Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Relação entre o Grau da Curva Hiperelíptica, a Tesselação Associada e o Correspondente Grupo Fuchsiano Aritmético

Erika Patricia Dantas de Oliveira Guazzi[1]
UTFPR, Campo Mourão, PR
Reginaldo Palazzo Júnior[2]
FEEC, UNICAMP, Campinas, SP

Resumo. Neste trabalho, exibimos a existência de uma relação entre o grau da curva hiperelíptica $y^2 = f(z)$, cujo grau de $f(z)$ é maior ou igual a 5, e os parâmetros p e q das tesselações regulares $\{p, q\}$. A importância desta relação está diretamente relacionada à construção de códigos clássicos como de códigos quânticos a serem utilizados em canais discretos sem memória. Além disso, para curvas hiperelípticas específicas, e consequentemente para as tesselações associadas satisfazendo a condição de Fermat, são apresentados os correspondentes grupos fuchsianos aritméticos. Destacamos a importância dos grupos fuchsianos aritméticos por estarem relacionados com a construção dos códigos reticulados.

Palavras-chave. Curvas hiperelípticas, Grupo fuchsiano, Tesselações regulares, Grupo fuchsiano aritmético

1 Introdução

Neste trabalho, utilizamos a geometria hiperbólica, em especial o modelo hiperbólico do disco aberto unitário $\Delta = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$, e as curvas hiperelípticas $y^2 = f(z)$, uma classe especial das curvas algébricas, na determinação do correspondente grupo fuchsiano e, consequentemente, do grupo fuchsiano aritmético. Para alcançar esse objetivo, faremos uso do algoritmo proposto em [6] na determinação do grupo fuchsiano cujo polígono fundamental tem como vértices as raízes associadas à curva hiperelíptica dada. Todavia, a região fundamental do polígono que irá uniformizar a curva hiperelíptica está associada a um subgrupo do grupo fuchsiano associado à curva hiperelíptica dada. Como consequência, os parâmetros p e q da tesselação $\{p, q\}$ associada são determinados. Agora, se os parâmetros p e q da correspondente tesselação $\{p, q\}$ satisfizerem a condição de Fermat então o correspondente grupo fuchsiano aritmético será apresentado. Chamamos a atenção ao fato de que a referida região fundamental tem área máxima quando comparada com a região fundamental determinada pelo procedimento proposto por Whittaker, [9].

Uma condição para se obter uma tesselação regular, consistindo de um arranjo de polígonos regulares (todos os lados ter o mesmo comprimento), é que o polígono cujos

[1]erikapatricia@utfpr.edu.br
[2]palazzo@dt.fee.unicamp.br

vértices são as raízes da curva hiperelíptica deve ser regular ou quase regular (ter somente uma aresta com comprimento diferente). Como resultado da aplicação do algoritmo proposto em [6] ao polígono regular ou quase regular, temos as transformações elípticas como os geradores do grupo fuchsiano. A determinação do subgrupo fuchsiano consiste em fixar uma das transformações elípticas e multiplica-la às demais. No caso do polígono ser regular a transformação elíptica a ser fixada pode ser qualquer uma. Todavia, no caso do polígono ser quase regular, a transformação elítpica a ser fixada é aquela associada à aresta com comprimento diferente. A região fundamental (obtida fixando uma transformação elíptica e realizando o produto desta pelas demais) nos dois casos será um polígono regular, denominado *polígono fundamental*.

Desse modo, ao repetir o processo de fixar uma transformação elíptica e realizar as composições com as demais transformações, obtemos o polígono fundamental e este sob a ação do correspondente subgrupo fuchsiano recobrirá o plano hiperbólico, uma vez que tais polígonos fundamentais interceptam-se somente nas arestas e vértices.

Diante deste contexto, o trabalho aborda a existência de uma relação entre o grau da curva hiperelíptica $y^2 = f(z)$, e as tesselações regulares possíveis, a saber, as três principais tesselações $\{4g, 4g\}$, $\{4g + 2, 2g + 1\}$ e $\{12g - 6, 3\}$, onde g é o gênero da superfície, conduzindo à construção tanto de códigos clássicos como de códigos quânticos, a serem utilizados na codificação de canais, bem como as respectivas vantagens de cada uma. Por fim, para curvas hiperelípticas específicas, e consequentemente para as tesselações associadas, tal que satisfaçam a condição de Fermat, indicamos a obtenção do grupo fuchsiano aritmético associado, cuja importância está relacionada à construção de uma classe de códigos corretores de erros denominada *códigos reticulados*.

