesselação, porém, devemos conhecer o conjunto de representantes dessas regiões, denotados nas figuras pela marca X. Esses pontos são dados pelos vetores reticulados $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m$ e nos indica onde deve haver um poliminó, o que facilita a construção da tesselação. Por exemplo, na Fig. 3 os representantes são dados pelos vetores $(0, 0), (2, 1), (4, 2), (1, 3)$ e $(3, 4)$. Portanto, o nosso problema é, fundamentalmente, determinar o conjunto de representantes dos poliminós usados para tesselar um reticulado. Para resolver esse problema, propomos uma abordagem algébrica.

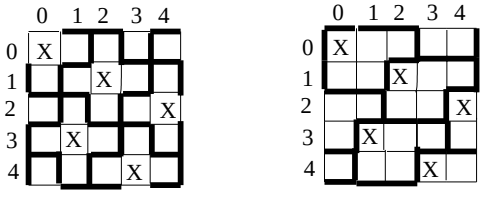

Fig. 3. Duas representações de regiões com área 5.

Esse conjunto de representantes corresponde a um código reticulado clássico, ou seja, é um subespaço vetorial de $\mathbb{Z}_m \times$

$\mathbb{Z}_m$, que denotaremos por $\mathcal{A}$. Para que a área do poliminó seja m, a cardinalidade de $\mathcal{A}$, denotada por $|\mathcal{A}|$, deve ser m.

Sabemos que a forma quadrática associada ao reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$ é dada por $\xi_1^2 + \xi_2^2$. Baseados nisso, usaremos a igualdade $a^2 + b^2 = m$ para encontrar os vetores reticulados $(a, b) \in \mathcal{A}$ com $a, b \in \mathbb{Z}_m$. Isso implica que a área do poliminó é de fato m. Através da soma usual de vetores, é possível achar todos os elementos de $\mathcal{A}$, contudo observe que a operação deve ser realizada módulo m, para que os pontos estejam dentro do reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$. Essa operação corresponde ao deslocamento de a unidades horizontalmente e b unidades verticalmente nas células do reticulado.

Note que, o conjunto dos representantes dos poliminós pode ser visto também como um subgrupo do grupo aditivo $(\mathbb{Z}_m \times \mathbb{Z}_m, +)$, e com isso podemos trabalhar com a estrutura de grupo. Nas proposições 1 e 2 veremos que, se a e b são relativamente primos tais que $m = a^2+b^2$, então $\mathcal{A} = \langle(a, b)\rangle$, do contrário, consideraremos $\mathcal{A} = \langle(a, b), (-b, a)\rangle$.

Proposição 1: Se a e b são inteiros primos entre si, então a ordem do grupo gerado pelo elemento (a, b) é m, ou seja, $o(\langle(a, b)\rangle) = m$.

Demonstração: Obviamente, temos que $ma = mb = 0$, e portanto $m(a, b) = (0, 0)$. Agora, suponha que existe $\tau \in \mathbb{N}$, com $0 < \tau < m$, tal que $\tau(a, b) = (0, 0)$. Então $\tau a = \tau b = 0$. Como a e b são relativamente primos, então existem inteiros α e β tais que $a\alpha+b\beta = 1$. Segue que $\tau = \tau a\alpha+\tau b\beta = 0$, o que contradiz a hipótese $0 < \tau < m$. Logo, $m = o(\langle(a, b)\rangle)$. ∎

O resultado vale para todo par (a, b) tal que $mdc(a, b) = 1$. Em particular, vale quando $mdc(a, b) = 1$ e $m = a^2 + b^2$. Obviamente, se $a \neq 0$ e $b = 0$ então $o(\langle(a, b)\rangle) = o(a) = a$, ou se $a = 0$ e $b \neq 0$ então $o(\langle(a, b)\rangle) = o(b) = b$.

Os seguintes fatos são facilmente demonstrados:

1) Se $mdc(a, b) = \delta \neq 0$ então $mdc(\frac{a}{\delta}, \frac{b}{\delta}) = 1$.
2) Se $m = a^2 + b^2$ e $mdc(a, b) = \delta \neq 0$, com $a \neq 0$ e $b \neq 0$, então δ divide m, uma vez que $\delta \mid a$ e $\delta \mid b$, e assim $\delta \mid a^2$ e $\delta \mid b^2$. Logo, $\delta \mid (a^2+b^2) = m$. Portanto, o quociente m/δ faz sentido.

Proposição 2: Se a e b não são relativamente primos, então $o(\langle(a, b)\rangle) = \frac{m}{\delta}$, onde $\delta = mdc\{a, b\}$.

