UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

UFRJ

Cotas inferiores para distâncias mínimas de Códigos Algébricos Geométricos

Erik Antonio Rojas Mendoza

Rio de Janeiro
Março 2019

Cotas inferiores para distâncias mínimas de Códigos Algébricos Geométricos

Erik Antonio Rojas Mendoza

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Dra. Luciane Quoos Conte

Rio de Janeiro
Março 2019

Cotas inferiores para distâncias mínimas de Códigos Algébricos Geométricos

Erik Antonio Rojas Mendoza

Dra. Luciane Quoos Conte

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática Pura.

Aprovada em 28 / 03 / 2019

Dra. Luciane Quoos Conte (UFRJ - Presidente)

Dr. Seyed Hamid Hassanzadeh Hafshejani (UFRJ)

Dr. Guilherme Chaud Tizziotti (UFU)

Dr. Alonso Sepúlveda Castellanos (UFU)

Ficha Catalográfica

Mendoza, Erik Antonio Rojas
M539c Cotas inferiores para distâncias mínimas de Códigos Algébricos Geométricos / Erik Antonio Rojas Mendoza. -- Rio de Janeiro, 2019.
67 f.

Orientadora: Luciane Quoos Conte.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Matemática, 2019.

1. Códigos AG. 2. Distância mínima. 3. Espaços de Riemann-Roch. 4. Semigrupos. I. Conte, Luciane Quoos, orient. II. Título.

Agradecimentos

À minha família. À minha mãe e meu pai por me ensinarem o valor das coisas, por incutir em mim os valores necessários para levar uma vida correta, por dar sempre o melhor deles para que seus filhos sejam felizes. Dedico este trabalho para eles. Aos meus irmãos por cuidar dos meus pais durante a minha ausência nesta aventura.

À minha orientadora pela paciência, pelos bons conselhos, por me permitir crescer matematicamente com seu apoio acadêmico, pelo apoio pessoal, por me lembrar que a matemática é divertida e, acima de tudo, pela confiança depositada em mim.

À Liss por me motivar a seguir este caminho. Por me dar força e estar sempre ao meu lado apesar da distância e das dificuldades. Por todo o amor demonstrado todos esses anos.

Aos meus amigos que fizeram parte dessa etapa, pelas discussões acadêmicas que sempre foram produtivas e pelos bons momentos de lazer. À minha amiga Nádia, que também contribuiu na realização deste trabalho, pelo seu apoio pessoal e bons conselhos em momentos importantes.

À CAPES e FAPERJ pelo apoio financeiro.

Resumo

Apresentamos diferentes tipos de cotas inferiores para a distância mínima dos Códigos Algébricos Geométricos (cotas básicas, cotas piso, cotas mistas e cotas ordem) sobre corpos de funções em uma variável sobre um corpo finito $\mathbb{F}_q$ mediante teoremas unificadores. Fornecemos a cota mista d_{ABZ^+} e reformulamos algumas cotas ordem usando a ferramenta de semigrupos. Estabelecemos uma hierarquia nos tipos de cotas apresentadas, determinando que as cotas ordem são as mais ótimas.

Palavras-Chaves: códigos AG, distância mínima, espaços de Riemann-Roch, semigrupos.

Abstract

We present different types of lower bounds for the minimum distance of the Geometric Algebraic Codes (basic bounds, floor bounds, mixed bounds and order bounds) on function fields in one variable on finite fields $\mathbb{F}_q$ through unifying theorems. We provide the mixed bound d_{ABZ^+} and reformulated some the order bounds using the semigroup tool. We have established a hierarchy in the types of bounds presented, determining that the order bound are the most optimal.

Keys-words: AG codes, minimum distance, Riemann-Roch spaces, semigroups.

Introdução

A partir da Era da Informação, que se inicia na década de oitenta, os computadores evoluíram sendo capazes de desenvolver tarefas mais sofisticadas, dentre elas a transmissão de dados. No processo de transmissão de informação é comum que os dados enviados por um remetente sejam diferentes dos dados recebidos pelo receptor. Isso se deve principalmente ao meio ou canal pelo qual a informação é enviada, pois nela existem fatores que fazem com que a informação seja modificada ou perdida, como por exemplo as interferências eletromagnéticas que estão no ambiente. Assim, surgiu a necessidade de resolver o problema de recuperar a mensagem original enviada. Já na década de 1940 Richard W. Hamming, C. E. Shannon e Marcel J. E. Golay desenvolviam métodos para resolver este problema, surgindo assim os Códigos Corretores de Erros. Em 1977, o matemático russo V. D. Goppa construiu códigos fazendo o uso de curvas algébricas sobre corpos finitos [7]. Estes códigos atualmente são chamados Códigos Algébricos Geométricos (ou simplesmente Códigos AG) e podem ser estudados a partir de duas abordagens, do ponto de vista de códigos lineares sobre corpos finitos, ou do ponto de vista de códigos diferenciais. Os códigos tem três parâmetros: o comprimento (n), a dimensão (k) e um parâmetro chamado distância mínima (d), a qual cumpre um papel importante pois quanto maior é o valor deste parâmetro, mais erros podem ser detectados e corrigidos. Atualmente, para os Códigos AG, em geral é complicado determinar o valor da distância mínima, mesmo usando ferramentas computacionais, e este problema tem sido objeto de estudo nas últimas décadas (ver [1], [2], [4], [8], [9], [11]), muitos dois quais desenvolveram métodos para estimar, mediante cotas inferiores, o valor deste parâmetro.

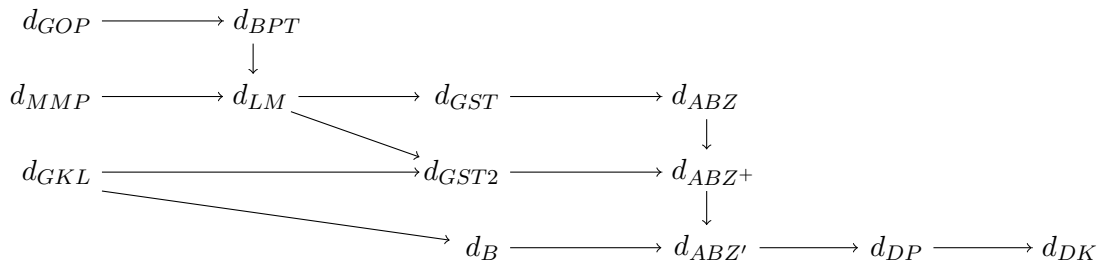
Neste trabalho fazemos um estudo dos Códigos AG, desenvolvemos as cotas básicas, as cotas piso, as cotas mistas e as cotas ordem para a distância mínima destes. Entre as cotas estudadas estão as cotas básicas desenvolvidas por V. D. Goppa (d_{GOP}) [7] e Garcia e Lax (d_{BPT}) [6], válidas para códigos do tipo $C_L(D, G)$ e $C_\Omega(D, G)$; as cotas piso desenvolvidas por Maharaj, Matthews e Pirsic (d_{MMP}) [11], Lundell e McCullough (d_{LM}) [9], Güneri, Stichtenoth e Taşkın (d_{GST}) [8, Teorema 2.4] e Duursma e Park (d_{ABZ}) [4, Teorema 2.4]; as cotas mistas desenvolvidas por Garcia, Kim e Lax (d_{GKL}) [5], Güneri, Stichtenoth e Taşkın (d_{GST2}) [8, Teorema 2.12] e fornecemos a cota mista d_{ABZ^+} (Teorema 4.30). Finalmente estão as cotas ordem desenvolvidas por Beelen (d_B) [1], Duursma e Park ($d_{ABZ'}$ e d_{DP}) [4, Teoremas 6.5 e Proposição 4.5] e Duursma e Kirov (d_{DK}) [2]. Todas estas cotas foram desenvolvidas independentemente e seria interessante termos critérios comparativos para estabelecer qual das cotas é a mais geral ou qual cota poderia determinar uma me-

lhor estimativa da distância mínima de um Código Algébrico Geométrico. Este trabalho de unificação das cotas é feito por Duursma, Kirov e Park em [3], onde são fornecidos teoremas que nos permitem comparar estas cotas.

Num primeiro momento usamos os espaços de Riemann-Roch como ferramenta principal para desenvolver todas as cotas mencionadas anteriormente com excepção das cotas d_{DP} e d_{DK}. O fato que as cotas d_{GST}, d_{GST2} e d_B sejam umas das melhores de seu tipo (piso, mista e ordem respeitivamente) mas não sejam comparáveis em geral (ver [3, Tabela 1]) nos faz fornecer a cota d_{ABZ^+} (Teorema 4.30) e provamos que a cota d_{GST2} é um caso particular desta cota (Corolário 4.32). Ao mesmo tempo estabelecemos que a cota d_{GST} é um caso particular da cota d_{ABZ} (Corolário 4.24) e que a cota d_B é um caso particular da cota $d_{ABZ'}$ (Corolário 4.40). Como as cotas d_{ABZ}, d_{ABZ^+} e $d_{ABZ'}$, as quais são obtidas originalmente seguindo o método AB de van Lint e Wilson [15] para códigos cíclicos, seguem a relação $d_{ABZ} \leq d_{ABZ^+} \leq d_{ABZ'}$ (Teoremas 4.15, 4.30 e 4.37), estabelecemos uma hierarquia entre as cotas piso, as cotas mistas e as cotas ordem, sendo estas últimas as melhores. Para exemplificar as cotas obtidas apresentamos exemplos de Códigos AG sobre o corpo de funções de Suzuki $\mathbb{F}_8(x, y)|\mathbb{F}_8$ definido pela equação

$$y^8 + y = x^2(x^8 + x).$$

Na segunda parte desenvolvemos uma ferramenta utilizando semigrupos de divisores livres de pontos de base, os quais são, junto ao teorema principal (Teorema 6.1), as peças chaves para reformular a cota ordem d_{DP} (Corolário 7.2) e a cota d_{DK} (Teorema 7.1) e poder compará-las com as demais cotas. O resultado deste trabalho é apresentado no diagrama a seguir.



No diagrama cada seta do tipo $d_X \longrightarrow d_Y$ indica que a cota d_Y melhora a cota d_X, isto pode acontecer por dois motivos: porque adicionamos hipóteses para melhorá-la ou porque a cota d_X é um caso particular da cota d_Y.

Nas duas primeiras seções introduzimos as ferramentas necessárias para definir um Código Algébrico Geométrico. Mais precisamente, na primeira seção introduzimos o conceito geral de Códigos Corretores de Erros, vemos quais são os parâmetros de um código e como estes se relacionam. Definimos também os códigos lineares e seu dual.

A segunda seção é dedicada ao estudo de corpo de funções. Nesta estudamos os conceitos de Anéis de Valorização, Lugares e Valorizações Discretas, e vemos que estes conceitos coincidem no estudo de corpo de funções. Também estudamos os conceitos de divisores e diferenciais de Weil, os quais são a base para a definição dos Códigos AG. Apresentamos teoremas fundamentais, como o teorema de Riemann-Roch e o teorema da Dualidade, e fornecemos também resultados que nos ajudam a desenvolver este trabalho, entre eles estão os resultados relacionados a Lacunas de Weierstrass.

Na seção 3 definimos os Códigos AG usando as ferramentas desenvolvidas nas seções 1 e 2. Definimos os códigos lineares do tipo $C_L(D, G)$ e códigos diferencias $C_\Omega(D, G)$, e vemos a relação existente entre eles. Fornecemos relação entre os parâmetros destes códigos. Finalizamos esta seção com o conceito de códigos equivalentes.

Na quarta seção apresentamos os diferentes tipos de cotas para a distância mínima de um Código Algébrico Geométrico, entre elas estão as cotas básicas, as cotas piso, as cotas mistas e as cotas ordem. Vemos também a relação entre elas e damos exemplos de como estas funcionam sobre o corpo de funções de Suzuki em $\mathbb{F}_8$.

Nas seções 5 e 6 desenvolvemos novas ferramentas para o estudo de cotas. Aqui introduzimos o conceito de semigrupos livres de pontos de base e apresentamos cotas inferiores para a distância mínima em função destes semigrupos. Além disso, apresentamos o teorema principal deste trabalho (Teorema 6.1), o qual fornece uma maneira de determinar estimativas para a distância mínima.

Na última seção retomamos o estudo das cotas ordem e reformulamos algumas cotas deste tipo fazendo uso do teorema principal e as ferramentas novas estudadas. Ao final do trabalho anexamos um apêndice onde colocamos algoritmos para calcular as diferentes cotas apresentadas.

Sumário

1 Códigos Corretores de Erros

Nesta seção introduzimos o conceito de Código Corretores de Erros, estudamos suas propriedades e a relação existente entre seus parâmetros no caso de que este seja linear. Desenvolvemos o conteúdo necessário para estudar, em uma seção posterior, uma subfamília destes, os chamados códigos AG.

Começamos definindo os conceitos básicos de um código.

Definição 1.1. *Seja $\mathcal{A}$ um conjunto finito não vazio (o qual será chamado alfabeto) e n um número natural. Um subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$ é chamado um código de comprimento n e os elementos de $\mathcal{C}$ são chamados palavras do código.*

Denotamos por S a cardinalidade do conjunto $\mathcal{A}$ e dizemos que o código $\mathcal{C}$ é um código S-ário de comprimento n. Definimos a seguir a distância entre dois elementos de $\mathcal{A}^n$.

Definição 1.2 (Distância de Hamming)**.** *Dados $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ dois elementos de $\mathcal{A}^n$, definimos a distância entre estes dois elementos como*

$$d(x, y) := |\{i : x_i \neq y_i\}|.$$

É fácil observar que a distância definida é uma métrica no conjunto $\mathcal{A}^n$. Agora definamos o conceito mais importante para nosso trabalho, a distância mínima de um código.

Definição 1.3. *Seja $\mathcal{C} \subseteq \mathcal{A}^n$ um código, definimos a distância mínima do código $\mathcal{C}$ por*

$$d(\mathcal{C}) := \min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}.$$

Vamos distinguir três parâmetros importantes num código $\mathcal{C}$: o comprimento do código (n), o número de palavras (M) e a distância mínima (d). Para enfatizar isso, diremos que $\mathcal{C}$ é um $[n, M, d]$ código.

A teoria de códigos corretores de erros foi desenvolvida para resolver problemas na transmissão de dados, pois muitas vezes a mensagem recebida é diferente daquela que foi enviada e isto pode ocorrer devido a erros humanos (como erros de digitação) ou erros de natureza externa chamados comumente de ruído (como ondas eletromagnéticas). Assim, os que trabalham nesta teoria desenvolvem métodos que permitam detectar e corrigir estes erros. A ideia básica desta teoria é codificar a mensagem inicial adicionando informação redundante, de forma que, ao receber a mensagem modificada pelo ruído, seja possível recuperar a mensagem original.

Exemplo 1.4. *Suponhamos que ao apertar as teclas* $\leftarrow$, $\uparrow$, $\rightarrow$ *e* $\downarrow$ *de um computador, este envie a seguinte informação binária a sua memória:*

$$\leftarrow = \ 00 \qquad \uparrow = \ 01 \qquad \rightarrow = \ 10 \qquad \downarrow = \ 11$$

Para ter a segurança de que a informação chegue ao receptor de forma correta, podemos codificar nossa informação mediante redundância definindo o código

$$\mathcal{C} = \{000000, 010101, 101010, 111111\}$$

o qual significa que ao apertar as teclas serão enviadas as seguintes informações:

$$\leftarrow = \ 000000 \qquad \uparrow = \ 010101 \qquad \rightarrow = \ 101010 \qquad \downarrow = \ 111111$$

Assim, neste caso, se houver problemas ao transmitir a informação e chega-se à memória do computador a palavra 100000*, esta procuraria a palavra mais próxima, que neste caso é* 000000 *correspondente à tecla* $\leftarrow$*, e a corrigiria.*

O seguinte resultado mostra a importância da distância mínima de um código para corrigir erros.

Teorema 1.5. *Seja* $\mathcal{C}$ *um código com distância mínima* d *e seja*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Então, é possível detectar até $d-1$ *erros e corrigir até* κ *erros.*

Demonstração. Seja x uma palavra de $\mathcal{C}$ transmitida e suponhamos que foi recebida a palavra y com $t \leq d-1$ erros cometidos durante a transmissão. Portanto temos que $d(x,y) = t \leq d-1 < d$, o qual significa que $y \notin \mathcal{C}$ pois d é a distância mínima. Assim o erro pode ser detectado.
Por outro lado, supondo que $t \leq \kappa$, seque que $d(x,y) = t \leq \kappa$. Se existe $x' \in \mathcal{C}$ tal que $d(y,x') = t \leq \kappa$ então

$$d(x,x') \leq d(x,y) + d(y,x') \leq 2\kappa < d.$$

Isto implica que $x' = x$ é a única palavra de $\mathcal{C}$ tal que $d(x,y) \leq \kappa$, ou seja, x é a palavra mais próxima de y e é possível corrigir y por x. □

Fixando como alfabeto o corpo finito $\mathbb{F}_q$, onde q é a potência de um número primo, temos as seguintes definições.

Definição 1.6. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código. O código $\mathcal{C}$ é denominado linear se $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$.*

Neste caso dizemos que $\mathcal{C}$ é um $[n, k, d]$ código, onde n é o comprimento, d é a distância mínima e k é a dimensão de $\mathcal{C}$ como subespaço vetorial de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$.