Este trabalho está organizado da seguinte maneira. Na Seção 2, serão apresentadas as tesselações, tanto na geometria euclidiana quanto na geometria hiperbólica, ressaltando as mais utilizadas na teoria de codificação. Na Seção 3, apresentamos a condição de Fermat, ou seja, a condição a ser satisfeita pelos parâmetros p e q da tesselação $\{p, q\}$ para que esta possua um grupo fuchsiano aritmético associado. Na Seção 4, exibimos a obtenção da região de uniformização de uma curva hiperelíptica dada. Na Seção 5 apresentamos os resultados decorrentes da relação entre o grau da curva hiperelíptica e as possíveis tesselações, e consequentemente, com os grupos fuchsianos aritméticos. Por fim, na Seção 6 serão apresentadas as conclusões.

2 Tesselações

Nesta seção, apresentamos o conceito e exemplos de tesselações, destacando suas particularidades. Em seguida, apresentamos as condições para a existência de uma tesselação regular no plano hiperbólico. Apresentamos as três principais tesselações $\{4g, 4g\}$, $\{4g+2, 2g+1\}$ e $\{12g-6, 3\}$, onde g é o gênero da superfície, por serem as mais empregadas na codificação de canais.

Definição 2.1. *Uma tesselação regular do plano, hiperbólico ou euclidiano, é uma cobertura de todo o plano por polígonos regulares, hiperbólicos ou euclidianos, não sobrepostos que se interceptam apenas nas arestas ou nos vértices. Todos os polígonos da tesselação*

DOI: 10.5540/03.2020.007.01.0428

têm o mesmo número de lados. Uma tesselação regular com q polígonos regulares de p lados é denotada por $\{p, q\}$.

Observação 2.1. *A tesselação* $\{p, q\}$ *é auto-dual se* $p = q$.

Na geometria euclidiana, existem apenas três tesselações regulares, isso por que os valores de p e q devem satisfazer $(p-2)(q-2) = 4$. Disso decorre que só existem as tesselações $\{3, 6\}$ (triângulos equiláteros com 6 triângulos equiláteros encontrando-se em cada vértice), $\{4, 4\}$ (quadrados com 4 quadrados encontrando-se em cada vértice) e $\{6, 3\}$ (hexágono regular com 3 hexágonos regulares encontrando-se em cada vértice). Por outro lado, na geometria hiperbólica existem infinitas tesselações regulares, pois p e q devem satisfazer $(p-2)(q-2) > 4$, veja [8] e [5] para maiores detalhes.

Dentre as infinitas tesselações no plano hiperbólico, destacamos as tesselações $\{4g, 4g\}$, $\{4g+2, 2g+1\}$ e $\{12g-6, 3\}$, onde $g = 0, 1, 2, \ldots$, é o gênero da superfície associada. Estas tesselações são as mais importantes para a codificação de canais tanto na teoria da codificação clássica quanto na teoria da codificação quântica.

A tesselação auto-dual $\{4g, 4g\}$ é comumente utilizada em sistemas de comunicação por apresentar uma implementação mais simples do que a implementação das outras duas tesselações. Entretanto, essa tesselação é a menos densa e apresenta uma maior taxa de erro dentre as três tesselações. Na tesselação $\{4g, 4g\}$ a taxa de erro não está muito longe da taxa de erro na tesselação $\{4g+2, 2g+1\}$. Todavia, a menor complexidade aponta na direção da utilização da tesselação auto-dual. A tesselação $\{12g-6, 3\}$ apesar de ser a mais densa e, portanto, conduzindo a um melhor desempenho, tem maior complexidade de implementação do demodulador do que as das demais tesselações, [4].

3 Grupo Fuchsiano Aritmético

Nesta seção, apresentamos um importante e interessante exemplo de grupo fuchsiano, o grupo fuchsiano aritmético, e as condições sob uma tesselação a fim de obter um grupo fuchsiano aritmético associado.

Definição 3.1. *Um grupo fuchsiano aritmético é um grupo fuchsiano derivado de uma álgebra dos quatérnios.*

Em outras palavras, um grupo fuchsiano aritmético é um subgrupo discreto de $PSL(2, \mathbb{R})$ obtido a partir de algumas construções aritméticas, [7].

Dada a tesselação $\{p, q\}$, exibimos as condições sobre p e q para que seja possível determinar o grupo fuchsiano aritmético associado, para maiores detalhes veja [3].