Demonstração: Como $mdc\{a, b\} = \delta$, segue que $a = a_0\delta$ e $b = b_0\delta$, para algum $a_0, b_0 \in \mathbb{Z}_>$. Logo,

$$\frac{m}{\delta}(a, b) = (\frac{m}{\delta}a_0\delta, \frac{m}{\delta}b_0\delta) = (ma_0, mb_0) = (0, 0).$$

Agora, suponha por absurdo que exista $0 < \tau < \frac{m}{\delta}$ tal que $\tau(a, b) = (0, 0)$. Assim, $\tau a = \tau b = 0$, e $0 < \tau\delta < m$. Por outro lado, como $mdc\{a, b\} = \delta$, então existem $\alpha, \beta \in \mathbb{Z}$ tais que $a\alpha + b\beta = \delta$. Logo, $\tau a\alpha + \tau b\beta = \tau\delta$, daí $\tau\delta = 0$ contradizendo a hipótese $0 < \tau\delta < m$. Conclui-se que $o(\langle(a, b)\rangle) = \frac{m}{\delta}$. ∎

Observe que o resultado vale quando $mdc(a, b) \neq 0$ divide m. Em particular, vale quando $m = a^2 + b^2$.

Como desejamos que $|\mathcal{A}| = m$, então nos casos em que a e b são relativamente primos, onde $m = a^2 + b^2$, consideramos o grupo $\mathcal{A}$ igual ao grupo cíclico $\langle(a, b)\rangle$. Nos casos onde a e b não são relativamente primos, ou seja $mdc(a, b) = \delta \neq 0, 1$, então iremos considerar o grupo $\mathcal{A}$ igual ao grupo gerado por dois elementos $\langle(a, b), (-b, a)\rangle$ cuja cardinalidade é m.

Enfatizamos que, nos casos onde $m = a^2 + b^2$ com $mdc(a, b) = 1$, o conjunto dos representantes dos poliminós, $\mathcal{A}$, é um código perfeito no sentido de ter apenas um representante X em cada linha ou coluna, [16].

Conhecido o subespaço formado pelos representantes X, é possível escolher os poliminós que podem tesselar o reticulado. Definimos o código quântico associado a essa tesselação da mesma maneira como foi construído o código de Kitaev. O comprimento do código proposto neste artigo é dado pelo número de arestas do poliminó. Como o poliminó tem área m, e cada aresta pertence simultaneamente a duas faces quadradas do reticulado original do toro, temos que a quantidade efetiva de arestas é $n = 2m$. A dimensão do código é $k = 2$ devido a este código ser construído no toro. E a distância do código é definida como o número mínimo de arestas no reticulado dual entre dois representantes dos poliminós. Essa distância d é dada por $d_M = |a| + |b|$, e é conhecida como *distância de Mannhein*. Portanto, os parâmetros dos códigos quânticos gerados por essas tesselações são $[[2m, 2, d_M]]$.

O poliminó pode ter formatos diferentes, porém os parâmetros n, k e d serão os mesmos, ou seja, o código quântico gerado é o mesmo. Entretanto, o formato do poliminó influencia no padrão de correção de erros. Esse formato pode ser considerado de uma maneira geral como a junção de um quadrado $a \times a$ com um quadrado $b \times b$. No entanto, pode-se encontrar outros poliminós que tesselam o mesmo reticulado, esse é um problema de geometria combinatorial. Decidir qual o melhor formato para o poliminó depende do tipo de grafo associado ao canal discreto sem memória, por exemplo, se o canal for simétrico então é melhor usar poliminós simétricos em relação à marca X (nem sempre isso será possível), porém se o canal não for simétrico, então é melhor escolher um poliminó mais adequado.

Com essa construção é possível reproduzir códigos tóricos já existentes, assim como gerar classes novas.

A. Reprodução dos códigos de Bombin e Martin-Delgado

Quando $m = 2r^2 + 2r + 1$, para $r = 1, 2, 3, \ldots$, reproduzimos os códigos de Bombin e Martin-Delgado. Com efeito, se $m = 2r^2 + 2r + 1$, então podemos escrevê-lo como soma de quadrados da seguinte forma $m = (r + 1)^2 + r^2$. Ou seja, $a = r + 1$ e $b = r$. Assim, a e b são primos entre si, portanto $\mathcal{A} = \langle(a, b)\rangle$. Segue que $d = |r + 1| + |r| = 2r + 1$, e $n = 2m = 2(2r^2 + 2r + 1) = 4r^2 + 2d = 4\frac{(d-1)^2}{4} + 2d = (d - 1)^2 + 2d = d^2 + 1$. Portanto $[[d^2 + 1, 2, d]]$. O formato do poliminó pode ser a junção de quadrados como visto anteriormente ou pode ser também a esfera de Lee de raio r utilizada em [8].