Observação 1.7. *A dimensão do código linear está relacionado com o número de palavras deste, pois se a dimensão é k então o número de palavras do código é q^k, onde q é a cardinalidade do alfabeto $\mathbb{F}_q$.*

Definição 1.8. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear e seja $c = (c_1, \ldots, c_n) \in \mathcal{C}$, então*

$$wt(c) := d(c, 0) = |\{i : c_i \neq 0\}|$$

é chamado peso da palavra c.

Com a definição do peso de uma palavra podemos provar que a distância mínima de um código linear $\mathcal{C}$ satisfaz

$$d(\mathcal{C}) = \min\{wt(c) : 0 \neq c \in \mathcal{C}\},$$

pois basta observar que os conjuntos $\{d(x, y) : x,\, y \in \mathcal{C}, x \neq y\}$ e $\{wt(c) : 0 \neq c \in \mathcal{C}\}$ são iguais uma vez que o código é linear.

Definição 1.9. *O produto interno canônico em $\mathbb{F}_q^n$ é definido por*

$$\langle a, b\rangle := \sum_{k=1}^{n} a_k b_k,$$

onde $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ estão em $\mathbb{F}_q^n$.

Definição 1.10. *Se $\mathcal{C} \subseteq \mathbb{F}_q^n$ é um código linear, então o espaço vetorial*

$$\mathcal{C}^{\perp} := \{x \in \mathbb{F}_q^n : \langle x, y\rangle = 0 \text{ para todo } y \in \mathcal{C}\}$$

é chamado o dual de $\mathcal{C}$.

Da álgebra linear sabemos que $\mathcal{C}^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$, portanto $\mathcal{C}^{\perp}$ é também um código linear.

Definição 1.11. *Os códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ em $\mathbb{F}_q^n$ são chamados equivalentes se existe um vetor $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$ tal que $\mathcal{C}_2 = a.\mathcal{C}_1$, ou seja,*

$$\mathcal{C}_2 = \{(a_1 c_1, \ldots, a_n c_n) : (c_1, \ldots, c_n) \in \mathcal{C}_1\}.$$

É fácil observar que dois códigos equivalentes tem sempre os mesmos parâmetros. A seguinte proposição relaciona os parâmetros de um código linear.

Proposição 1.12 (Cota de Singleton)**.** *Para um $[n, k, d]$ código linear $\mathcal{C} \subseteq \mathbb{F}_q^n$ temos*

$$k + d \leq n + 1.$$

Demonstração. Seja o subespaço E de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$ dado por

$$E = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ para } i \geq d\}.$$

Temos que $\dim E = d - 1$. Além disso, se $a \in E$ então $wt(a) \leq d - 1$, portanto $E \cap \mathcal{C} = \emptyset$. Assim $k + (d - 1) = \dim \mathcal{C} + \dim E = \dim (\mathcal{C} + E) \leq n$, logo $k + d \leq n + 1$. □

Do Exemplo 1.4 e do Teorema 1.5, é claro que quanto maior sejam o comprimento do código, o número de palavras dele e a distância mínima, mais efetivo vai ser o código. Mas pela cota de Singleton temos que

$$k + d \leq n + 1,$$

ou seja, os parâmetros k e d estão controlados por n. A questão de achar valores satisfatórios (dependendo do problema) para estes parâmetros é conhecida como o problema principal da teoria de códigos.

2 Corpos de funções

Nesta seção vamos fornecer as ferramentas algébricas necessárias para a construção dos códigos algébricos geométricos. Mais detalhes podem ser encontrados em [12], [13] e [14].

Seja K um corpo.

Definição 2.1. *Um corpo de funções $F|K$ em uma variável sobre K é uma extensão de corpos $F \supseteq K$ tal que F é uma extensão finita de $K(x)$, para algum $x \in F$ transcendente sobre K.*

Definição 2.2. *Seja $F|K$ um corpo de funções. Definimos o corpo de constantes de $F|K$ como*

$$\overline{K} := \{z \in F : z \text{ é algébrico sobre } K\}.$$

Notemos que $\overline{K}$ é o fecho algébrico de K sobre F. Além disso, é importante ver que $F|\overline{K}$ é também um corpo de funções.

2.1 Anéis de valorização, lugares e valorizações discretas

A seguir, definimos os conceitos de anel de valorização, lugar e valorização discreta, e veremos como estes conceitos são equivalentes.

Definição 2.3. *Um anel de valorização de um corpo de funções $F|K$ é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:*

i) $K \subsetneq \mathcal{O} \subsetneq F$, *e*

ii) para todo $z \in F$ *temos que* $z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$.

Vejamos como se comportam os anéis de valorização de corpos de funções.

Proposição 2.4. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $F|K$, então:*

i) $\mathcal{O}$ é um anel local.

ii) Seja $0 \neq x \in F$ *e P o único ideal maximal de $\mathcal{O}$, então* $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.

Teorema 2.5. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $F|K$ e seja P seu único ideal maximal, então:*

i) P é um ideal principal.

ii) Se $P = \langle t \rangle$ *então cada* $0 \neq z \in F$ *tem uma única representação da forma* $z = t^n u$ *para algum* $n \in \mathbb{Z}$ *e* $u \in \mathcal{O}^\times$. *Aqui* $\mathcal{O}^\times$ *é o conjunto das unidades do anel $\mathcal{O}$ e t é dito o elemento uniformizante local em P.*

iii) $\mathcal{O}$ é um domínio de ideais principais. Mais precisamente, se $P = \langle t \rangle$ *e* $\{0\} \neq I \subseteq \mathcal{O}$ *é um ideal, então* $I = \langle t^n \rangle$ *para algum* $n \in \mathbb{N}$.

Um anel de valorização que satisfaz as propriedades do Teorema 2.5 é chamado um anel de valorização discreta. Em particular, todo anel de valorização de um corpo de funções é um anel de valorização discreta.

Outros dois conceitos importantes são os lugares de um corpo de funções e as valorizações discretas.

Definição 2.6. *Seja $F|K$ um corpo de funções. Um lugar P de $F|K$ é um ideal maximal de algum anel de valorização de $F|K$ e denotamos por*

$$\mathbb{P}_F := \{P : P \text{ é um lugar de } F|K\}$$

o conjunto de todos os lugares de $F|K$.

Observação 2.7. *Se P é um lugar de $F|K$ então ele determina completamente o seu anel de valorização correspondente, de fato, $\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}$. Aqui $\mathcal{O}_P$ é chamado anel de valorização do lugar P. Com isto vemos que os conceitos de anel de valorização e lugar são equivalentes.*

Definição 2.8. *Uma valorização discreta de $F|K$ é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

i) $v(x) = \infty \Leftrightarrow x = 0$.

ii) $v(xy) = v(x) + v(y)$ *para todo* $x, y \in F$.

iii) $v(x + y) \geq \min\{v(x), v(y)\}$ *para todo* $x, y \in F$.

iv) Existe um elemento $z \in F$ *tal que* $v(z) = 1$.

v) $v(a) = 0$ *para todo* $0 \neq a \in K$.

Neste contexto o símbolo ∞ é um elemento satisfazendo $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todo $n, m \in \mathbb{Z}$.

Vejamos agora como cada elemento de $\mathbb{P}_F$ define uma valorização discreta de $F|K$, de fato, para cada lugar $P \in \mathbb{P}_F$ definimos a função

$$v_P : F \to \mathbb{Z} \cup \{\infty\}$$

dada por $v_P(0) = \infty$ e para cada $0 \neq z \in F$ temos que, pelo Teorema 2.5, ele pode ser escrito de forma única como $z = t^n u$, onde $P = \langle t \rangle$, $u \in \mathcal{O}_P^\times$ e $n \in \mathbb{Z}$. Assim definimos $v_P(z) = n$.

Teorema 2.9. *Seja $F|K$ um corpo de funções e $P \in \mathbb{P}_F$ um lugar, então a função v_P define uma valorização discreta de $F|K$. Além disso temos*

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},$$

$$\mathcal{O}_P^\times = \{z \in F : v_P(z) = 0\},$$

$$P = \{z \in F : v_P(z) > 0\}.$$

Por outro lado, suponha que v seja uma valorização discreta de $F|K$. Então o conjunto $P := \{z \in F : v(z) > 0\}$ é um lugar de $F|K$ e $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ é o seu anel de valorização correspondente.

Deste modo vimos que os conceitos de anel de valorização num corpo de funções, um lugar e uma valorização discreta são conceitos equivalentes.

Definição 2.10. *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se $v_P(z) > 0$, e P é um polo de z se $v_P(z) < 0$.*

A próxima proposição mostra que todo corpo de funções tem pelo menos um lugar.

Proposição 2.11. *Seja $F|K$ um corpo de funções. Um elemento de F transcendente sobre K tem pelo menos um zero e um polo, em particular $\mathbb{P}_F \neq \emptyset$.*

Seja P um lugar de $F|K$ e $\mathcal{O}_P$ seu anel de valorização correspondente. Notemos primeiro que o quociente $\mathcal{O}_P/P$ é um corpo, pois P é um ideal maximal, e contém o corpo K. Para cada $x \in \mathcal{O}_P$ definamos $x(P) := x + P \in \mathcal{O}_P/P$ e para cada $x \notin \mathcal{O}_P$, $x(P) := \infty$. Deste modo construímos uma aplicação $x \mapsto x(P)$ de F em $\mathcal{O}_P/P \cup \{\infty\}$.

Definição 2.12. *Seja P um lugar do corpo de funções $F|K$,*

i) $F_P := \mathcal{O}_P/P$ é o corpo de classes residuais de P. A aplicação $x \mapsto x(P)$ de F em $F_P \cup \{\infty\}$ é chamada aplicação de classes residuais com respeito a P.

ii) $deg\, P := [F_P : K]$ é chamado o grau de P. Um lugar com grau 1 é chamado um lugar racional.

Observação 2.13. *Note que se $deg\, P = 1$ então $F_P = K$.*

O seguinte resultado diz que todo lugar de um corpo de funções tem grau finito.

Proposição 2.14. *Se P é um lugar do corpo de funções $F|K$ e $0 \neq x \in P$, então*

$$deg\, P \leq [F : K(x)] < \infty.$$

2.2 Divisores

Na seção anterior dissemos que $F|\overline{K}$ também é um corpo de funções, onde $\overline{K}$ é o corpo de constantes do corpo de funções $F|K$. De agora em diante assumiremos que $\overline{K} = K$, isto é, o corpo K será algebricamente fechado sobre o corpo F.

Definição 2.15. *O grupo dos divisores de $F|K$ é definido como o grupo abeliano livre gerado pelos lugares de $F|K$. Este grupo é denotado por $Div(F)$ e seus elementos são chamados divisores. Em outras palavras um divisor é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} v_P(D)P$$

com $v_P(D) \in \mathbb{Z}$ *e* $v_P(D) = 0$ *para quase todo* P.
Definimos o suporte do divisor D *como*

$$supp\, D := \{P \in \mathbb{P}_F : v_P(D) \neq 0\}.$$

Podemos definir um ordem parcial no grupo $Div(F)$ da seguinte maneira:

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F.$$

Se $D_1 \leq D_2$ e $D_1 \neq D_2$ escrevemos $D_1 < D_2$. Além disso, um divisor D será chamado de efetivo se $D \geq 0$.

Definição 2.16. *Definimos o grau de um divisor* D *como*

$$deg\, D = \sum_{P \in \mathbb{P}_F} v_P(D) deg\, P.$$

Note que o grau de todo divisor é um número inteiro pela Proposição 2.14. Agora, pela Proposição 2.11 temos que a seguinte definição tem sentido.

Definição 2.17. *Seja* $0 \neq x \in F$ *e denotemos por* Z *(resp.* N*) ao conjunto dos zeros (resp. polos) de* x *em* $\mathbb{P}_F$*, então definimos os divisores*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \quad (x)_\infty := -\sum_{P \in N} v_P(x)P \quad e \quad (x) := (x)_0 - (x)_\infty.$$

Claramente temos que $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e $(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$.

Observação 2.18. *É importante notar que para todo elemento* $0 \neq x \in F$ *temos*

$$x \in K \Leftrightarrow (x) = 0.$$

Isto é porque estamos supondo que K *é algebricamente fechado em* F.

Os seguintes conceitos desempenham um papel importante no desenvolvimento deste trabalho.

Definição 2.19. *Sejam* A *e* B *elementos de* $Div(F)$*. Dizemos que o divisor* A *é equivalente ao divisor* B*, e denotamos* $A \sim B$*, se existe* $0 \neq x \in F$ *tal que*

$$A = B + (x).$$

É fácil verificar que esta relação é uma relação de equivalência em $Div(F)$. Agora definimos o espaço de Riemann-Roch de um divisor.

Definição 2.20. *Sejam A um divisor, definimos o espaço de Riemann-Roch associado ao divisor A como*

$$L(A) := \{x \in F : (x) + A \geq 0\} \cup \{0\}.$$

Proposição 2.21. *Para cada divisor $A \in Div(F)$, o espaço de Riemann-Roch associado ao divisor A é um espaço vetorial finito dimensional sobre K.*

Vejamos agora algumas das propriedades deste espaço.

Proposição 2.22. *Seja A um divisor, então*

i) $L(A) \neq \{0\}$ *se e somente se existe um divisor $A' \geq 0$ tal que $A \sim A'$.*

ii) $L(0) = K$.

iii) Se $A < 0$ temos que $L(A) = \{0\}$.

iv) Se A' é um divisor tal que $A' \sim A$ então $L(A') \cong L(A)$.

Proposição 2.23. *Sejam A e B elementos de $Div(F)$ tais que $A \leq B$, então*

i) $L(A) \subseteq L(B)$ *e* $\dim(L(B)/L(A)) \leq deg\, B - deg\, A$.

ii) Se $deg\, A = deg\, B$ então $A = B$.

Definição 2.24. *Para $A \in Div(F)$, o inteiro $\ell(A) := \dim L(A)$ é chamada a dimensão do divisor A.*

Proposição 2.25. *Sejam $0 \neq x \in F$ e $A \in Div(F)$, então*

i) $deg\,(x) = 0$.

ii) Se A' é um divisor tal que $A \sim A'$ temos $\ell(A) = \ell(A')$ e $deg\, A = deg\, A'$.

iii) Se $deg\, A < 0$ então $\ell(A) = 0$.

O seguinte resultado é fundamental para definir o gênero de um corpo de funções.

Proposição 2.26. *Existe uma constante $\gamma \in \mathbb{Z}$ não negativa tal que*

$$deg\, A - \ell(A) \leq \gamma$$

para todo $A \in Div(F)$.

Definição 2.27. *O gênero de um corpo de funções $F|K$ é definido por*

$$g := \max\{deg\, A - \ell(A) + 1 : A \in Div(F)\}.$$

Teorema 2.28. *Seja $F|K$ um corpo de funções de gênero g, então*

i) Para todo divisor $A \in Div(F)$ temos $\ell(A) \geq deg\, A + 1 - g$.

ii) Existe um inteiro c, que depende somente do corpo de funções $F|K$, tal que $\ell(A) = deg\, A + 1 - g$ para todo divisor A com $deg\, A \geq c$.

O seguinte resultado será usado nas próximas seções.

Proposição 2.29. *Sejam A, B, $E \in Div(F)$ tal que $A \leq B$, $0 \leq E$ e $supp\, E \cap supp\,(B - A) = \emptyset$, então a aplicação*

$$\varphi : \frac{L(A+E)}{L(A)} \longrightarrow \frac{L(B+E)}{L(B)}$$

dada por $\varphi(x + L(A)) = x + L(B)$ é uma aplicação linear injetiva.

Demonstração. Primeiro vejamos que φ esta bem definida. Note que $L(A) \subseteq L(A+E)$, $L(B) \subseteq L(B+E)$ e $L(A+E) \subseteq L(B+E)$. Sejam $x, y \in L(A+E)$ tais que $x + L(A) = y + L(A)$, então $x - y \in L(A) \subseteq L(B)$, portanto $\varphi(x + L(A)) = \varphi(y + L(A))$. Por outro lado, é claro que φ é uma aplicação linear. Para demonstrar a injetividade basta ver que $\mathrm{Ker}(\varphi) = \{[0]\}$. Seja $x \in L(A+E)$ tal que $x + L(A) \in \mathrm{Ker}(\varphi)$, então $\varphi(x + L(A)) = x + L(B) = L(B)$, assim $x \in L(B)$. Como $x \in L(A+E)$ e $A \leq B$ segue que $x \in L(B+E)$, logo temos

$$(x) + B + E \geq B - A \quad \text{e} \quad (x) + B + E \geq E.$$

Mas como $\mathrm{supp}\, E \cap \mathrm{supp}\,(B - A) = \emptyset$ temos que $(x) + B + E \geq B - A + E$, ou seja $(x) + A \geq 0$. Portanto $x \in L(A)$. □

Proposição 2.30. *Sejam A, $B \in Div(F)$ e P um lugar racional tais que $L(A-P) \neq L(A)$ e $L(B - P) \neq L(B)$, então*

$$L(A + B - P) \neq L(A + B).$$

Demonstração. Se A é um divisor e P é um lugar racional tais que $L(A - P) \neq L(A)$ então existe $z_1 \in L(A)$ satisfazendo

$$(z_1) \geq -A \quad \text{e} \quad (z_1) \ngeq -A + P.$$

Disto segue que

$$v_P(z_1) \geq -v_P(A) \quad \text{e} \quad v_P(z_1) < -v_P(A) + 1,$$

e portanto $v_P(z_1) = -v_P(A)$. Analogamente para o divisor B, temos que existe um $z_2 \in L(B)$ com $v_P(z_2) = -v_P(B)$.
Por outro lado, como $z_1 \in L(A)$ e $z_2 \in L(B)$ segue que $z_1 z_2 \in L(A+B)$. Supondo que $z_1 z_2 \in L(A+B-P)$ temos que $-v_P(A) - v_P(B) \geq -v_P(A) - v_P(B) + 1$, contradição; portanto $z_1 z_2 \notin L(A+B-P)$ o que implica $L(A+B) \neq L(A+B-P)$. □

2.3 Diferenciais de Weil e Teorema de Riemann-Roch

Nesta seção $F|K$ denota um corpo de funções com gênero g e $\overline{K} = K$.