Definição 3.2. *Um número de Fermat é um número primo da forma* $p_s = 2^{2^s} + 1$, *onde* $s \geq 0$ *é um inteiro positivo.*

Teorema 3.1. *(Condição de Fermat) [3] Seja* Γ *um grupo fuchsiano derivado de uma tesselação* $\{p, q\}$, *é possível determinar os geradores de* Γ, *e então, o grupo fuchsiano aritmético, se p e q podem ser fatorados como*

$$2^k \quad ou \quad 2^k p_1 p_2 \ldots p_s$$

DOI: 10.5540/03.2020.007.01.0428

onde k é um número natural e os p_i's são números de Fermat distintos.

Sem perda de generalidade, considere o caso de polígonos hiperbólicos regulares com lados opostos emparelhados. Através da aplicação do algoritmo proposto em [3], página 63 na subseção 3.2.1, para a construção do grupo fuchsiano aritmético, obtemos os **geradores do grupo fuchsiano aritmético**. Estes geradores são dados por

$$G_1 = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{pmatrix} A_1 \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{pmatrix} \begin{pmatrix} -\frac{1}{2}i & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}i \end{pmatrix}$$

e

$$G_k = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{pmatrix}^{k-1} A_1 \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{pmatrix}^{-(k-1)} \begin{pmatrix} -\frac{1}{2}i & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}i \end{pmatrix}$$

onde $k = 2, \ldots, \frac{p}{2}$ e

$$A_1 = \begin{pmatrix} \frac{2\cos(\pi/q)}{2\sin(\pi/p)} & \frac{\sqrt{2\cos(\pi/p)+2\cos(\pi/q)}e^{i\pi\left(\frac{p+1}{p}\right)}}{e\sin(\pi/p)} \\ \frac{\sqrt{2\cos(\pi/p)+2\cos(\pi/q)}e^{i\pi\left(\frac{p+1}{p}\right)}}{e\sin(\pi/p)} & \frac{2\cos(\pi/q)}{2\sin(\pi/p)}. \end{pmatrix}.$$

4 Exemplo da obtenção da região fundamental

Nesta seção, apresentamos de forma sintetizada a aplicação do algoritmo, veja [6], para a curva hiperelíptica $y^2 = z^5 - 1$. Destacamos que tal procedimento é válido para as curvas hiperelípticas da forma $y^2 = z^n + 1$, $y^2 = z^n - 1$, e $y^2 = z^n + z^{n-1} + \ldots + z^2 + z + 1$, onde $n \in \mathbb{N}$ e $n = 2g + 1$ ou $n = 2g + 2$ (g é o gênero da superfície). Por hipótese, todas as curvas satisfazem a conjectura de Whittaker, para maiores detalhes veja [6].

Exemplo 4.1. *Dada a curva hiperelíptica $y^2 = z^5 - 1$, de gênero 2, temos que suas raízes são $c_1 = 0.309017+0.9510565i$, $c_2 = -0.809017+0.5877853i$, $c_3 = -0.809017-0.5877853i$, $c_4 = 0.309017 - 0.9510565i$ e $c_5 = 1$. As raízes estão sobre a fronteira de Δ, veja Figura 1, e o polígono formado é regular.*

Note que o polígono em Δ formado pelas raízes da curva hiperelíptica $y^2 = z^5 - 1$ é regular, veja Figura 1. Desta maneira, podemos fixar qualquer uma das transformações elípticas, cada uma associada a uma correspondente aresta do polígono e, então, fazermos o produto desta transformação às demais. Em particular, fixando a transformação T_1, obtemos a região fundamental que uniformizará a curva hiperelíptica como mostrada na Figura 2.

5 Resultados

Nesta seção, exibimos os resultados estabelecidos a partir da análise realizada na aplicação do algoritmo proposto em [6], para a curva hiperelíptica $y^2 = z^5 - 1$, bem como para as curvas hiperelípticas da forma $y^2 = z^n + 1$, $y^2 = z^n - 1$, e $y^2 = z^n + z^{n-1} + \ldots + z^2 + z + 1$, onde $n \in \mathbb{N}$ e $n = 2g + 1$ ou $n = 2g + 2$ (g é o gênero da superfície).