Exemplo 1: Seja $m = 5$, então as únicas soluções para $a^2 + b^2 = 5$ são $a = \pm 2$ e $b = \pm 1$ ou vice-versa. Sem perda de generalidade, digamos que $\mathcal{A} = \langle(2, 1)\rangle$, ou seja, $\mathcal{A} = \{(0, 0), (2, 1), (4, 2), (1, 3)$ e $(3, 4)\}$. Note que as operações são feitas módulo 5. Esses elementos representam os poliminós, que neste caso, podem ser as esferas de Lee de raio $r = 1$ ou também podem ser quadrados 2×2 junto com

quadrados 1×1, veja Fig. 3. Como $d = |2| + |1| = 3$, obtemos um código $[[10, 2, 3]]$.

B. Reprodução dos códigos de Kitaev

Quando m é um quadrado perfeito, as únicas soluções para $m = a^2 + b^2$ são $a = \pm\sqrt{m}$, $b = 0$ ou vice-versa. Sem perda de generalidade, consideramos $\mathcal{A} = \langle(\sqrt{m}, 0), (0, \sqrt{m})\rangle$. Marcando os representantes no reticulado obtemos poliminós quadrados $\sqrt{m} \times \sqrt{m}$. Temos que os parâmetros dos códigos são $n = 2m$, $k = 2$ e $d = |\sqrt{m}|$, logo $n = 2d^2$. Portanto reproduzimos os parâmetros dos códigos tóricos de Kitaev $[[2d^2, 2, d]]$.

Exemplo 2: Para $m = 4$, temos que as únicas soluções para $4 = a^2 + b^2$ são $a = \pm 2$ e $b = 0$ ou vice-versa. Sem perda de generalidade, considere $a = 2$ e $b = 0$. O vetor $(2, 0)$ nos proporciona duas marcas X no reticulado, $(2, 0), (0, 0)$, enquanto o vetor $(0, 2)$ produz as marcas em $(0, 2), (0, 0)$. Como $\mathcal{A}$ deve ser um subgrupo, então a soma dos seus elementos também pertence a $\mathcal{A}$, ou seja, $\mathcal{A} = \{(0, 0), (2, 0), (0, 2), (2, 2)\}$. Os poliminós são definidos como quadrados 2×2, veja Fig. 4. Contando o número de arestas do poliminó temos que $n = 8$. Além disso, pode-se verificar que a distância é $d = |2| + |0| = 2$. Logo, temos um código $[[8, 2, 2]]$.

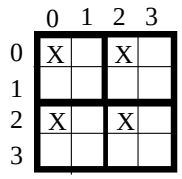

Fig. 4. Código de Kitaev $[[8, 2, 2]]$.

C. Nova classe de códigos tóricos $[[d^2, 2, d]]$

Considere agora os valores de m que são o dobro de um quadrado perfeito, ou seja, $m = a^2 + a^2$. Neste caso, o conjunto dos representantes dos poliminós é gerado por dois elementos (a, a) e $(-a, a)$. Temos que $d = 2a$ e $n = 2m = 2(2a^2) = 4a^2 = d^2$. Logo obtemos um código tórico com parâmetros $[[d^2, 2, d]]$. Em termos de taxa de codificação este código é melhor que os anteriores, $k/n \sim 1/d^2$. Um dos possíveis poliminós neste caso é um retângulo $2a \times a$. Esses poliminós não são simétricos quanto ao representante X, por isso esse tipo de código pode ser útil em um canal não simétrico.

Exemplo 3: Seja $m = 8$. Temos que as únicas soluções para $8 = a^2 + b^2$ são $a, b = \pm 2$. Sem perda de generalidade, considere $a = b = 2$. Assim, $\mathcal{A} = \langle(2, 2), (-2, 2)\rangle = \{(0, 0), (2, 2), \ (4, 4), \ (6, 6), (6, 2), (2, 6), (0, 4), (4, 0)\}$. Os poliminós podem ser quadrados 2×2 juntos a quadrados 2×2, ou seja, um retângulo 4×2. Obtemos um código $[[16, 2, 4]]$. Na Fig. 5 mostramos dois modelos de tesselações para esse exemplo.