Definição 2.31. *Para um divisor A, o inteiro*

$$i(A) := \ell(A) - deg\, A + g - 1$$

é chamado índice de especialidade do divisor A.

Note que, pelo Teorema 2.28, $i(A)$ é sempre um inteiro não negativo.

Definição 2.32. *Um adele é um elemento $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ do produto direto $\prod_{P \in \mathbb{P}_F} F$ tal que $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$. O conjunto de todos os adeles do corpo de funções $F|K$ será denotado como $\mathcal{A}_F$.*

O conjunto $\mathcal{A}_F$ vem ser um espaço vetorial sobre K. Além disso, podemos identificar F com um subconjunto de $\mathcal{A}_F$, de fato, somente basta identificar cada $x \in F$ com o adele $(x)_{P \in \mathbb{P}_F}$. Esta identificação tem sentido pois todo elemento de F tem um número finito de polos pela Proposição 2.11. Assim podemos estender naturalmente a valorização v_P definindo

$$v_P(\alpha) := v_P(\alpha_P)$$

onde α_P é a P-componente de $\alpha \in \mathcal{A}_F$.

Definição 2.33. *Para $A \in Div(F)$ definimos*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F : v_P(\alpha) + v_P(A) \geq 0 \text{ para todo } P \in \mathbb{P}_F\}.$$

Claramente o conjunto $\mathcal{A}_F(A)$ é um K-subespaço vetorial de $\mathcal{A}_F$.

Definição 2.34. *Uma diferencial de Weil de $F|K$ é um mapa K-linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in Div(F)$. O conjunto de todas as diferenciais de Weil de $F|K$ será denotado por Ω_F. Para $A \in Div(F)$ definimos*

$$\Omega_F(A) := \{\omega \in \Omega_F : \omega \text{ se anula em } \mathcal{A}_F(A) + F\}.$$

Pode-se mostrar que Ω_F é um K-espaço vetorial e $\Omega_F(A)$ é um K-subespaço vetorial de Ω_F. Além disso temos que $\dim_F \Omega_F = 1$.

Proposição 2.35. *Para $A \in Div(F)$ temos $\dim \Omega_F(A) = i(A)$.*

Lema 2.36. *Seja $0 \neq \omega \in \Omega_F$. Existe um único divisor W tal que ω se anula em $\mathcal{A}_F(W) + F$, e se ω se anula em $\mathcal{A}_F(A) + F$ para $A \in Div(F)$, então $A \leq W$.*

A seguinte definição mostra como relacionar o conceito de divisor com as diferenciais de Weil.

Definição 2.37. *Seja $F|K$ um corpo de funções, então*

i) O divisor (ω) de um diferencial de Weil $\omega \neq 0$ é o único divisor de $F|K$ satisfazendo:

   a) ω se anula em $\mathcal{A}_F((\omega)) + F$, e

   b) se ω se anula em $\mathcal{A}_F(A) + F$ então $A \leq (\omega)$.

ii) Para $0 \neq \omega \in \Omega_F$ e $P \in \mathbb{P}_F$, definimos $v_P(\omega) := v_P((\omega))$.

iii) Um divisor W é chamado de divisor canônico de $F|K$ se $W = (\omega)$ para algum $\omega \in \Omega_F$.

Observação 2.38. *A existência e unicidade do divisor (ω) para $0 \neq \omega \in \Omega_F$ segue do Lema 2.36.*

Observação 2.39. *Da Definição 2.34 segue que $\Omega_F(A) = \{\omega \in \Omega_F : \omega = 0 \text{ ou } (\omega) \geq A\}$. Também podemos observar que $\dim \Omega_F(0) = g$.*

Proposição 2.40. *Dado $F|K$ um corpo de funções, então*

i) Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos $(x\omega) = (x) + (\omega)$.

ii) Qualquer dois divisores canônicos de $F|K$ são equivalentes.

Os seguintes teoremas são resultados centrais na teoria de corpos de funções.

Teorema 2.41 (Teorema da Dualidade)**.** *Sejam A um divisor arbitrário e W um divisor canônico de $F|K$, então*

$$i(A) = \ell(W - A).$$

Teorema 2.42 (Teorema de Riemann-Roch)**.** *Seja W um divisor canônico de $F|K$. Então para qualquer divisor $A \in Div(F)$ temos*

$$\ell(A) = deg\, A + 1 - g + \ell(W - A).$$

Como consequência do Teorema 2.42 temos os seguintes resultados.

Corolário 2.43. *Para qualquer divisor canônico W temos*

$$deg W = 2g - 2 \qquad e \qquad \ell(W) = g.$$

Corolário 2.44. *Se A é um divisor tal que $deg\, A \geq 2g - 1$, então*

$$\ell(A) = deg\, A + 1 - g.$$

Definição 2.45. *Seja $P \in \mathbb{P}_F$.*

i) Para $x \in F$ seja $i_P(x) \in \mathcal{A}_F$ o adele cuja P-componente é x e as demais componentes são zero.

ii) Para uma diferencial de Weil $\omega \in \Omega_F$ definimos a componente local $\omega_P : F \to K$ por $\omega_P(x) := \omega(i_P(x))$.

Claramente ω_P é um mapa K-linear.

Observação 2.46. *Seja P um lugar racional e η uma diferencial de Weil tal que $v_P(\eta) \geq -1$, então*

$$\eta_P(1) = 0 \Leftrightarrow v_P(\eta) \geq 0.$$

2.4 Lacunas

Nesta seção vamos introduzir o conceito de lacunas, estudaremos suas propriedades e veremos que esta é uma ferramenta útil para nosso trabalho. Para mais detalhes ver [12].

Proposição 2.47. *Seja $A \in Div(F)$ e P um lugar racional, então*

$$L(A + nP) = L(A + (n-1)P) \Leftrightarrow L(W - A - nP) \neq L(W - A - (n-1)P),$$

onde W é um divisor canônico e n um número inteiro.

Definição 2.48. *Seja P um lugar racional e B um divisor. Dizemos que o número natural n é uma B-lacuna em P se não existe $x \in F$ tal que*

$$((x) + B)_\infty = nP.$$

Na definição de acima, quando $B = 0$ as B-lacunas são chamadas simplesmente de lacunas de Weierstrass.

Definição 2.49. *Seja P um lugar racional e B um divisor. Dizemos que o número n é uma ordem em P para B se existe $w \in \Omega_F(B)$ tal que $v_P((w) - B) = n$.*

Proposição 2.50. *Seja P um lugar racional e B um divisor, então as seguintes proposições são equivalentes:*

i) n é uma ordem em P para B.

ii) Existem $w \in \Omega_F$ e um divisor $E \geq 0$ tal que $(w) - B \sim nP + E$.

O seguinte teorema estabelece uma relação entre os conceitos de lacuna e ordem. Antes um resultado prévio.

Lema 2.51. *Sejam P um lugar racional e B um divisor, então n é uma B-lacuna em P se e somente se $L((n-1)P + B) = L(nP + B)$.*

Teorema 2.52. *Sejam P um lugar racional e B um divisor, então n é uma B-lacuna em P se e somente se $(n-1)$ é uma ordem em P para B.*

3 Códigos Algébricos Geométricos

Passaremos agora à construção dos Códigos Algébricos Geométricos, os quais são uma subfamília dos Códigos Corretores de Erros. Estes são obtidos usando a ferramenta desenvolvida na seção anterior, os corpos de funções. Para esta construção fixamos a seguinte notação que será válida para o resto de nosso trabalho:

- $F|\mathbb{F}_q$ representa um corpo de funções de gênero g com corpo de constantes $\mathbb{F}_q$.
- D é o divisor definido por $D := P_1 + \cdots + P_n$ onde os P_i são lugares racionais distintos em $F|\mathbb{F}_q$.
- G um divisor tal que $\operatorname{supp} D \cap \operatorname{supp} G = \emptyset$.
- K representa um divisor canônico.

Fixada a notação, observe que para um $x \in L(G)$ e para $P \in \operatorname{supp} D$ temos $v_P(x) \geq 0$ pois $(x)+G \geq 0$ e $\operatorname{supp} D \cap \operatorname{supp} G = \emptyset$, logo $x \in \mathcal{O}_P$ e $x(P) \in \mathcal{O}_P/P \cong \mathbb{F}_q$ pois $\deg P = 1$. Deste modo, a seguinte definição tem sentido.

Definição 3.1. *O código algébrico geométrico $C_L(D,G)$ associado aos divisores D e G é definido como*

$$C_L(D,G) := \{(x(P_1), \ldots, x(P_n)) : x \in L(G)\} \subseteq \mathbb{F}_q^n.$$

O seguinte resultado dá o valor do parâmetro k e uma estimativa para a distância mínima d a qual será de importância mais adiante.

Teorema 3.2. *O código $C_L(D,G)$ é um $[n,k,d]$ código com parâmetros*

$$k = \ell(G) - \ell(G-D) \quad e \quad d \geq n - deg\, G.$$

Demonstração. Definindo o mapa

$$ev_D : L(G) \longrightarrow \mathbb{F}_q^n$$

dada por $ev_D(x) = (x(P_1), \ldots, x(P_n))$, temos que ela é uma aplicação linear e sua imagem é $C_L(D,G)$, assim ela é um código linear. Além disso

$$\operatorname{Ker}(ev_D) = \{x \in L(G) : v_{P_i}(x) > 0 \text{ para } i = 1, \ldots, n\} = L(G-D),$$

portanto $k = \dim(C_L(D,G)) = \ell(G) - \ell(G-D)$.
Supondo que $C_L(D,G) \neq 0$, seja $x \in L(G)$ tal que $wt(ev_D(x)) = d$, então exatamente $n-d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ em $\operatorname{supp} D$ são zeros de x, logo

$$0 \neq x \in L(G - (P_{i_1} + \cdots + P_{i_{n-d}}))$$

e segue que $0 \leq \deg(G - (P_{i_1} + \cdots + P_{i_{n-d}})) = \deg G - n + d$. □

Outro código AG pode ser associado aos divisores D e G usando componentes locais de diferenciais de Weil.

Definição 3.3. *Definimos o código algébrico geométrico $C_\Omega(D,G)$ associados aos divisores D e G como*

$$C_\Omega(D,G) := \{(\eta_{P_1}(1), \ldots, \eta_{P_n}(1)) : \eta \in \Omega_F(G-D)\} \subseteq \mathbb{F}_q^n.$$

Da mesma maneira que para o código $C_L(D,G)$, o seguinte resultado apresenta estimativas para seus parâmetros.

Teorema 3.4. *O código $C_\Omega(D,G)$ é um $[n,k,d]$ código com parâmetros*

$$k = i(G-D) - i(G) \quad e \quad d \geq deg\, G - (2g-2).$$

Demonstração. Consideramos a aplicação linear

$$\varrho_D : \Omega_F(G-D) \longrightarrow \mathbb{F}_q^n$$

dada por $\varrho(w) = (w_{P_1}(1), \ldots, w_{P_n}(1))$. A imagem de dita aplicação é $C_\Omega(D,G)$, assim ela é um código linear. Da Observação 2.46 temos $\mathrm{Ker}(\varrho_D) = \Omega_F(G)$ e, portanto, $k = i(G-D) - i(G)$. Por outro lado, seja $\varrho_D(w) \in C_\Omega(D,G)$ uma palavra tal que $wt(\varrho_D(w)) = m > 0$, então $w_{P_i}(1) = 0$ para certos índices $i = i_1, \ldots, i_{n-m}$, logo

$$w \in \Omega_F(G - (D - \sum_{j=1}^{n-m} P_{i_j}))$$

da Observação 2.46. Como $\Omega_F(A) \neq 0$, onde $A = G - (D - \sum_{j=1}^{n-m} P_{i_j})$, temos que $\deg A \leq 2g-2$ do Corolário 2.44, logo

$$2g - 2 \geq \deg G - (n - (n-m)) = \deg G - m,$$

mas como m é arbitrário segue que $d \geq \deg G - (2g-2)$. □

Podemos relacionar os códigos $C_L(D,G)$ e $C_\Omega(D,G)$ mediante o seguinte teorema.

Teorema 3.5. *Sejam $C_L(D,G)$ e $C_\Omega(D,G)$ os códigos AG associados aos divisores D e G, então*

$$C_\Omega(D,G) = C_L(D,G)^\perp.$$

Demonstração. Ver [14, Teorema 2.2.8]. □

Outra relação entre estes dois códigos vem no seguinte resultado que nos diz que os códigos obtidos via diferenciais de Weil são, de fato, códigos do tipo $C_L(D,.)$.

Proposição 3.6. *Existe uma diferencial de Weil η com $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para todo $i = 1, \ldots, n$ tal que*

$$C_\Omega(D,G) = C_L(D, D - G + (\eta)).$$

Demonstração. Ver [14, Proposição 2.2.10]. □

Agora vejamos outro resultado que relaciona divisores equivalentes e códigos equivalentes.

Proposição 3.7. *Seja D um divisor,*

i) Se G_1 e G_2 são divisores equivalentes tal que $\operatorname{supp} G_1 \cap \operatorname{supp} D = \operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset$, então os códigos $C_L(D, G_1)$ e $C_L(D, G_2)$ são equivalentes. O mesmo acontece com códigos do tipo $C_\Omega(D, G)$.

ii) Se um código $\mathcal{C} \subseteq \mathbb{F}_q^n$ é equivalente a $C_L(D, G)$ (resp. $C_\Omega(D, G)$), então existe um divisor G' equivalente a G tal que $\operatorname{supp} G' \cap \operatorname{supp} D = \emptyset$ e $\mathcal{C} = C_L(D, G')$ (resp. $C_\Omega(D, G')$).

Demonstração. *i*) Como $G_1 \sim G_2$ então existe $0 \neq z \in F$ tal que $G_2 = G_1 - (z)$ e $v_P(z) = 0$ para $P \in \operatorname{supp} D$. Assim definindo $a := (z(P_1), \ldots, z(P_n)) \in (\mathbb{F}_q^*)^n$ a aplicação $x \mapsto xz$ de $L(G_1)$ a $L(G_2)$ é bijeção, logo $C_L(D, G_2) = a.C_L(D, G_1)$. Analogamente para o caso $C_\Omega(D, G)$.
ii) Seja $\mathcal{C} = a.C_L(D, G)$ com $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, escolha $z \in F$ tal que $z(P_i) = a_i$ para $i = 1, \ldots, n$ e defina $G' := G - (z)$, então $\mathcal{C} = C_L(D, G)$. Analogamente para o caso $C_\Omega(D, G)$. □

Uma vez que temos claros os conceitos descritos acima, podemos começar com o objetivo do trabalho de estudar cotas inferiores para a distância mínima de códigos AG.

4 Cotas inferiores para distâncias mínimas

Desta seção em diante estudaremos as diferentes cotas inferiores para a distancia mínima de um código AG e como podemos melhorá-la, melhorando a eficiência do nosso código bem como o número de erros que pode ser corrigidos. Além disso, veremos como algumas das diferentes cotas apresentadas neste trabalho podem ser comparadas.

4.1 Cotas básicas

As duas primeiras cotas que apresentamos são as cotas básicas dos Códigos AG. Uma delas já foi vista na seção anterior, a chamada cota de Goppa, e a outra é uma melhora da cota de Goppa assumindo uma condição adicional.

A cota de Goppa (d_{GOP}) para nosso parâmetro d são justamente as cotas

$$d(C_L(D,G)) \geq \deg(D-G) \quad \text{e} \quad d(C_\Omega(D,G)) \geq \deg(G-K)$$

dadas no Teorema 3.2 e no Teorema 3.4 respectivamente.

Observação 4.1. *É importante notar que um código algébrico geométrico $\mathcal{C}$ pode ser representado de duas formas, como $C_L(D,G_1)$ ou $C_\Omega(D,G_2)$. Suponhamos que estas sejam suas representações, isto é, $\mathcal{C} = C_L(D,G_1) = C_\Omega(D,G_2)$. Pela Proposição 3.6, $C_\Omega(D,G_2) = C_L(D,D-G_2+K)$, onde K é um divisor canônico satisfazendo as condições de dita Proposição. Pela Proposição 3.7 segue que $D-G_1 \sim G_2-K$, fazendo $C \sim D-G_1 \sim G_2-K$ temos*

$$d(\mathcal{C}) = d(C_L(D,G_1)) = d(C_\Omega(D,G_2)) \geq deg\, C,$$

ou seja, a cota de Goppa somente depende do grau do divisor C (chamado de suporte mínimo), independentemente da escolha da representação do código $\mathcal{C}$.

Observação 4.2. *Para casos posteriores, quando trabalhamos com o código $C_L(D,G)$ nosso divisor C representará o divisor $D-G$, e quando trabalhamos com o código $C_\Omega(D,G)$ nosso divisor C representará o divisor $G-K$.*

Como dito anteriormente temos que a Cota de Goppa se reduz ao seguinte enunciado: seja $\mathcal{C}$ um código AG (independentemente da sua representação) e C seu suporte mínimo, então

$$d(\mathcal{C}) \geq \deg C.$$

No seguinte resultado, veremos que adicionando uma hipótese podemos melhorar essa cota.