DOI: 10.5540/03.2020.007.01.0428

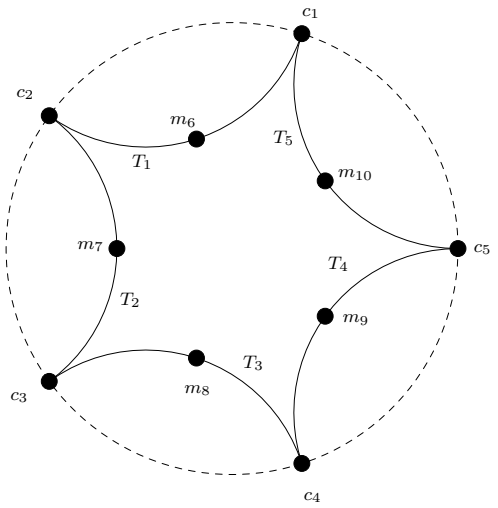

Figura 1: Polígono formado pelas raízes de $z^5 - 1 = 0$ em Δ

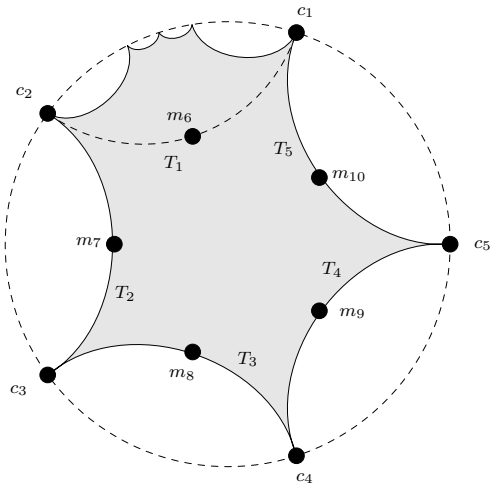

Figura 2: Região fundamental associada à curva $y^2 = z^5 - 1$ em Δ

Considere a curva hiperelíptica $y^2 = z^5 - 1$, cujas raízes formam um polígono de 5 lados, Figura 1. Ao fixarmos uma transformação elíptica (fixar aresta) e multiplica-la às demais, resultará em uma região fundamental consistindo de um polígono de 8 lados, Figura 2. Assim, a tesselação $\{p, q\}$ associada à curva hiperelíptica dada satisfaz $p = 8$. A fim de determinar o valor adequado de q, utilizamos a condição $(p-2)(q-2) > 4$. Então, a tesselação associada é $\{8, q\}$, onde q satisfaz a condição $q > 8/3$. Além disso, dentre as possíveis tesselações $\{8, q\}$, onde $q > 8/3$, escolhemos aquela que satisfaça a condição de Fermat, veja Teorema 3.1. Note que $p = 8 = 2^3$ e, assim, para todo valor de $q \geq 3$ que possa ser decomposto na forma 2^k ou $2^k p_1 p_2 \dots p_s$, onde k é um número natural e os p_i's são números de Fermat distintos, obtemos um grupo fuchsiano aritmético associado.

DOI: 10.5540/03.2020.007.01.0428

Por exemplo, as tesselações $\{8,3\}$, $\{8,4\}$, $\{8,5\}$, $\{8,6\}$, $\{8,8\}$, $\{8,10\}$, $\{8,12\}$, $\{8,16\}$ e $\{8,20\}$, satisfazem a condição de Fermat. Assim, um grupo fuchsiano aritmético associado a cada uma dessas tesselações hiperbólicas pode ser obtido.

De forma geral, observamos que, dada uma curva hiperelíptica de grau n, $n \in \mathbb{N}$ e $n \geq 3$, as suas raízes formam um polígono de n lados. Desse modo, a sua região fundamental será um polígono de $2n-2$ lados. Assim, a tesselação $\{p,q\}$ associada à curva hiperelíptica dada satisfaz $p = 2n-2$. Com o objetivo de determinar o valor adequado de q, temos que existe uma tesselação regular $\{p,q\}$ do plano hiperbólico se, e somente se, $(p-2)(q-2) > 4$, veja [5, 8].

Em particular, para a curva hiperelíptica de grau $n = 2g+1$, segue que $p = 2(2g+1) - 2 = 4g+2-2 = 4g$. Então, a tesselação associada é a tesselação $\{4g,q\}$, onde q satisfaz a condição $(p-2)(q-2) > 4$. De forma análoga, dada a curva hiperelíptica de grau $n = 2g+2$ temos que $p = 2(2g+2)-2 = 4g+4-2 = 4g+2$. Logo, a tesselação associada é $\{4g+2,q\}$, onde q satisfaz a condição $(p-2)(q-2) > 4$. No caso da curva hiperelíptica ter grau $n = 6g-2$, decorre que $p = 2(6g-2)-2 = 12g-4-2 = 12g-6$. Dessa forma, a tesselação associada é $\{12g-6,q\}$, onde q satisfaz a condição $(p-2)(q-2) > 4$.