Podemos obter várias classes novas de códigos tóricos impondo condições a a e b ou m. Por exemplo, se considerarmos

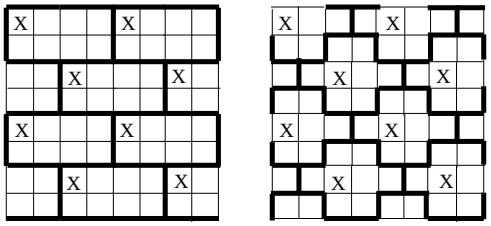

Fig. 5. Duas representações do código $[[16, 2, 4]]$.

os valores de m tais que $m = a^2 + b^2$, onde $b = a - 2$. Temos que $d = d_M = 2a - 2$ e $n = 2m = 2(a^2 + (a - 2)^2) = 2(2a^2 - 4a + 4) = 4(a^2 - 2a + 2)$. Substituindo o valor de $a = \frac{d+2}{2}$, seque que $n = d^2 + 4$. Assim, obtemos a classe de códigos $[[d^2 + 4, 2, d]]$. Mais geralmente, se considerarmos $b = a - \varsigma$, temos a classe de códigos $[[d^2 + \varsigma^2, 2, d]]$.

Assim como essas classes, podemos encontrar muitas outras de acordo com as condições impostas sobre a, b e m.

V. CONCLUSÕES

Através de uma abordagem algébrica é possível utilizar o conceito de poliminó, já usado para códigos clássicos, para gerar um método de obtenção de códigos quânticos tóricos por meio da tesselação do reticulado quadrado do toro por translações desse poliminó. Códigos definidos assim mantém as mesmas propriedades dos códigos tóricos de Kitaev, como a localidade dos operadores estabilizadores. Além disso, os códigos continuam sendo definidos no reticulado $\mathbb{Z}^2$ que é ortogonal e auto-dual.

O modelo do poliminó usado na tesselação determina o padrão de correção de erros do código. As esferas de Lee de raio r, na métrica de Lee, proporcionam códigos cujo padrão de correção de erros é simétrico, porém existem outros poliminós que podem ser utilizados para os casos onde o canal não seja simétrico. Pode-se determinar o código que melhor se adapta ao problema.

Além de reproduzir classes de códigos já conhecidas, esse método permite encontrar outras classes de códigos tóricos, como por exemplo, a classe $[[d^2, 2, d]]$ que é a melhor em termos de comprimento do código, e consequentemente a melhor quanto a taxa de codificação.

AGRADECIMENTOS

Este trabalho foi financiado pela Fapesp 2007/56052-8 e 2009/50837-9, CNPq 303364/2004-1, e CAPES-PROCAD 0121/01-0.

REFERÊNCIAS

[1] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124, 1994.

[2] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52**, pp. 2493, 1995.

[3] A. M. Steane, *Multiple particle interference and quantum error correction*, Proc. R. Soc. Lond. A **452**, pp. 2551–2577, 1996.

[4] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A **54**, pp. 1098, 1996.

[5] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Letters **77**, pp. 793, 1996.

[6] D. Gottesman, *Class of quantum error-correcting codes saturating the quantum Hamming bound*, Phys. Rev. A **54**, pp. 1862, 1996.
[7] A. Yu Kitaev, *Fault-tolerant quantum computation by anyons*, Annals of Physics **303**, pp. 2, 2003.
[8] H. Bombin and M. A. J. Martin-Delgado, *Homological error correction: classical and quantum codes*, J. Math. Phys. **48**, pp. 052105, 2007.
[9] S. W. Golomb, *Polyominoes*, Princeton University Press, Princeton, New Jersey, 1994.
[10] S. W. Golomb, *Perfect codes in the Lee metric and the packing of polyominoes*, SIAM J. Appl. Math. Vol 18, No. 2, January 1970.
[11] C. Almeida and R. Palazzo Jr, *Two-dimensional interleaving using the set partitioning technique*, Electronics Letters, **EE45**, pp. 203-205, 1996.
[12] P. W. Shor, *Fault-tolerant quantum computation*, Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pp. 56, 1996.
[13] E. Dennis, A. Kitaev, A. Landahl and J. Preskill, *Topological quantum memory*, J. Mathematical Physics **43**, pp. 4452, 2002.
[14] S. K. Stein and S. Szabó, *Algebra and Tiling: Homomorphisms in the service of geometry*, The Mathematical Association of America, 1994.
[15] J. H. Conway and N. J. A. Sloane, *Sphere Packings Lattices and Groups*, Springer-Verlag, 1988.
[16] S. I. R. Costa, M. Muniz, E. Agustini and R. Palazzo Jr., *Graphs, tessellations, and perfect codes on flat tori*, IEEE Transactions on Information Theory, **50**, No. 10, 2004.