Definição 4.3. *Dizemos que um divisor A tem um ponto de base P, onde P é um lugar racional, se $L(A) = L(A-P)$.*

Vejamos a Cota Ponto de Base para códigos AG do tipo $C_L(D,G)$.

Teorema 4.4. *Se o divisor C tem um ponto de base P e $P \notin supp\, D$, então*

$$d(C_L(D,G)) \geq deg\, C + 1.$$

Demonstração. Primeiro vamos provar a seguinte afirmação:
Existe uma palavra $c \in C_L(D,G)$ com $wt(c) = \deg C = w$ se e somente se $C \sim P_{i_1} + P_{i_2} + \cdots + P_{i_w}$ para w lugares racionais distintos $P_{i_1}, \ldots, P_{i_w} \in \operatorname{supp} D$.

Seja $c \in C_L(D,G)$ com peso w, sem perda de generalidade podemos supor que $c = (x(P_1), \ldots, x(P_n))$ com $x(P_i) \neq 0$ para $1 \leq i \leq w$ e $x(P_i) = 0$ para $w+1 \leq i \leq n$, onde $x \in L(G)$. Como $x(P_i) = 0$ para $w+1 \leq i \leq n$ temos $v_{P_i}(x) \geq 1$ para $w+1 \leq i \leq n$, e como $x \in L(G)$ e $\operatorname{supp} D \cap \operatorname{supp} G = \emptyset$ segue que

$$\begin{aligned}(x) &\geq P_{w+1} + \cdots + P_n - G \\ &\geq P_{w+1} + \cdots + P_n + C - D \\ &\geq C - P_1 - P_2 - \cdots - P_w.\end{aligned}$$

Mas $\deg(x) = \deg(C - P_1 - P_2 - \cdots - P_w) = 0$, assim $(x) = C - P_1 - P_2 - \cdots - P_w$, ou seja, $C \sim P_1 + \cdots + P_w$.
Por outro lado, se $C \sim P_{i_1} + P_{i_2} + \cdots + P_{i_w}$ então existe $0 \neq x \in F$ tal que

$$\begin{aligned}(x) &= C - P_{i_1} - P_{i_2} - \cdots - P_{i_w} \\ &= D - G - P_{i_1} - P_{i_2} - \cdots - P_{i_w} \\ &= P_1 + \cdots + \widehat{P_{i_1}} + \cdots + \widehat{P_{i_w}} + \cdots + P_n - G,\end{aligned}$$

onde se conclui que $x \in L(G)$, $x(P_{i_j}) \neq 0$ para $1 \leq j \leq w$ e $x(P) = 0$ para os demais lugares racionais no $\operatorname{supp} D$. Logo $c = (x(P_1), \ldots, x(P_n)) \in C_L(D,G)$ é tal que $wt(c) = \deg C$.
Voltando à demostração da proposição, supondo que existe uma palavra $c \in C_L(D,G)$ com peso $wt(c) = \deg C = w$, então existem $P_{i_1}, \ldots, P_{i_w} \in \operatorname{supp} D$ e $0 \neq z \in F$ tais que $C + (z) = P_{i_1} + \cdots + P_{i_w} \geq 0$, ou seja $z \in L(C) = L(C - P)$, logo $C + (z) = P_{i_1} + P_{i_2} + \cdots + P_{i_w} \geq P$ com $P \notin \operatorname{supp} D$, que é uma contradição, assim $d(C_L(D,G)) > \deg C$ ou $d(C_L(D,G)) \geq \deg C + 1$. □

Esta cota também pode ser aplicada para um código do tipo $C_\Omega(D,G)$, mas para provar isto precisamos de um resultado prévio.

Lema 4.5. *Dado um divisor $G \sim K + C$ e um lugar racional P, existem divisores A e B tais que $G \sim A + B + P$, $L(A+P) = L(A)$ e $L(B+P) = L(B)$ se e somente se $L(C) = L(C-P)$.*

Demonstração. Pela Proposição 2.47 temos que $L(K-A) \neq L(K-A-P)$ e $L(K-B) \neq L(K-B-P)$, e pela Proposição 2.30 segue que $L(K-A+K-B) \neq L(K-A+K-B-P)$. Agora, como $G \sim A + B + P$ e $G \sim K + C$ temos que $K - C + P \sim K - A + K - B$ e portanto $L(K - C + P) \neq L(K - C)$. Usando novamente a Proposição 2.47 concluímos que $L(C) = L(C - P)$.
Por outro lado, fazendo $A = C - P$ e $B = K$ temos que $G \sim K + C = A + B + P$ e

$L(A+P) = L(C) = L(C-P) = L(A)$. Para mostrar que $L(B+P) = L(B)$ observamos que $\deg(K+P) = 2g-1$, com isso $\ell(K+P) = \deg(K+P) + 1 - g = g = \ell(K)$. Logo como $L(K) \subseteq L(K+P)$ segue que $L(K) = L(K+P)$, ou seja, $L(B) = L(B+P)$. $\square$

Vejamos agora a Cota Ponto de Base para códigos AG do tipo $C_\Omega(D,G)$.

Teorema 4.6. *Se o divisor C tem um ponto de base P com $P \notin \operatorname{supp} D$, então*

$$d(C_\Omega(D,G)) \geq deg\, C + 1.$$

Demonstração. Suponha que $d(C_\Omega(D,G)) = \deg C = w$, logo existe $\eta \in \Omega_F(G-D)$ e, sem perda de generalidade, podemos supor que $v_{P_i}(\eta) = -1$ para $i = 1, \ldots, w$ e $v_{P_i}(\eta) \geq 0$ para $i = w+1, \ldots, n$ pela Observação 2.46. Assim temos

$$(\eta) \geq G - (P_1 + \cdots + P_w).$$

Além disso, $2g-2 = \deg(\eta) \geq \deg G - w = 2g-2$, disto segue que

$$K = (\eta) = G - (P_1 + \cdots + P_w).$$

Por outro lado, do Lema 4.5 temos que $L(A+P) = L(A)$, logo pelo Teorema 2.52 e pela Proposição 2.50 existe um divisor $E \geq 0$ com $P \notin \operatorname{supp} E$ tal que $K - A \sim E$, portanto

$$\begin{aligned} K + (P_1 + \cdots + P_w) &= G \\ &\sim A + B + P \\ &\sim K - E + B + P, \end{aligned}$$

e assim

$$E + (P_1 + \cdots + P_w) \sim B + P.$$

Segue que existe $0 \neq x \in F$ tal que

$$E + (P_1 + \cdots + P_w) - P = B + (x)$$

e

$$(B + (x))_\infty = P,$$

isto é, 1 é uma B-lacuna em P, o qual é uma contradição pois temos por hipótese $L(B+P) = L(B)$ do Lema 4.5. Concluímos $d(C_\Omega(D,G)) \geq \deg C + 1$. $\square$

A Cota Ponto de Base pode ser enunciada da seguinte maneira: seja $\mathcal{C}$ um código AG (independentemente da sua representação) determinado pelo divisor D e seja C seu suporte mínimo. Se C tem um ponto de base P, onde P é um lugar racional tal que $P \notin \operatorname{supp} D$, então

$$d(\mathcal{C}) \geq \deg C + 1.$$

Assim obtemos uma melhora de uma unidade para a Cota de Goppa assumindo uma condição adicional que é a do divisor C tendo um ponto de base.

Observação 4.7. *Para exemplificar estas cotas e as demais que serão desenvolvidas, trabalharemos um caso específico. Consideremos o corpo de funções de Suzuki $\mathbb{F}_q(x,y)|\mathbb{F}_q$ definido pela equação*

$$y^q + y = x^{q_0}(x^q + x),$$

onde $q = 2q_0^2$ e $q_0 = 2^s$, $s \geq 1$. Este corpo de funções tem $q^2 + 1$ lugares racionais e seu gênero está dado por $q_0(q-1)$. Vamos trabalhar o caso $q_0 = 2$, ou seja no corpo de funções de Suzuki sobre o corpo $\mathbb{F}_8$ denotado por $\mathbb{F}_8(x,y)|\mathbb{F}_8$. Para os cálculos usamos os algoritmos desenvolvidos na plataforma Magma Calculator ([10]), que se encontram no Apêndice.

Exemplo 4.8. *De acordo com a Observação 4.7, seja P um lugar racional do corpo de funções de Suzuki e D a soma dos demais lugares racionais. Assim temos que $8 = \ell(46P - K) \neq \ell(45P - K) = 7$ e $\ell(45P - K) = \ell(44P - K) = 7$ onde K é um divisor canônico, portanto P é ponto de base do divisor $45P - K$ mas não é ponto de base do divisor $46P - K$. Logo, considerando o código $C_\Omega(D, G)$ para $G = 46P$ e $G = 45P$ obtemos as estimativas para a distância mínima, mostrada na Tabela 1, fazendo uso do Algoritmo A.*

Código	n	k	d_{GOP}	d_{BPT}
$C_\Omega(D, G = 45P)$	64	32	19	20
$C_\Omega(D, G = 46P)$	64	31	20	–

Tabela 1: Cotas básicas

No seguinte diagrama podemos ver a relação entre as cotas estudadas até o momento:

$$d_{GOP} \longrightarrow d_{BPT}$$

4.2 Cotas piso

De agora em diante trabalharemos cotas para os códigos AG do tipo $C_\Omega(D, G)$. Entre a classificação das cotas inferiores para Códigos AG estão as cotas piso, as quais serão estudadas nesta seção, assim como sua conexão com as cotas básicas. Veremos as cotas piso d_{MMP} [11], d_{LM} [9], d_{GST} [8, Teorema 2.4] e d_{ABZ} [4, Teorema 2.4].

Um dos objetivos deste trabalho é unificar estas cotas mediante teoremas e ver a relação existente entre elas. Para isto vamos desenvolver primeiro a cota denominada d_{ABZ} dada por Duursma e Park [4, Teorema 2.4], e logo veremos como as demais cotas piso são casos particulares desta última.

Lema 4.9. *Sejam G um divisor e η uma diferencial de Weil distinta de zero com divisor $(\eta) = G - D' + E$, tal que $D', E \geq 0$ e $supp\, E \cap supp\, D' = \emptyset$. Para divisores A, B e Z, tais que $G = A + B + Z$, $Z \geq 0$ e $supp\, Z \cap supp\, D' = \emptyset$, temos:*

$$deg\, D' \geq \ell(A) - \ell(A - D') + \ell(B) - \ell(B - D').$$

Demonstração. Definindo a aplicação linear

$$\varphi : \frac{L(A)}{L(A - D')} \longrightarrow \frac{L(A + E)}{L(A + E - D')} \quad \text{dada por } \varphi(x + L(A - D')) = x + L(A + E - D'),$$

temos que, da Proposição 2.29, φ está bem definida e é injetiva. Disto segue que

$$\ell(A) - \ell(A - D') \leq \ell(A + E) - \ell(A + E - D'). \tag{1}$$

De maneira análoga obtemos

$$\ell(B) - \ell(B - D') \leq \ell(B + Z) - \ell(B + Z - D') \tag{2}$$

definindo a aplicação linear

$$\psi : \frac{L(B)}{L(B - D')} \longrightarrow \frac{L(B + Z)}{L(B + Z - D')} \quad \text{dada por } \psi(x + L(B - D')) = x + L(B + Z - D').$$

Por outro lado

$$\begin{aligned} i(A + E - D') - i(A + E) &= \ell(A + E - D') - \deg(A + E - D') + g - 1 \\ &\quad - \ell(A + E) + \deg(A + E) - g + 1 \\ &= \ell(A + E - D') - \ell(A + E) + \deg D'. \end{aligned}$$

Deste modo

$$\deg D' = \ell(A+E) - \ell(A+E-D') + i(A+E-D') - i(A+E).$$

Por hipótese temos $(\eta) = G - D' + E = A + B + Z - D' + E$, então

$$\begin{aligned}
\deg D' &= \ell(A+E) - \ell(A+E-D') + i(A+E-D') - i(A+E) \\
&= \ell(A+E) - \ell(A+E-D') + i((\eta) - B - Z) \\
&\quad - i((\eta) - B - Z + D') \\
&= \ell(A+E) - \ell(A+E-D') + \ell(B+Z) - \ell(B+Z-D') \\
&\geq \ell(A) - \ell(A-D') + \ell(B) - \ell(B-D') \qquad \text{de (1) e (2).}
\end{aligned}$$

□

Definição 4.10. *Dizemos que uma palavra $c = (\eta_{P_1}(1), \ldots, \eta_{P_n}(1)) \in C_\Omega(D,G)$ tem suporte D', onde $0 \leq D' \leq D$, se $\eta_P(1) \neq 0$ para $P \in \operatorname{supp} D'$ e $\eta_P(1) = 0$ para $P \in \operatorname{supp}(D - D')$.*

Observação 4.11. *Pela Observação 2.46 temos que $v_P(\eta) = -1$ para $P \in \operatorname{supp} D'$ e $v_P(\eta) \geq 0$ para $P \in \operatorname{supp}(D - D')$.*

Observação 4.12. *Note que se uma palavra $c \in C_\Omega(D,G)$ tem suporte D', então $wt(c) = \deg D'$.*

Lema 4.13. *Uma palavra $0 \neq c \in C_\Omega(D,G)$ tem suporte D' somente se existe uma diferencial de Weil não nula $\eta \in \Omega_F(G - D')$.*

Demonstração. Se existe $0 \neq c \in C_\Omega(D,G)$ com suporte D' podemos supor que $D' = P_1 + P_2 + \cdots + P_d$ sem perda de generalidade, então exite uma diferencial de Weil $\eta \in \Omega_F(G - D)$ distinto de zero tal que $\eta_P(1) \neq 0$ para $P \in \operatorname{supp} D'$ e $\eta_P(1) = 0$ para $P \in \operatorname{supp}(D - D')$, logo

$$(\eta) \geq G - P_1 - \cdots - P_n,$$

mas pela Observação 4.11 temos que $v_P(\eta) \geq 0$ para $P \in \operatorname{supp}(D - D')$, o que implica

$$\begin{aligned}
(\eta) &\geq G - P_1 - \cdots - P_d \\
&= G - D'.
\end{aligned}$$

Assim concluímos que $\eta \in \Omega_F(G - D')$. □

Observação 4.14. *Note que para cada palavra $0 \neq c \in C_\Omega(D,G)$ com suporte D' existe $\eta \in \Omega_F(G-D')$ diferencial de Weil diferente de zero, mas $\{0\} \neq \Omega_F(G-D') = \Omega_F(K+C-D') \cong L(D'-C)$, logo existe um divisor $E_1 \geq 0$ tal que $D' \sim C + E_1$.*

Teorema 4.15 (Cota d_{ABZ})**.** *Seja $G = K + C = A + B + Z$, onde A, B e Z são divisores tais que $Z \geq 0$ e $\operatorname{supp} D \cap \operatorname{supp} Z = \emptyset$, então*

$$d(C_\Omega(D,G)) \geq \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C).$$

Demonstração. Seja $0 \neq c = (\eta_{P_1}(1), \ldots, \eta_{P_n}(1))$ uma palavra arbitrária do código $C_\Omega(D,G)$ com suporte D', então, pelo Lema 4.13, $\eta \in \Omega_F(G-D')$. Assim $(\eta) \geq G - D'$, e existe um divisor $E \geq 0$ tal que $(\eta) = G - D' + E$ com $\operatorname{supp} D' \cap \operatorname{supp} E = \emptyset$ pela Observação 4.11. Também notemos que $D' \sim C + E_1$ com $E_1 \geq 0$ pela Observação 4.14. Além disso $\operatorname{supp} D' \cap \operatorname{supp} Z = \emptyset$ pois $\operatorname{supp} D \cap \operatorname{supp} Z = \emptyset$ por hipótese. Logo, pelo Lema 4.9 segue que

$$\begin{aligned} \deg D' &\geq \ell(A) - \ell(A-D') + \ell(B) - \ell(B-D') \\ &\geq \ell(A) - \ell(A-D'+E_1) + \ell(B) - \ell(B-D'+E_1) \\ &= \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C). \end{aligned} \tag{3}$$

Finalmente, como a palavra c foi escolhida arbitrariamente concluímos que

$$d(C_\Omega(D,G)) \geq \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C).$$

□

Note que a cota inferior do Teorema 4.15,

$$d \geq \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C), \tag{4}$$

pode ser escrita em duas formas diferentes:

$$\begin{aligned} \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C) &= i(A) + \deg A - g + 1 - i(A-C) \\ &\quad - \deg(A-C) + g - 1 + \ell(B) - \ell(B-C) \\ &= \deg C + i(A) - i(A-C) + \ell(B) - \ell(B-C) \\ &= \deg C + i(K+C-B-Z) - i(K-B-Z) \\ &\quad + \ell(B) - \ell(B-C) \\ &= \deg C + \ell(B+Z-C) - \ell(B+Z) + \ell(B) \\ &\quad - \ell(B-C). \end{aligned} \tag{5}$$

e

$$\begin{aligned}\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C) &= \deg C+\ell(B+Z-C)-\ell(B+Z)+\ell(B)\\ &\quad -\ell(B-C)\\ &= \deg C+i(B+Z-C)+\deg(B+Z-C)\\ &\quad -g+1-\ell(B+Z)+\ell(B)-i(B-C)\\ &\quad -\deg(B-C)+g-1\\ &= \deg C+i(B+Z-C)+\deg Z-\ell(B+Z)\\ &\quad +\ell(B)-i(B-C)\\ &= \deg C+\deg Z+i(K-A)-i(K-A-Z)\\ &\quad -\ell(B+Z)+\ell(B)\\ &= \deg C+\deg Z+\ell(A)-\ell(A+Z)+\ell(B)\\ &\quad -\ell(B+Z). \qquad (6)\end{aligned}$$

Esta última forma de expressar (4) tem como consequência as demais cotas tipo piso.