Como consequência, temos os seguintes resultados:

Proposição 5.1. *Dada a curva hiperelíptica de grau n, com n raízes distintas em Δ, então os parâmetros p e q da tesselação $\{p,q\}$ são dados por $p = 2n-2$ e $q > \frac{2(n-1)}{(n-2)}$.*

Proposição 5.2. *Considere uma curva hiperelíptica que satisfaça a Proposição 5.1. Se o grau da curva é*

1. $2g+1$ *então a tesselação associada é $\{4g,q\}$, onde q satisfaz $(4g-2)(q-2) > 4$;*
2. $2g+2$ *então a tesselação associada é $\{4g+2,q\}$, onde q satisfaz $4g(q-2) > 4$;*
3. $6g-2$ *então a tesselação associada é $\{12g-6,q\}$, onde q satisfaz $(12g-8)(q-2) > 4$;*

onde g é o gênero da superfície associada.

E mais, estas curvas estão associadas, em parte, às três principais tesselações exibidas anteriormente, pois foi determinado somente o valor de p, enquanto q tem vários valores possíveis. Recordamos que na Seção 3, foram expostas as condições sobre p e q para que seja possível determinar o grupo fuchsiano aritmético associado à tesselação $\{p,q\}$, a saber, p e q tem que serem decompostos na forma 2^k ou $2^k p_1 p_2 \dots p_s$ onde $k \in \mathbb{Z}_+$ e os p_i's são números distintos de Fermat. Chamamos a atenção ao fato de que a condição de Fermat é uma possível, e não a única, condição a ser satisfeita na determinação de grupos fuchsianos aritméticos.

Assim, para cada uma das curvas hiperelípticas consideradas, é possível verificar a partir de quais tesselações $\{p,q\}$ um grupo fuchsiano aritmético pode ser obtido. Este último implica fortemente na construção de códigos geometricamente uniformes.

Desta forma, dado o grau da curva hiperelíptica, estabelecemos as possíveis tesselações, veja as Proposições 5.1 e 5.2. Dentre as possíveis tesselações, escolhemos aquela que satisfaça a condição de Fermat, veja Teorema 3.1. Consequentemente, obtemos o grupo fuchsiano aritmético associado. A partir disso, um reticulado hiperbólico é derivado, do qual a constelação de sinais GU pode ser construída.

DOI: 10.5540/03.2020.007.01.0428

6 Conclusões

Neste trabalho foi estabelecida uma relação entre o grau da curva hiperelíptica e a tesselação associada à superfície gerada pelo subgrupo fuchsiano. Por fim, dentre as possíveis tesselações, indicamos como identificá-las a um grupo fuchsiano aritmético. Destacamos que, a partir do conhecimento do grupo fuchsiano aritmético, é possível a obtenção de reticulados, os quais são importantes em projetos de modulações e códigos corretores de erros utilizados em sistemas de comunicações, de forma a atingir a menor complexidade nos processos de demodulação e de decodificação bem como o de melhor desempenho a ser alcançado pelo sistema de comunicações.

Agradecimentos

À FAPESP e CNPq pela apoio financeiro durante o período desta pesquisa.

Referências

[1] J. W. Anderson. Hyperbolic Geometry. In *Springer Undergraduate Mathematics Series*. Springer, 2008.

[2] A. F. Beardon. The geometry of discrete groups. Springer Science & Business Media, 1983.

[3] C. W. O. Benedito. Construção de grupos fuchsianos aritméticos provenientes de álgebras dos quatérnios e ordens maximais dos quatérnios associados a reticulados hiperbólicos. Tese de Doutorado, FEEC/UNICAMP, 2014.

[4] R. G. Cavalcante, H. Lazari, J. D. Lima e R. Palazzo Jr. A New Approach to the Design of Digital Communication. In: AMERICAN MATHEMATICAL SOC. *Algebraic Coding Theory and Information Theory: DIMACS Workshop, Algebraic Coding Theory and Information Theory, December 15-18, 2003, Rutgers University, Piscataway, New Jersey*. [S.l.], v. 68: 145-177, 2003.

[5] A. P. Firby e C. F. Gardiner. Surface topology. Elsevier, 2001.

[6] E. P. D. O. Guazzi. Caracterizações algébrica e geométrica das regiões de uniformização de curvas hiperelípticas via equação diferencial fuchsiana para a construção de constelações de sinais hiperbólicas. Tese de Doutorado, FEEC/UNICAMP, 2019.

[7] S. Katok. Fuchsian Groups. The University of Chicago Press: Chicago, 1992.

[8] C. Walkden. Hyperbolic geometry. MATH30141/60771: Manchester University, 2012.

[9] J. M. Whittaker, The uniformisation of algebraic curves, *Journal of the London Mathematical Society.*, 1930.