Observação 4.16. *É fácil observar que na equação* (5) *ao fazer* $Z=0$ *obtemos a Cota de Goppa (*d_{GOP}*).*

Agora introduziremos os conceitos e resultados básicos para obter a cota piso d_{MMP}.

Definição 4.17. *Dados os divisores* A *e* B*, definimos o máximo divisor comum entre* A *e* B *como sendo o divisor*

$$mdc(A,B)=\sum_{P\in\mathbb{P}_F}\min\{v_P(A),\,v_P(B)\}P.$$

Proposição 4.18. *Sejam* A *e* B *divisores, então*

$$L(A)\cap L(B)=L(mdc(A,B)).$$

Demonstração. Seja $x\in L(A)\cap L(B)$ e seja $P\in\mathbb{P}_F$, então temos que $v_P(x)+v_P(A)\geq 0$ e $v_P(x)+v_P(B)\geq 0$, portanto $v_P(x)+\min\{v_P(A),v_P(B)\}\geq 0$, logo $x\in L(mdc(A,B))$. Por outro lado note que $L(mdc(A,B))\subseteq L(A)$ e $L(mdc(A,B))\subseteq L(B)$, logo $L(mdc(A,B))\subseteq L(A)\cap L(B)$. □

Proposição 4.19. *Seja* A *um divisor com* $\ell(A)>0$*. Suponha que* A' *é um divisor de grau mínimo tal que* $L(A)=L(A')$*, então* $A\geq A'$*. Consequentemente,* A' *é o único divisor com esta propriedade.*

Demonstração. Temos que $L(A) = L(A) \cap L(A') = L(mdc(A, A'))$, logo pela minimalidade do grau de A' segue que $\deg A' \leq \deg mdc(A, A')$. Mas por outro lado $mdc(A, A') \leq A'$, logo $\deg A' = \deg mdc(A, A')$, o que implica $A' = mdc(A, A') \leq A$.
Suponhamos que existem A' e A'' divisores com grau mínimo tal que $L(A) = L(A') = L(A'')$. Logo temos que $L(A') = L(A'')$, pela minimalidade dos graus obtemos $A' \leq A''$ e $A'' \leq A'$ pelo anterior demonstrado, assim $A' = A''$. □

Assim, o seguinte conceito fica bem definido.

Definição 4.20. *Dado um divisor A com $l(A) > 0$, o piso de A é o único divisor A' de grau mínimo tal que $L(A) = L(A')$. Denotaremos o piso de A por $\lfloor A \rfloor$. Além disso, chamamos parte fixa do divisor A ao divisor $E_A = A - \lfloor A \rfloor$.*

Agora vejamos as demais cotas piso.

Corolário 4.21 (Cota d_{MMP})**.** *Seja $G = K + C = A + B + Z$ com $Z \geq 0$ e $supp\, D \cap supp\, Z = \emptyset$ tal que $H = A + Z = B + Z$ e $\lfloor H \rfloor = A = B$, então*

$$d(C_\Omega(D, H + \lfloor H \rfloor)) \geq deg\, C + deg\, E_H.$$

Demonstração. Note que das hipóteses temos que $Z = H - \lfloor H \rfloor$ e $\ell(A) = \ell(A + Z) = \ell(B) = \ell(B + Z)$ pois $L(H) = L(\lfloor H \rfloor)$. Logo do Teorema 4.15 e da equação (6) temos que

$$\begin{aligned} d(C_\Omega(D, H + \lfloor H \rfloor)) &\geq \deg C + \deg (H - \lfloor H \rfloor) \\ &= \deg C + \deg E_H. \end{aligned}$$

□

A seguinte cota, dada por Lundell e McCullough [9], é uma generalização da cota piso d_{MMP} e a sua vez é também uma generalização da cota básica d_{BPT}.

Corolário 4.22 (Cota d_{LM})**.** *Seja $G = K + C = A + B + Z$ com $Z \geq 0$ tal que $L(A + Z) = L(A)$, $L(B + Z) = L(B)$ e $supp\, D \cap supp\, Z = \emptyset$. Então*

$$d(C_\Omega(D, G)) \geq deg\, C + deg\, Z.$$

Demonstração. Do Teorema 4.15 e da equação (6), como $L(A+Z) = L(A)$ e $L(B+Z) = L(B)$ segue imediatamente

$$d(C_\Omega(D, G)) \geq \deg C + \deg Z.$$

□

Observação 4.23. *Note que fazendo $A = B = \lfloor H \rfloor$ e $Z = H - \lfloor H \rfloor$ obtemos a cota piso d_{MMP}. Além disso, fazendo $Z = P$, onde P é um lugar racional, obtemos a cota d_{BPT} pelo Lema 4.5.*

A cota dada por Güneri, Stichtenoth e Taşkın [8, Teorema 2.4] é uma generalização da cota d_{LM}. Apresentamos esta cota em sua forma original no seguinte resultado.

Corolário 4.24 (Cota d_{GST})**.** *Sejam $\overline{A}$, $\overline{B}$, $\overline{C}$, $\overline{Z} \in Div(F)$ satisfazendo as seguintes condições:*

i) $(supp\,\overline{A} \cup supp\,\overline{B} \cup supp\,\overline{C} \cup supp\,\overline{Z}) \cap supp\,D = \emptyset$,

ii) $L(\overline{A}) = L(\overline{A} - \overline{Z})$ *e* $L(\overline{B}) = L(\overline{B} + \overline{Z})$, *e*

iii) $L(\overline{C}) = L(\overline{B})$.

Se $G = \overline{A} + \overline{B}$, então

$$d(C_\Omega(D, G)) \geq deg\,C + deg\,\overline{Z} + i(\overline{A}) - i(G - \overline{C}).$$

Demonstração. Podemos supor que $\overline{C} \leq \overline{B} + \overline{Z}$ pois caso a desigualdade não fosse satisfeita poderíamos considerar o divisor $mdc(\overline{C}, \overline{B} + \overline{Z})$ que satisfaz $\operatorname{supp} mdc(\overline{C}, \overline{B} + \overline{Z}) \cap \operatorname{supp} D = \emptyset$, $L(mdc(\overline{C}, \overline{B} + \overline{Z})) = L(\overline{B})$ e $mdc(\overline{C}, \overline{B} + \overline{Z}) \leq \overline{B} + \overline{Z}$. Assim, existe um $\widehat{Z} \geq 0$ tal que $\overline{C} + \widehat{Z} = \overline{B} + \overline{Z}$. Escrevendo

$$G = \overline{A} + \overline{B} = (\overline{A} - \overline{Z}) + \overline{C} + \widehat{Z} = A + B + Z$$

onde $A = \overline{A} - \overline{Z}$, $B = \overline{C}$ e $Z = \widehat{Z}$ temos que $Z \geq 0$ e $\operatorname{supp} D \cap \operatorname{supp} Z = \emptyset$ por hipótese. Logo pelo Teorema 4.15 e a equação (6) temos

$$\begin{aligned} d(C_\Omega(D, G)) &\geq \deg C + \deg Z + \ell(A) - \ell(A + Z) + \ell(B) - \ell(B + Z) \\ &= \deg C + \deg Z + \ell(A) - \ell(A + Z) \\ &= \deg C + \deg \widehat{Z} + \ell(\overline{A} - \overline{Z}) - \ell(\overline{A} - \overline{Z} + \widehat{Z}) \\ &= \deg C + \deg \widehat{Z} + \ell(\overline{A}) - \ell(G - \overline{C}) \\ &= \deg C + \deg (\widehat{Z} + \overline{A} - G + \overline{C}) + i(\overline{A}) - i(G - \overline{C}) \\ &= \deg C + \deg \overline{Z} + i(\overline{A}) - i(G - \overline{C}). \end{aligned}$$

□

Observação 4.25. *Fazendo $\overline{Z} \geq 0$ e $\overline{B} = \overline{C}$ temos que $G - \overline{C} = G - \overline{B} = \overline{A}$, portanto obtemos a cota d_{LM}.*

Na cota d_{GST} devemos procurar valores ótimos para os divisores para poder garantir uma melhora na diferença $i(\overline{A}) - i(G - \overline{C})$, porém, as vezes isto não é uma tarefa fácil. No seguinte resultado notamos que fazendo $\overline{Z} = 0$ nossa melhora só vai depender da escolha de dois parâmetros, os divisores $\overline{B}$ e $\overline{C}$.

Corolário 4.26. *Seja $G = K + C = \overline{A} + \overline{B}$ e $\overline{B} = \overline{C} + \widehat{Z}$ tal que $L(\overline{B}) = L(\overline{C})$ e $\widehat{Z} \geq 0$. Para D com $supp\, D \cap supp\, \widehat{Z} = \emptyset$ temos*

$$d(C_\Omega(D, G)) \geq deg\, C + \ell(\overline{B} - C) - \ell(\overline{C} - C).$$

Demonstração. Com a decomposição $G = \overline{A} + \overline{C} + \widehat{Z} = A + B + Z$, onde $A = \overline{A}$, $B = \overline{C}$ e $Z = \widehat{Z}$ temos que $Z \geq 0$ e $\operatorname{supp} D \cap \operatorname{supp} Z = \emptyset$, logo pelo Teorema 4.15 e a equação (5) temos

$$\begin{aligned} d(C_\Omega(D, G)) &\geq \deg C + \ell(\overline{C} + \widehat{Z} - C) - \ell(\overline{C} + \widehat{Z}) + \ell(\overline{C}) - \ell(\overline{C} - C) \\ &= \deg C + \ell(\overline{B} - C) - \ell(\overline{B}) + \ell(\overline{C}) - \ell(\overline{C} - C) \\ &= \deg C + \ell(\overline{B} - C) - \ell(\overline{C} - C). \end{aligned}$$

□

O último teorema desta seção formula a cota d_{GST} em função de um só parâmetro.

Teorema 4.27 (Formulação de d_{GST} mediante um parâmetro)**.** *Seja $G = K + C$. Para um divisor B tal que $supp\, D \cap supp\, (B - \lfloor B \rfloor) = \emptyset$, temos*

$$d(C_\Omega(D, G)) \geq deg\, C + \ell(B - C) - \ell(\lfloor B \rfloor - C).$$

Demonstração. Tomando $\overline{A} = G - B$, $\overline{B} = B$, $\overline{C} = \lfloor B \rfloor$ e $\widehat{Z} = B - \lfloor B \rfloor$ temos que $G = \overline{A} + \overline{B}$, $\overline{B} = \overline{C} + \widehat{Z}$, $\widehat{Z} \geq 0$, $\operatorname{supp} D \cap \operatorname{supp} \widehat{Z} = \emptyset$ e $L(\overline{B}) = L(\overline{C})$, logo pelo Corolário 4.26 segue que

$$d(C_\Omega(D, G)) \geq \deg C + \ell(B - C) - \ell(\lfloor B \rfloor - C).$$

□

Exemplo 4.28. *Com a mesma notação na Observação 4.7, sejam P e Q dois lugares racionais do corpo de funções de Suzuki. Tomamos, para cada código, as seguintes decomposições dependendo da cota indicada:*
$C_\Omega(D, G = 32P + Q)$*:*

$$\begin{aligned} d_{LM} &: A = 18P,\ B = 13P \text{ e } Z = P + Q \\ d_{GST} &: \overline{A} = 19P + Q,\ \overline{B} = 13P,\ \overline{C} = 13P \text{ e } \overline{Z} = P + Q \\ d_{ABZ} &: A = 13P,\ B = 13P \text{ e } Z = 6P + Q \end{aligned}$$

e
$C_\Omega(D, G = 24P + 6Q)$*:*

$$\begin{aligned} d_{LM} &: A = 16P,\ B = 10P + 2Q \ e\ Z = 2Q \\ d_{GST} &: \overline{A} = 16P + 2Q,\ \overline{B} = 8P + 4Q,\ \overline{C} = 8P \ e\ \overline{Z} = 2Q \\ d_{ABZ} &: A = 16P,\ B = 8P \ e\ Z = 6Q. \end{aligned}$$

Assim, fazendo uso do Algoritmo B, obtemos os valores das cotas e as melhoras mostradas na Tabela 2.

Código	n	k	d_{LM}	d_{GST}	d_{ABZ}
$C_\Omega(D, G = 32P + Q)$	63	43	9	9	10
$C_\Omega(D, G = 24P + 6Q)$	63	46	6	7	7

Tabela 2: Cotas piso

Até agora, as cotas estudadas estão relacionadas da seguinte maneira:

$$\begin{array}{ccccccc} d_{GOP} & \longrightarrow & d_{BPT} & & & & \\ & & \downarrow & & & & \\ d_{MMP} & \longrightarrow & d_{LM} & \longrightarrow & d_{GST} & \longrightarrow & d_{ABZ} \end{array}$$

4.3 Cotas mistas

Nesta seção vamos apresentar as cotas mistas d_{GKL} [5] e d_{GST2} [8], e fornecemos também a cota d_{ABZ^+}. Estudaremos a relação entre elas e, por sua vez, a relação com as cotas estudadas anteriormente. Primeiro apresentamos a cota d_{ABZ^+} que apresenta uma melhora da cota d_{ABZ}.

Lema 4.29. *Sejam os divisores C, A e A' tais que $A' \leq A$ e:*

i) $L(A' - C) \neq L(A' - C - P)$ e $L(A') = L(A' - P)$ para algum lugar P, e

ii) $L(A - C) \neq L(A - C - Q)$, para todo lugar Q com $A' \leq A - Q \leq A$.

Então $L(A - C) \neq L(A - D')$ para qualquer divisor $D' \sim C + E$ tal que $P \notin \operatorname{supp} D'$ e $D', E \geq 0$.

Demonstração. Seja D' um divisor tal que $D' \sim C + E$ com $P \notin \operatorname{supp} D'$ e $D', E \geq 0$.
Caso 1: Se $\operatorname{supp} E \cap \operatorname{supp}(A - A') \neq \emptyset$
Pela hipótese existe $Q \in \operatorname{supp} E \cap \operatorname{supp}(A - A')$. Como $Q \in \operatorname{supp} E$ e $E \geq 0$ temos $0 \leq Q \leq E$. Por outro lado, como $Q \in \operatorname{supp}(A - A')$ e $A - A' \geq 0$ temos $0 \leq Q \leq A - A'$ o que implica $A' \leq A - Q \leq A$. Assim, pela segunda condição $L(A - C) \neq L(A - C - Q)$. Mas como temos $Q \leq E$ e $D' \sim C + E$ segue que

$$L(A - D') \cong L(A - C - E) \subseteq L(A - C - Q) \subsetneq L(A - C).$$

Caso 2: Se $\operatorname{supp} E \cap \operatorname{supp}(A - A') = \emptyset$
Definindo a aplicação

$$\varphi : \frac{L(A' - C)}{L(A' - C - E)} \longrightarrow \frac{L(A - C)}{L(A - C - E)}$$

dada por $\varphi(x + L(A' - C - E)) = x + L(A - C - E)$, temos que está bem definida e é injetiva pela Proposição 2.29, logo

$$\ell(A' - C) - \ell(A' - C - E) \leq \ell(A - C) - \ell(A - C - E),$$

mas como $D' \sim C + E$ segue que

$$\ell(A' - C) - \ell(A' - D') \leq \ell(A - C) - \ell(A - D'). \tag{7}$$

Pela primeira condição $L(A' - C) \neq L(A' - C - P)$ e $L(A') = L(A' - P)$, portanto

$$\ell(A' - C - P) < \ell(A' - C) \tag{8}$$

e $L(A' - D') = L(A' - D' - P)$, de fato, seja $x \in L(A' - D')$ então

$$(x) + A' \geq D',$$

mas como $D' \geq 0$ temos que $x \in L(A') = L(A' - P)$, e como $P \notin \operatorname{supp} D'$ segue que

$$(x) + A' \geq D' + P.$$

Deste modo temos $L(A' - D') = L(A' - D' - P)$ e portanto

$$\ell(A' - D') = \ell(A' - D' - P). \tag{9}$$

Além disso observe que

$$A' - P - D' \sim A' - P - C - E \leq A' - P - C,$$

logo

$$\ell(A' - P - D') \leq \ell(A' - P - C), \tag{10}$$

Assim de (7), (8), (9) e (10) segue que

$$\begin{aligned} \ell(A - C) - \ell(A - D') &\geq \ell(A' - C) - \ell(A' - D') \\ &> \ell(A' - C - P) - \ell(A' - P - D') \\ &\geq 0. \end{aligned}$$

□

Teorema 4.30 (Cota d_{ABZ^+})**.** *Seja $G = K+C = A+B+Z$ com $Z \geq 0$ e $\operatorname{supp} D \cap \operatorname{supp} Z = \emptyset$. Defina $\delta(A) \in \{0, 1\}$ como 1 se existe um divisor $A' \leq A$ tal que:*

i) $\operatorname{supp}(A - A') \subseteq \operatorname{supp} Z$,

ii) existe um lugar $P \in \operatorname{supp} Z$ com $L(A' - C) \neq L(A' - C - P)$ e $L(A') = L(A' - P)$, e

iii) para todo lugar $Q \in \operatorname{supp} Z$ temos $L(A - C) \neq L(A - C - Q)$,

e como 0 caso contrário. Então

$$d(C_\Omega(D, G)) \geq \ell(A) - \ell(A - C) + \ell(B) - \ell(B - C) + \delta(A) + \delta(B).$$

Demonstração. Dada uma palavra $0 \neq c \in C_\Omega(D, G)$ com suporte D' existe um divisor $E \geq 0$ tal que $D' \sim C + E$ pela Observação 4.14. Além disso concluímos que

$$\deg D' \geq \ell(A) - \ell(A - D') + \ell(B) - \ell(B - D')$$

pela equação (3). Se não existe A' que satisfaz as condições descritas então $\delta(A) = 0$. Por outro lado, se existe tal A' temos um lugar $P \in \operatorname{supp} Z$ com $L(A' - C) \neq L(A' - C - P)$ e $L(A') = L(A' - P)$. Além disso, para um lugar Q tal que $A' \leq A - Q \leq A$ temos $0 \leq Q \leq A - A'$, ou seja, $Q \in \operatorname{supp}(A - A') \subseteq \operatorname{supp} Z$, portanto $L(A - C) \neq L(A - C - Q)$. Também note que como $\operatorname{supp} D' \cap \operatorname{supp} Z = \emptyset$ e $P \in \operatorname{supp} Z$ então $P \notin \operatorname{supp} D'$. Assim, do Lema 4.29 temos $L(A - C) \neq L(A - D')$, o que implica $1 = \delta(A) \leq \ell(A - C) - \ell(A - D')$, ou seja, $\ell(A) - \ell(A - C) + \delta(A) \leq \ell(A) - \ell(A - D')$.
De maneira análoga obtemos $\ell(B) - \ell(B - C) + \delta(B) \leq l(B) - \ell(B - D')$, portanto

$$\deg D' \geq \ell(A) - \ell(A - C) + \delta(A) + \ell(B) - \ell(B - C) + \delta(B).$$

Mas como a palavra c foi escolhida arbitrariamente temos que

$$d(C_\Omega(D, G)) \geq \ell(A) - \ell(A - C) + \ell(B) - \ell(B - C) + \delta(A) + \delta(B).$$

□

Observação 4.31. *Notemos que a cota d_{ABZ^+} é uma melhora de até duas unidades com respeito à cota d_{ABZ}.*

Os autores Güneri, Stichtenoth e Taşkın [8, Teorema 2.12] também fornecem a cota d_{GST2} que é uma melhora da cota d_{LM} que, por sua vez, é uma generalização da cota d_{GKL} dada por Garcia, Kim e Lax [5] que será apresentada mais tarde.

Corolário 4.32 (Cota d_{GST2})**.** *Seja $G = K+C$ e suponha que existem divisores $\overline{A}$, $\overline{B}$, $\overline{Z} \in Div(F)$ satisfazendo as seguintes condições:*

i) $(supp\,\overline{A} \cup supp\,\overline{B} \cup supp\,\overline{Z}) \cap supp\,D = \emptyset$,

ii) $supp\,(\overline{A} - \overline{B}) \subseteq supp\,\overline{Z}$,

iii) $\overline{Z} \geq 0$, $L(\overline{A}) = L(\overline{A} - \overline{Z})$ *e* $L(\overline{B}) = L(\overline{B} + \overline{Z} + Q)$ *para todo* $Q \in supp\,\overline{Z}$, *e*

iv) $\overline{B} + \overline{Z} + P \leq \overline{A}$ *para algum* $P \in supp\,\overline{Z}$.

Se $G = \overline{A} + \overline{B}$, então temos

$$d(C_\Omega(D,G)) \geq deg\,C + deg\,\overline{Z} + 1.$$

Demonstração. Fazendo $A = \overline{A} - \overline{Z}$, $B = \overline{B}$, $A' = B + P$ e $Z = \overline{Z}$ temos $G = K + C = \overline{A} + \overline{B} = A + B + Z$. Vejamos que são satisfeitas as condições do Teorema 4.30, de fato, temos $A' = B + P = \overline{B} + P \leq \overline{A} - \overline{Z} = A$. Além disso $A - A' = \overline{A} - \overline{B} - \overline{Z} - P$, como $\operatorname{supp}(\overline{A} - \overline{B}) \subseteq \operatorname{supp}\overline{Z}$ e $P \in \operatorname{supp}\overline{Z}$ temos $\operatorname{supp}(A - A') \subseteq \operatorname{supp}\overline{Z} = \operatorname{supp} Z$.
Por outro lado temos que $L(\overline{A}) = L(\overline{A} - P)$, pois $L(\overline{A}) = L(\overline{A} - \overline{Z}) \subseteq L(\overline{A} - P) \subseteq L(\overline{A})$.
Além disso, por hipótese temos $L(A + Z) = L(A)$.
Sabemos também que

$$\begin{aligned}\ell(A' - C) = \ell(B + P - C) = \ell(K - A - Z + P) = i(A + Z - P) = i(\overline{A} - P)\\ = \ell(\overline{A} - P) - \deg\overline{A} + \deg P + g - 1\end{aligned}$$

e

$$\begin{aligned}\ell(A' - C - P) = \ell(B - C) = \ell(K - A - Z) = i(A + Z) = i(\overline{A})\\ = \ell(\overline{A}) - \deg\overline{A} + g - 1,\end{aligned}$$

logo como $L(\overline{A}) = L(\overline{A} - P)$ temos $L(A' - C) \neq L(A' - C - P)$.
Note que $L(\overline{B}) \subseteq L(\overline{B} + P) \subseteq L(\overline{B} + \overline{Z} + Q) = L(\overline{B})$ para todo $Q \in \operatorname{supp}\overline{Z}$, disto segue que $L(B + P) = L(B)$, ou seja, $L(A' - P) = L(A')$.

Observamos também que para todo $Q \in \operatorname{supp} Z$ temos $L(\overline{B}+\overline{Z}) \subsetneq L(\overline{B}+\overline{Z}+Q) = L(\overline{B}) \subsetneq L(\overline{B}+\overline{Z})$, logo $L(B+Z) = L(B)$ e $L(\overline{B}+\overline{Z}) = L(\overline{B}+\overline{Z}+Q)$ para todo $Q \in \operatorname{supp} Z$. Além disso

$$\ell(A-C) = \ell(K-\overline{B}-\overline{Z}) = i(\overline{B}+\overline{Z}) = \ell(\overline{B}+\overline{Z}) - \deg(\overline{B}+\overline{Z}) + g - 1$$

e

$$\begin{aligned}\ell(A-C-Q) &= \ell(K-\overline{B}-\overline{Z}-Q) = i(\overline{B}+\overline{Z}+Q) \\ &= \ell(\overline{B}+\overline{Z}+Q) - \deg(\overline{B}+\overline{Z}) - \deg Q + g - 1,\end{aligned}$$

mas como $L(\overline{B}+\overline{Z}) = L(\overline{B}+\overline{Z}+Q)$ segue que $L(A-C) \neq L(A-C-Q)$ para todo $Q \in \operatorname{supp} Z$.
Logo dado uma palavra $0 \neq c \in C_\Omega(D,G)$ com suporte D', do Lema 4.13 e a Observação 4.14 existe um divisor $E \geq 0$ tal que $D' \sim C + E$ e por hipótese $\operatorname{supp} D' \cap \operatorname{supp} Z = \emptyset$. Além disso tínhamos que $L(A+Z) = L(A)$ e $L(B+Z) = L(B)$, logo

$$\begin{aligned}\deg D' &\geq \ell(A) - \ell(A-C) + \ell(B) - \ell(B-C) + 1 && \text{do Teorema 4.30} \\ &= \deg C + \deg \overline{Z} + \ell(A) - \ell(A+\overline{Z}) + \ell(B) - \ell(B+\overline{Z}) + 1 && \text{da equação (6)} \\ &= \deg C + \deg \overline{Z} + 1.\end{aligned}$$

Como c foi uma palavra escolhida arbitrariamente temos

$$d(C_\Omega(D,G)) \geq \deg C + \deg \overline{Z} + 1.$$

□

Assim obtemos, adicionando hipóteses a mais, uma melhora de uma unidade para a cota d_{LM}. A seguir, apresentamos a cota d_{GKL}.

Corolário 4.33 (Cota d_{GKL})**.** *Seja H um divisor e P um lugar racional tal que, para certos inteiros α, β, t com $\beta \geq \alpha + t$ e $t \geq 1$, temos*

$$L(H+\alpha P+tP) = L(H+\alpha P-P) \quad e \quad L(H+\beta P) = L(H+\beta P-tP).$$

Se $(\operatorname{supp} H \cup \{P\}) \cap \operatorname{supp} D = \emptyset$, então para $G = 2H + (\alpha+\beta-1)P$ temos

$$d(C_\Omega(D,G)) \geq \deg C + t + 1.$$

Demonstração. Fazendo $\overline{A} = \beta P + H$, $\overline{B} = (\alpha-1)P + H$ e $\overline{Z} = tP$ temos que todas as hipóteses do Corolário 4.32 são satisfeitas, logo

$$d(C_\Omega(D,G)) \geq \deg C + t + 1.$$

□

Exemplo 4.34. *Com a mesma notação na Observação 4.7, sejam P e Q dois lugares racionais do corpo de de funções de Suzuki. Tomamos, para cada código, as seguintes decomposições dependendo da cota indicada:*
$C_\Omega(D, G = 32P + Q)$:

$$d_{GST2} : \overline{A} = 19P + Q,\ \overline{B} = 13P \text{ e } \overline{Z} = P + Q$$
$$d_{ABZ^+} : A = 13P,\ B = 13P \text{ e } Z = 6P + Q$$

e
$C_\Omega(D, G = 27P)$:

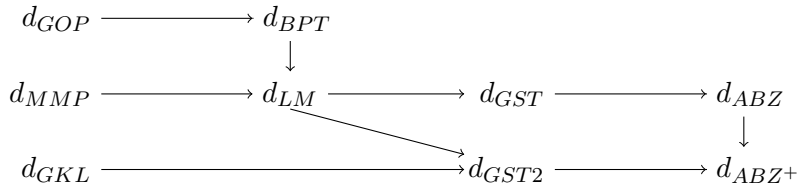
$$d_{GST2} : \overline{A} = 27P,\ \overline{B} = 0 \text{ e } \overline{Z} = P$$
$$d_{ABZ^+} : A = 13P,\ B = 13P,\ Z = 6P,\ A' = 9P \text{ e } B' = 11P.$$

Assim, fazendo uso do Algoritmo C, obtemos os valores das cotas e suas melhoras mostradas na Tabela 3.

Código	n	k	d_{GST2}	d_{ABZ^+}
$C_\Omega(D, G = 32P + Q)$	63	43	10	10
$C_\Omega(D, G = 27P)$	64	50	3	4

Tabela 3: Cotas mistas

Como as cotas d_{GST}, d_{GST2} não são comparáveis em geral (ver [3, Tabela 1]), o fornecimento da cota d_{ABZ^+} estabelece uma hierarquia das cotas mistas sobre as cotas piso. Isto pode-se ver no seguinte diagrama onde resumimos a relação entre as cotas estudadas neste trabalho até o momento.



4.4 As Cotas ordem d_B e $d_{ABZ'}$

Nesta seção daremos inicio ao estudo das cotas ordem. Para começar, somente apresentaremos duas cotas, as quais são obtidas usando as ferramentas fornecidas até agora. As demais cotas ordem serão apresentadas nas seguintes seções fazendo uso de novas ferramentas.

Definição 4.35. *Sejam C um divisor e P um lugar racional (ambos fixos), para um divisor A definimos o conjunto $\Delta'(A)$ como*

$$\Delta'(A) := \{A_i = A - iP : i \geq 0,\ L(A_i) = L(A_i - P) \text{ e } L(A_i - C) \neq L(A_i - C - P)\}.$$

Observação 4.36. *Note que o conjunto $\Delta'(A)$ é sempre finito, de fato, só basta observar que $i \notin \Delta'(A)$ para $i > \deg A - \deg C$.*

Agora apresentamos a cota ordem dada por Duursma e Park [4, Teorema 6.5].

Teorema 4.37 (Cota $d_{ABZ'}$)**.** *Seja $G = K + C = A + B + Z$ com $Z \geq 0$ e $\operatorname{supp} Z \cap \operatorname{supp} D = \emptyset$. Para um lugar racional P tal que $P \notin \operatorname{supp} D$ temos*

$$d(C_\Omega(D, G)) \geq \min\{d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|,\ d(C_\Omega(D, G + P))\}.$$

Demonstração. Seja $0 \neq c \in C_\Omega(D, G)$ uma palavra com suporte D', pela Observação 4.14 existe um divisor $E \geq 0$ tal que $D' \sim C + E$. Seguindo a demonstração do Teorema 4.15 obtemos

$$\deg D' \geq \ell(A) - \ell(A - D') + \ell(B) - \ell(B - D').$$

Caso 1: Se $P \notin \operatorname{supp} E$
Seja $A_i \in \Delta'(A)$, logo $L(A_i) = L(A_i - P)$ e $L(A_i - C) \neq L(A_i - C - P)$. Note que $L(A_i - D') = L(A_i - D' - P)$, de fato, seja $x \in L(A_i - D')$, então temos

$$(x) + A_i \geq D',$$

mas como $P \notin \operatorname{supp} D'$ e $x \in L(A_i - P)$, pois $L(A_i - D') \subseteq L(A_i) = L(A_i - P)$, segue que

$$(x) + A_i \geq D' + P,$$

ou seja $L(A_i - D') = L(A_i - D' - P)$. Por outro lado como $L(A_i - C) \neq L(A_i - C - P)$, temos que $\ell(A_i - C - P) + 1 = \ell(A_i - C)$, assim

$$\ell(A_i - C) - \ell(A_i - D') = \ell(A_i - C - P) - \ell(A_i - D' - P) + 1. \tag{11}$$

Notemos também que para qualquer divisor A_i podemos definir a aplicação linear

$$\varphi : \frac{L(A_i - C - P)}{L(A_i - C - E - P)} \longrightarrow \frac{L(A_i - C)}{L(A_i - C - E)}$$

dada por $\varphi(x + L(A_i - C - E - P)) = x + L(A_i - C - E)$ a qual esta bem definida e é injetiva pela Proposição 2.29, logo temos

$$\ell(A_i - C - P) - \ell(A_i - C - E - P) \leq \ell(A_i - C) - \ell(A_i - C - E)$$

o qual é o mesmo que

$$\ell(A_i - C - P) - \ell(A_i - D' - P) \leq \ell(A_i - C) - \ell(A_i - D') \tag{12}$$

pois temos que $D' \sim C + E$. Pelo terceiro item da Proposição 2.25 temos

$$\ell(A-C) - \ell(A-D') = \sum_{i \geq 0} [(\ell(A_i - C) - \ell(A_i - D')) - (\ell(A_i - C - P) - \ell(A_i - D' - P))],$$

onde $A_i = A - iP$, e pelas equações (11) e (12) segue que

$$\ell(A-C) - \ell(A-D') \geq |\Delta'(A)|.$$

Analogamente temos que

$$\ell(B-C) - \ell(B-D') \geq |\Delta'(B)|.$$

Portanto

$$\begin{aligned} \deg D' &\geq \ell(A) - \ell(A-C) + |\Delta'(A)| + \ell(B) - \ell(B-C) + |\Delta'(B)| \\ &= d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|, \end{aligned}$$

e como a palavra c é arbitraria segue que

$$d(C_\Omega(D,G)) \geq d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|.$$

Caso 2: Se $P \in \operatorname{supp} E$
Para este caso conclui-se $d(C_\Omega(D,G)) = d(C_\Omega(D, G+P))$. Assim temos

$$d(C_\Omega(D,G)) \geq \min\{d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G+P))\}.$$

□

Observação 4.38. *Adicionando hipóteses a mais no Teorema 4.30 obtemos* $d_{ABZ^+} \leq d_{ABZ'}$.

Exemplo 4.39. *Com a mesma notação na Observação 4.7, vamos calcular a cota* $d_{ABZ'}$ *para o código* $C_\Omega(D, G = 27P + Q)$ *para certa decomposição de* G. *Sejam* P *e* Q *lugares racionais distintos do corpo de funções de Suzuki. Para calcular a cota* d_{ABZ} *tomamos a decomposição* $A = 13P$, $B = 13P$ *e* $Z = P + Q$, *e fazendo uso do Algoritmo B obtemos*

$d_{ABZ} = 4$. *Para calcular a cota* $d_{ABZ'}$ *devemos calcular primeiro os conjuntos* $\Delta'(A)$ *e* $\Delta'(B)$. *Tomando* Q *como um lugar racional tal que* $Q \notin supp\, D$ *obtemos que*

$$\Delta'(A) = \{A - 2Q,\, A - 4Q\} \qquad e \qquad \Delta'(B) = \{B - 2Q,\, B - 4Q\}.$$

Portanto temos

$$d_{ABZ'} = \min\{4 + 2 + 2,\, d(C_\Omega(D, 27P + 2Q))\} = \min\{8,\, d(C_\Omega(D, 27P + 2Q))\}, \quad (13)$$

mas nós não conhecemos o valor de $d(C_\Omega(D, 27P+2Q))$, *e também é importante dizer que é complicado achar seu valor mediante métodos computacionais, mas podemos fazer uma estimativa desta. Para o código* $C_\Omega(D, 27P + 2Q)$, *tomamos a decomposição* $A = 13P$, $B = 13P$ *e* $Z = P + 2Q$. *Para esta decomposição temos que* $d_{ABZ} = 6$ *e tomando* P *como lugar racional tal que* $P \notin supp\, D$ *obtemos*

$$\Delta'(A) = \{A - 2P\} \qquad e \qquad \Delta'(B) = \{B - 2P\},$$

logo

$$d(C_\Omega(D, 27P + 2Q)) \geq d_{ABZ'} = \min\{8,\, d(C_\Omega(D, 28P + 2Q)\}. \quad (14)$$

Finalmente estimamos o valor de $d(C_\Omega(D, 28P + 2Q))$, *para isto consideramos a decomposição* $A = 13P$, $B = 13P$ *e* $Z = 2P + 2Q$ *obtendo* $d_{ABZ} = 8$, *assim*

$$d(C_\Omega(D, 28P + 2Q)) \geq 8. \quad (15)$$

Logo de (13), (14) *e* (15) *temos que para o código* $C_\Omega(D, 27P + Q)$ *a cota* $d_{ABZ'}$ *é* 8 *para a decomposição dada.*

A seguinte cota é dada por Beelen [1] e pode ser vista como um caso particular da cota $d_{ABZ'}$.

Corolário 4.40 (Cota d_B)**.** *Seja* $G = K + C = A + B$. *Para um lugar racional* P *tal que* $P \notin supp\, D$ *temos*

$$d(C_\Omega(D, G)) \geq \min\{d_{GOP} + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G + P))\}.$$

Demonstração. Considerando $Z = 0$, temos que $d_{ABZ} = d_{GOP}$ pela Observação 4.16. Logo pelo Teorema 4.37 segue que

$$d(C_\Omega(D, G)) \geq \min\{d_{GOP} + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G + P))\}.$$

□

Agora vejamos que a cota d_{GKL} é um caso particular da cota d_B.

Corolário 4.41. *Seja H um divisor e P um lugar racional tal que, para inteiros α, β, t com $\beta \geq \alpha + t$ e $t \geq 1$, temos*

$$L(H + \alpha P + tP) = L(H + \alpha P - P) \quad e \quad L(H + \beta P) = L(H + \beta P - tP).$$

Se $(supp\, H \cup \{P\}) \cap supp\, D = \emptyset$, então para $G = 2H + (\alpha + \beta - 1)P$ temos

$$d(C_\Omega(D, G)) \geq deg\, C + t + 1.$$

Demonstração. Para $0 \leq i \leq t$ fixo, sejam $A = H + \alpha P + iP - P$ e $B = H + \beta P$. Assim temos que $G + iP = A + B$, logo pelo Corolário 4.40 segue que

$$d(C_\Omega(D, G + iP)) \geq \min\{\deg C + i + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G + iP + P))\}.$$

Vejamos que os divisores

$$H + \alpha P + iP,\, H + \alpha P + (i+1)P, \ldots,\, H + \alpha P + (t-1)P \text{ e } H + \beta P$$

estão em $\Delta'(B)$, de fato, para j com $i \leq j \leq t - 1$ e $i \neq t$ temos que $H + \alpha P + jP = B - (\beta - \alpha - j)P$ onde $\beta - \alpha - j \geq 0$ pois $j \leq t - 1$. Por outro lado

$$L(H + \alpha P - P) \subseteq L(H + \alpha P) \subseteq L(H + \alpha P + P) \subseteq \cdots \subseteq L(H + \alpha P + tP),$$

logo da hipótese $L(H + \alpha P - P) = L(H + \alpha P + tP)$ segue que $L(H + \alpha P + jP) = L(H + \alpha P + jP - P)$ para $i \leq j \leq t - 1$.
De modo análogo temos que $L(H + \beta P + (i - j)P) = L(H + \beta P + (i - j - 1)P)$ para j tal que $i \leq j \leq t - 1$, mas

$$H + \beta P + (i - j)P = G - H + (i + 1 - \alpha - j)P,$$

assim $L(G - H + (i - j - \alpha)P) = L(G - H + (i + 1 - \alpha - j)P)$ e da Proposição 2.47 segue que

$$L(K - G + H - (i - j - \alpha)P) \neq L(K - G + H - (i + 1 - \alpha - j)P)$$

ou equivalentemente

$$L(H + \alpha P + jP - \overline{C}) \neq L(H + \alpha P + jP - \overline{C} - P),$$

onde $\overline{C}$ é o suporte minimo do código $C_\Omega(D, G + iP)$. Além disso é fácil ver que $H + \beta P$ está em $\Delta'(B)$, pois a demonstração é totalmente análoga. Portanto $|\Delta'(B)| \geq t - i + 1$, assim

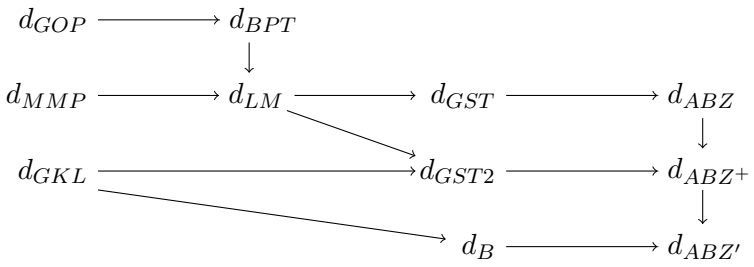
$$\begin{aligned} d(C_\Omega(D, G + iP)) &\geq \min\{\deg C + i + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G + iP + P))\} \\ &\geq \min\{\deg C + t + 1,\, d(C_\Omega(D, G + iP + P))\}. \end{aligned}$$

para todo i tal que $0 \leq i \leq t$. Logo

$$\begin{aligned} d(C_\Omega(D,G)) &\geq \min\{\deg C + t + 1,\, d(C_\Omega(D, G+P))\} \\ &\geq \min\{\deg C + t + 1,\, d(C_\Omega(D, G+2P))\} \\ &\quad \vdots \\ &\geq \min\{\deg C + t + 1,\, d(C_\Omega(D, G+tP+P))\} \\ &\geq \deg C + t + 1, \end{aligned}$$

pois $d(C_\Omega(D, G+tP+P)) \geq \deg C+t+1$ pela cota de Goppa para $C_\Omega(D, G+tP+P)$. $\square$

No seguinte diagrama resumimos a relação entre as cotas estudadas neste trabalho até o momento.



Do diagrama vemos que existe uma hierarquia entre as cotas básicas, as cotas piso, as cotas mistas e as cotas ordem, sendo estas últimas as mais ótimas até agora.

5 Semigrupos livres de pontos de base

Nesta seção introduzimos novas ferramentas para desenvolver as cotas ordem. Sendo $Pic(F) = Div(F)/\sim$, onde $\sim$ é a relação de equivalência da Definição 2.19, definimos o conjunto $\Gamma = \{A \in Pic(F) : L(A) \neq 0\}$ e observamos que tem estrutura de semigrupo, de fato, se A e B são elementos de Γ, então existe um divisor efetivo N representante de B, logo $0 \neq L(A) \subseteq L(A+N) = L(A+B)$, portanto $A+B \in \Gamma$. Agora, pela Proposição 2.30, podemos definir o seguinte semigrupo:

Definição 5.1. *Seja P um lugar racional, definimos o semigrupo Γ_P como*

$$\Gamma_P = \{A \in \Gamma : L(A) \neq L(A-P)\}.$$

Note que o semigrupo Γ_P é composto por todos os elementos $A \in \Gamma$ que não tem como ponto de base ao lugar racional P, ou, em outras palavras, os elementos $A \in \Gamma$ que estão livres de ter a P como ponto de base. Este conceito pode ser generalizado, tomando um conjunto finito S de lugares racionais podemos definir $\Gamma_S = \bigcap_{P \in S} \Gamma_P$, e por convenção denotamos $\Gamma_\emptyset = \Gamma$.

Definição 5.2. *Para um elemento $C \in Pic(F)$ e para conjuntos finitos de lugares racionais S e S' definimos*

$$\Gamma(C; S, S') = \{A : A \in \Gamma_S \ \ e \ \ A - C \in \Gamma_{S'}\},$$

$$\gamma(C; S, S') = \min\{\deg A : A \in \Gamma(C; S, S')\}.$$

Os seguintes resultados são fundamentais, pois expressaremos as cotas ordem em função de semigrupos.

Lema 5.3. *Dado um conjunto finito S de lugares racionais e um divisor $D = P_1 + \cdots + P_n$ tal que $P_i \notin S$ para $i = 1, \ldots, n$, temos*

$$d(C_\Omega(D, G)) \geq \gamma(G - K; S, \emptyset).$$

Além disso, para um lugar racional $P \notin supp\, D$ temos

$$\min wt\,(C_\Omega(D, G) \backslash C_\Omega(D, G + P)) \geq \gamma(G - K; S, P).$$

Demonstração. Ver [4, Lemas 4.2 e 4.3]. □

Proposição 5.4. *Sejam S e S' conjuntos finitos de pontos racionais e seja $C \in Pic(F)$. Para um lugar racional P tal que $P \notin S'$,*

$$\Gamma(C; S, S') = \Gamma(C; S, S' \cup \{P\}) \cup \Gamma(C + P; S, S').$$

Demonstração. Seja $A \in \Gamma(C; S, S')$, logo $A \in \Gamma_S$ e $A - C \in \Gamma_{S'}$. Para $P \notin S'$ há duas possibilidades, se $L(A - C) \neq L(A - C - P)$ então $A - C \in \Gamma_{S' \cup \{P\}}$, portanto $A \in \Gamma(C; S, S' \cup \{P\})$. Por outro lado se $L(A - C) = L(A - C - P)$ e $S' = \emptyset$ segue imediatamente que $A \in \Gamma(C + P; S, S')$, e se $S' \neq \emptyset$ temos que para qualquer $N \in S'$ tem-se $L(A - C - N) \neq L(A - C)$ pois $A - C \in \Gamma_{S'}$, logo

$$L(A - C - P - N) \subseteq L(A - C - N) \subsetneq L(A - C) = L(A - C - P),$$

assim $L(A - C - P - N) \neq L(A - C - P)$ para todo $N \in S'$, portanto $A \in \Gamma(C + P; S, S')$.

Por outro lado, é evidente que $\Gamma(C; S, S' \cup \{P\}) \subseteq \Gamma(C; S, S')$. Como $P \notin S'$ então $P \in \Gamma_{S'}$, de fato, se $S' = \emptyset$ é trivial, se $P \notin \Gamma_{S'}$ e $S' \neq \emptyset$ então existe um lugar racional $N \in S'$ tal que é ponto de base de P, isto é $\mathbb{F}_q = L(0) = L(P) = L(P - N)$. Isto só acontece se $P = N \in S'$. Logo segue que $P \in \Gamma_{S'}$. Agora, se $A \in \Gamma(C + P; S, S')$ temos $A - C - P \in \Gamma_{S'}$, logo pela propriedade de semigrupo segue que $A - C \in \Gamma_{S'}$, assim $A \in \Gamma(C; S, S')$. □

Teorema 5.5. *Seja $C \in Pic(F)$ e sejam S, S', T e T' conjuntos finitos de lugares racionais tais que T e T' são disjuntos e $T \cup T' = S'$, então*

$$\Gamma(C; S, T') = \bigcup_{\lambda \in \Lambda} \Gamma(C + \lambda; S, S'),$$

onde Λ é o semigrupo gerado pelos lugares em T (incluindo o divisor zero).

Demonstração. Se $T = \emptyset$ é trivial. Primeiro provaremos o teorema para o caso $T = \{P\}$. Seja $j \geq 0$ arbitrário, então temos que

$$\Gamma(C; S, T') = \bigcup_{0 \leq i \leq j} \Gamma(C + iP; S, T' \cup \{P\}) \cup \Gamma(C + jP + P; S, T'), \tag{16}$$

de fato, como $P \notin T'$ e pela Proposição 5.4 temos

$$\Gamma(C; S, T') = \Gamma(C; S, T' \cup \{P\}) \cup \Gamma(C + P; S, T'),$$

mas podemos fazer o mesmo com o segundo membro, assim teríamos

$$\Gamma(C + P; S, T') = \Gamma(C + P; S, T' \cup \{P\}) \cup \Gamma(C + 2P; S, T').$$

Fazendo o mesmo procedimento até o término j temos

$$\Gamma(C; S, T') = \bigcup_{0 \leq i \leq j} \Gamma(C + iP; S, T' \cup \{P\}) \cup \Gamma(C + jP + P; S, T').$$

Por um lado note que

$$\bigcup_{0 \leq i} \Gamma(C + iP; S, T' \cup \{P\}) \subseteq \Gamma(C; S, T').$$

Agora, se $A \in \Gamma(C; S, T')$ podemos escolher um $j \geq 0$ tal que $\deg A - \deg C \leq j$, assim $\deg(A - C - jP - P) < 0$ e portanto $A \notin \Gamma(C + jP + P; S, T')$, logo de (16) temos que $A \in \Gamma(C + iP; S, T' \cup \{P\})$ para algum i com $0 \leq i \leq j$, o que implica que

$$\Gamma(C; S, T') = \bigcup_{0 \leq i} \Gamma(C + iP; S, T' \cup \{P\}).$$

Para o caso geral suponhamos que $T = \{T_1, T_2, \ldots, T_m\}$, logo teríamos

$$\begin{aligned}
\bigcup_{\lambda\in\Lambda} \Gamma(C+\lambda; S, S') &= \bigcup_{0\leq i_1} \cdots \bigcup_{0\leq i_m} \Gamma(C + i_1T_1 + \cdots + i_mT_m; S, T' \cup \{T_1, \ldots, T_m\}) \\
&= \bigcup_{0\leq i_1} \cdots \bigcup_{0\leq i_{m-1}} \Gamma(C + i_1T_1 + \cdots + i_{m-1}T_{m-1}; S, T' \cup \{T_1, \ldots, T_{m-1}\}) \\
&\quad \vdots \\
&= \bigcup_{0\leq i_1} \Gamma(C + i_1T_1; S, T' \cup \{T_1\}) \\
&= \Gamma(C; S, T').
\end{aligned}$$

□

6 Teorema Principal

Na seção anterior vimos que a distância mínima do código $C_\Omega(D, G)$ está limitada inferiormente pelo valor $\gamma(G - K; S, \emptyset)$. Em geral, a distância mínima de um código poderá ser limitada inferiormente por valores da forma $\gamma(C; S, S')$ (será visto na seguinte seção); portanto, para obter cotas inferiores para a distância mínima basta obter cotas inferiores para $\gamma(C; S, S')$. Nesta seção abordaremos este problema, dando um teorema que nos permita estimar cotas inferiores para $\gamma(C; S, S')$.

Teorema 6.1. *Dado um divisor C, conjuntos finitos de lugares racionais S e S' e uma sequência de divisores $\{A_0, A_1, \ldots, A_n\}$ tal que $A_i = A_{i-1} + P_i$ para $i = 1, \ldots, n$ onde os P_i são pontos racionais. Definimos os conjuntos $\Delta, \Delta', I, I' \subseteq \{1, 2, \ldots, n\}$ como segue*

$$\Delta = \{i : A_i \in \Gamma_{P_i} \text{ e } A_i - C \notin \Gamma_{P_i}\}, \qquad I = \{i : P_i \in S\},$$

$$\Delta' = \{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - C \in \Gamma_{P_i}\}, \qquad I' = \{i : P_i \in S'\}.$$

Então $\gamma(C; S, S') \geq |\Delta \cap I'| + |\Delta' \cap I| - |\Delta'|$. Em particular, $\gamma(C; S, S') \geq |\Delta|$ para $\Delta \subseteq I'$ e $\Delta' \subseteq I$.

Demonstração. Seja D um divisor arbitrário de Γ, então

$$\begin{aligned}
\deg D &\geq \ell(A_n) - \ell(A_n - D) \\
&\geq \ell(A_n) - \ell(A_n - D) - (\ell(A_0) - \ell(A_0 - D)) \\
&= (\ell(A_n) - \ell(A_0)) - (\ell(A_n - D) - \ell(A_0 - D)) \\
&= \sum_{i=1}^{n}(\ell(A_i) - \ell(A_{i-1})) - \sum_{i=1}^{n}(\ell(A_i - D) - \ell(A_{i-1} - D)) \\
&= \sum_{i=1}^{n}(\ell(A_i) - \ell(A_i - P_i)) - \sum_{i=1}^{n}(\ell(A_i - D) - \ell(A_i - D - P_i)) \\
&= \sum_{i=1}^{n}[(\ell(A_i) - \ell(A_i - P_i)) - (\ell(A_i - D) - \ell(A_i - D - P_i))] \\
&= |\{i : A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i}\}| - |\{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i}\}|. \quad (17)
\end{aligned}$$

Tomando $D \in \Gamma(C; S, S')$ com grau mínimo temos

$$\Delta \cap I' \subseteq \{i : A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i}\}$$

e

$$\{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i}\} \subseteq \Delta' \backslash I,$$

de fato, se $i \in I'$ segue que $P_i \in S'$ e portanto $D \in \Gamma(C; S, S') \subseteq \Gamma(C; S, P_i)$; logo $D - C \in \Gamma_{P_i}$. Assim se $i \in \Delta \cap I'$ implica que

$$\begin{aligned}
i \in \Delta \cap I' &\Rightarrow D - C \in \Gamma_{P_i},\ A_i \in \Gamma_{P_i} \text{ e } A_i - C \notin \Gamma_{P_i} \\
&\Rightarrow A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i} \\
&\Rightarrow i \in \{i : A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i}\}.
\end{aligned}$$

Disto segue que

$$\Delta \cap I' \subseteq \{i : A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i}\},$$

e portanto

$$|\Delta \cap I'| \leq |\{i : A_i \in \Gamma_{P_i} \text{ e } A_i - D \notin \Gamma_{P_i}\}|. \quad (18)$$

Por outro lado suponhamos primeiro que D e $D - C$ tenham um ponto de base P em comum, isto é

$$L(D - P) = L(D) \qquad \text{e} \qquad L(D - C - P) = L(D - C). \quad (19)$$

Notemos que se $P \in S$ então $D \in \Gamma_S \subseteq \Gamma_P$, logo $L(D-P) \neq L(D)$ o qual é uma contradição com (19); portanto $P \notin S$. Se $P \in S'$ então $D \in \Gamma(C; S, S') \subseteq \Gamma(C; S, P)$, o que implica $L(D-C-P) \neq L(D-C)$, contradição com (19); portanto $P \notin S'$, obtendo assim que $P \notin S \cup S'$. Além disso, note que $D \in \Gamma(0; S, S)$ trivialmente, logo como $P \notin S$ e pela Proposição 5.4 temos que $D \in \Gamma(P; S, S)$, é dizer $D - P \in \Gamma_S$. Analogamente se demonstra que $D-C-P \in \Gamma_{S'}$, portanto teríamos $D-P \in \Gamma(C, S, S')$ o qual contradisse a minimalidade do grau do D, isto implica que D e $D-C$ não podem ter um mesmo ponto de base, o que é o mesmo dizer que se $D \notin \Gamma_P$ então $D - C \in \Gamma_P$ para todo ponto racional P. Agora, tomando $i \in \{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i}\}$ temos

$$\begin{aligned} A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i} &\Rightarrow A_i \notin \Gamma_{P_i},\ A_i - D \in \Gamma_{P_i} \text{ e } D \notin \Gamma_{P_i} \\ &\Rightarrow A_i \notin \Gamma_{P_i},\ A_i - D \in \Gamma_{P_i},\ D \notin \Gamma_{P_i} \text{ e } D - C \in \Gamma_{P_i} \\ &\Rightarrow A_i \notin \Gamma_{P_i},\ A_i - C \in \Gamma_{P_i} \text{ e } P_i \notin S \\ &\Rightarrow i \in \Delta' \backslash I. \end{aligned}$$

Assim temos

$$\{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i}\} \subseteq \Delta' \backslash I,$$

e portanto

$$|\{i : A_i \notin \Gamma_{P_i} \text{ e } A_i - D \in \Gamma_{P_i}\}| \leq |\Delta' \backslash I| = |\Delta'| - |\Delta' \cap I|. \tag{20}$$

Logo, de (17), (18) e (20) obtemos

$$\gamma(C; S, S') \geq |\Delta \cap I'| + |\Delta' \cap I| - |\Delta'|.$$

Claramente se $\Delta \subseteq I'$ e $\Delta' \subseteq I$ implica que

$$\gamma(C; S, S') \geq |\Delta|.$$

□

Considerando as notações da Observação 4.7, temos os seguintes exemplos:

Exemplo 6.2. *Tomando dois lugares racionais diferentes P e Q no corpo de funções de Suzuki, definimos o divisor $C = -3P + 6Q$. Além disso definimos nossa sequência de divisores $A_i = iP$ e tomamos $S = S' = \{P\}$. Note que ao dar a sequencia de divisores $\{A_i\}$ estamos dando também os lugares racionais P_i, neste caso $P_i = P$ para todo i. Logo, é fácil ver que $\Delta \subseteq I'$ e $\Delta' \subseteq I$ sem calcular ainda os conjuntos Δ e Δ', portanto temos $\gamma(C; P, P) \geq |\Delta|$. Ao calcular o conjunto Δ, com o Algoritmo D, obtemos*

$$\Delta = \{0, 8, 12, 13, 16, 24\}.$$

Assim temos que $\gamma(C;P,P) \geq 6$. Se trabalhamos com a sequência $A_i = iP + 3Q$ estamos nas mesmas condições anteriores, logo calculando o conjunto Δ temos

$$\Delta = \{0, 8, 11, 12, 13, 16, 24\},$$

portanto temos $\gamma(C;P,P) \geq 7$, obtendo assim uma melhora de uma unidade.

Exemplo 6.3. *Definindo o divisor $C = 2P+2Q$ e aplicando o teorema com as sequências de divisores indicadas obtemos os seguintes resultados:*

$$\begin{aligned} A_i = iP: &\quad \Delta = \{0, 8, 10, 13, 16, 21, 29\} \qquad \Delta' = \{14, 15, 27\} \\ A_i = iP + 2Q: &\quad \Delta = \{0, 8, 13, 16, 19, 21, 29\} \qquad \Delta' = \{2, 14, 15\}. \end{aligned}$$

Em ambos casos obtemos $\gamma(C;P,P) \geq 7$. Note que os divisores iP para $i \in \{0, 8, 10, 13\}$ e os divisores $iP+2Q$ para $i \in \{16, 19, 21, 29\}$ contribuem ao conjunto Δ, portanto tomando a sequência

$$0,\ P,\ \ldots,\ 14P,\ 15P,\ 15P+Q,\ 15P+2Q,\ 16P+2Q, \ldots,\ 28P+2Q,\ 29P+2Q$$

e definindo $S = \{P,\ Q\}$ e $S' = \{P\}$ temos que $\gamma(C;S,S') \geq 8$.

Os exemplos anteriores podem ser verificados usando o Algoritmo D. Este algoritmo calcula a cota inferior para $\gamma(C;S;S')$ dada pelo Teorema 6.1.

Vejamos agora como formulamos a cota $d_{ABZ'}$ em função de semigrupos.

Definição 6.4. *Sejam C um divisor e P um lugar racional (ambos fixos), para um divisor A definimos o conjunto*

$$\Delta(A) := \{A_i = A - iP : i \geq 0,\ A_i \in \Gamma_P \ e\ A_i - C \notin \Gamma_P\}.$$

Corolário 6.5 (Cota $d_{ABZ'}$)**.** *Seja $G = K + C = A + B + Z$ tal que $Z \geq 0$ e P um lugar racional com $P \in supp\, Z$, então*

$$\gamma(C; supp\, Z, P) \geq |\Delta(A)| + |\Delta(B)|. \tag{21}$$

Demonstração. Aplicamos o Teorema 6.1 tomando uma sequência de divisores $\{A_i\}$ que contenham aos divisores da forma $B - iP,\ B - (i-1)P,\ \ldots,\ B$ e aos divisores da forma $B + Z + P, \ldots,\ B + Z + jP$ com i e j suficientemente grandes. □

Para recuperar a forma da cota $d_{ABZ'}$ como no Teorema 4.37, notemos que para $A_i = A - iP$ temos

$$\begin{aligned}\ell(A) - \ell(A - C) &= \sum_{i\geq 0}[(\ell(A_i) - \ell(A_i - P)) - (\ell(A_i - C) - \ell(A_i - C - P))] \\ &= |\Delta(A)| - |\Delta'(A)|.\end{aligned}$$

Analogamente, para o divisor B temos $\ell(B) - \ell(B - C) = |\Delta(B)| - |\Delta'(B)|$, logo (21) é equivalente com

$$\gamma(G - K; \operatorname{supp} Z, P) \geq d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|. \tag{22}$$

Também note que $C_\Omega(D, G + P) \subseteq C_\Omega(D, G)$. Seja $c \in C_\Omega(D, G)$ tal que $wt(c) = d(C_\Omega(D, G))$. No caso exista uma palavra $c_1 \in C_\Omega(D, G + P)$ tal que $wt(c_1) = wt(c)$ temos que

$$d(C_\Omega(D, G)) = d(C_\Omega(D, G + P)).$$

Por outro lado, se não existir tal palavra e supondo que $\operatorname{supp} Z \cap \operatorname{supp} D = \emptyset$ e $P \in \operatorname{supp} Z$ segue que

$$\begin{aligned}d(C_\Omega(D, G)) &= \min \operatorname{wt}(C_\Omega(D, G) \backslash C_\Omega(D, G + P)) \geq \gamma(G - K; \operatorname{supp} Z, P) \\ &\geq d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|,\end{aligned}$$

pelo Lema 5.3 e a desigualdade (22). Isto implica que

$$d(C_\Omega(D, G)) \geq \min\{d_{ABZ} + |\Delta'(A)| + |\Delta'(B)|,\, d(C_\Omega(D, G + P))\}.$$

7 Voltando às cotas ordem

Nesta última seção vamos apresentar cotas ordem em forma de semigrupos. Estas cotas são dadas em função das ferramentas desenvolvidas nas duas seções anteriores. A razão pela qual vamos mostrar estas cotas em uma forma diferente é com o objetivo de poder compará-las. Para olhar tais cotas na sua forma original ver [2] e [4].

Pelo Lema 5.3, temos que para estimar uma cota inferior para a distância mínima do código $C_\Omega(D, G)$ basta estimar uma cota inferior para $\gamma(C; S, \emptyset)$ com $\operatorname{supp} D \cap S = \emptyset$. Para começar, na seção anterior vimos a cota $d_{ABZ'}$ na forma de semigrupos, agora veremos a cota dada por Duursma e Park [4, Proposição 4.5] e a cota dada por Duursma e Kirov [2], e veremos a relação entre elas.

Teorema 7.1 (Cota d_{DK})**.** *Seja C um divisor e sejam S' e S conjuntos finitos de lugares racionais, então temos*

$$\gamma(C; S, \emptyset) = \min_{\lambda \in \Lambda'} \gamma(C + \lambda; S, S')$$

onde Λ' é o semigrupo gerado pelos elementos de S'.

Demonstração. Pelo Teorema 5.5 temos

$$\Gamma(C; S, \emptyset) = \bigcup_{\lambda \in \Lambda'} \Gamma(C + \lambda; S, S'),$$

onde Λ' é o semigrupo gerado pelos lugares em S'. Logo segue que

$$\begin{aligned} \gamma(C; S, \emptyset) &= \min \left\{ \deg A : A \in \bigcup_{\lambda \in \Lambda'} \Gamma(C + \lambda; S, S') \right\} \\ &= \min_{\lambda \in \Lambda'} \{ \deg A : A \in \Gamma(C + \lambda; S, S') \} \\ &= \min_{\lambda \in \Lambda'} \gamma(C + \lambda; S, S'). \end{aligned}$$

□

Dado um código $C_\Omega(D, G)$ e conjuntos finitos de lugares racionais S e S' tal que $\operatorname{supp} D \cap S = \emptyset$, podemos determinar uma cota inferior para cada valor $\gamma(C + \lambda; S, S')$, com λ fixo, usando o Teorema 6.1 tomando qualquer sequencia de divisores $A_0, \ldots, A_n$. Vamos denotar esta cota por $\gamma_{DK}(C + \lambda; S, S')$. Portanto, pelo Teorema 7.1 e o Lema 5.3, determinamos uma cota inferior para a distância mínima do código $C_\Omega(D, G)$ que está dada por

$$d(C_\Omega(D, G)) \geq \min_{\lambda \in \Lambda'} \gamma_{DK}(C + \lambda; S, S'),$$

a qual chamamos cota d_{DK} correspondente aos conjuntos S e S'. Note que o conjunto finito S tem só uma restrição, $\operatorname{supp} D \cap S = \emptyset$.

A cota ordem d_{DP}, dada por Duursma e Park [4, Proposição 4.5], é um caso particular da cota d_{DK}.

Corolário 7.2 (Cota d_{DP})**.** *Com as hipóteses do Teorema 7.1 temos*

$$\gamma(C; S, \emptyset) \geq \min_{\lambda \in \Lambda'} \left(\max_{Q \in S'} \gamma(C + \lambda; S, Q) \right),$$

onde Λ' é o semigrupo gerado pelos elementos de S'.

Demonstração. Note que para todo $\lambda \in \Lambda'$

$$\Gamma(C+\lambda; S, S') = \bigcap_{Q \in S'} \Gamma(C+\lambda; S, Q),$$

assim temos $\Gamma(C+\lambda; S, S') \subseteq \Gamma(C+\lambda; S, Q)$ para todo $Q \in S'$, logo $\gamma(C+\lambda; S, S') \geq \gamma(C+\lambda; S, Q)$ para todo $Q \in S'$, portanto

$$\gamma(C+\lambda; S, S') \geq \max_{Q \in S'} \gamma(C+\lambda; S, Q).$$

Disto e do Teorema 7.1 segue que

$$\gamma(C; S, \emptyset) = \min_{\lambda \in \Lambda'} \gamma(C+\lambda; S, S') \geq \min_{\lambda \in \Lambda'} \left(\max_{Q \in S'} \gamma(C+\lambda; S, Q) \right).$$

□

Da mesma maneira que para a cota d_{DK}, dado um código $C_\Omega(D, G)$ e um conjunto finito de lugares racionais S tal que $\operatorname{supp} D \cap S = \emptyset$ e, a diferença da cota d_{DK}, vamos tomar S' com um só elemento, é dizer, $S' = \{P\}$ onde P é um lugar racional. Podemos determinar uma cota inferior para $\gamma(C+iP; S, P)$, com i fixo tal que $i \geq 0$, usando o Teorema 6.1 com qualquer sequencia de divisores $A_0, \ldots, A_n$. Denotaremos esta cota inferior por $\gamma_{DP}(C+iP; S, P)$. Assim, pelo Corolário 7.2 e o Lema 5.3, obtemos uma cota inferior para a distância mínima do código $C_\Omega(D, G)$ que está dada por

$$d(C_\Omega(D, G)) \geq \min_{\lambda \in \Lambda'} \left(\max_{Q \in S'} \gamma_{DP}(C+\lambda; S, Q) \right) = \min_{i \geq 0} \{\gamma_{DP}(C+iP; S, P)\},$$

a qual chamamos cota d_{DP} correspondente aos conjuntos S e $S' = \{P\}$.

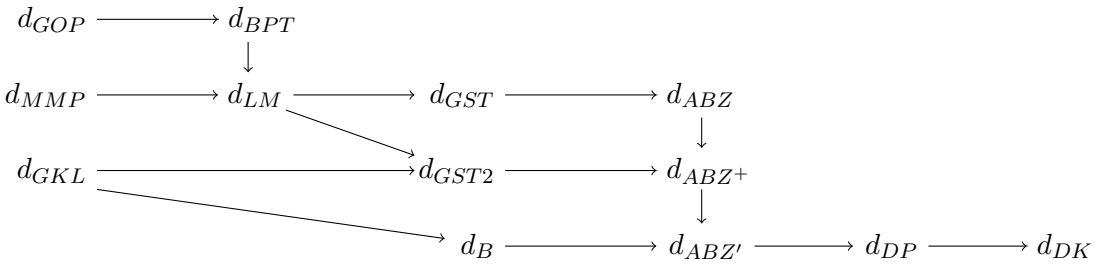
Observação 7.3. *A cota $d_{ABZ'}$ é um caso particular da cota d_{DP}, pois neste caso tomamos $S = \operatorname{supp} Z$ e $S' = \{P\}$, onde A, B e Z são divisores tais que $Z \geq 0$ e $K + C = A + B + Z$ e P é um lugar racional tal que $P \in \operatorname{supp} Z$. Assim temos*

$$\gamma(C+iP; \operatorname{supp} Z, P) \geq |\Delta(A)| + |\Delta(B)|$$

para todo $i \geq 0$. Esta última desigualdade obtém-se fazendo uso do Teorema 6.1 tomando uma sequência de divisores $\{A_i\}$ que contenham aos divisores da forma $B - iP$, $B - (i-1)P$, $\ldots$, B e aos divisores da forma $B + Z + P, \ldots, B + Z + jP$ com i e j suficientemente grandes.

Observação 7.4. *De forma análoga, a cota d_B é também um caso particular da cota d_{DP}. Ela toma uma sequência de divisores no formato $A_k = B + kP$, onde $k \in \mathbb{Z}$, e os conjuntos $S = S' = \{P\}$.*

Assim, todas as cotas estudadas neste trabalho e as relações existentes entre elas podem ser representadas no seguinte diagrama:



Apêndice

Neste trabalho são calculadas as cotas apresentadas em um exemplo explícito mediante algoritmos desenvolvidos no programa "Magma Calculator". O código usado foi o código gerado para o corpo de funções de Suzuki sobre o corpo $\mathbb{F}_8$. Todos os algoritmos começaram com as seguintes linhas:

```
p:=2;
n:=3;
F<a>:=GF(p^n); //corpo finito com p^n elementos
PS<x,y,z>:=ProjectiveSpace(F,2); //espaço projetivo
W:=z^9*y-z^7*x^3+z^2*y^8-x^10; //curva Suzuki homogeneizada
C1:=Curve(PS,W); //curva homogeneizada no espaço projetivo
Pl:=Places(C1,1); //lugares racionais da curva C1
K:=CanonicalDivisor(C1); //definição do divisor canônico
D:=[Pl[i]:i in [3..#Pl]]; //definição do divisor D
```

Cada algoritmo deve ser complementado com as seguintes linhas dependendo de cada caso a ser usado. Em alguns casos, de acordo com a definição dos divisores, algumas linhas devem ser modificadas.

A Algoritmo para Cotas Básicas

```
G:=a*Pl[1]+b*Pl[2];
C:=G-K;
//Cota GOP
"d_GOP: ", Degree(C);
//Cota BPT
if (Dimension(C-1*Pl[1]) eq Dimension(C)) or
(Dimension(C-1*Pl[2]) eq Dimension(C)) then
 "d_BPT: ", Degree(C) +1;
else
 "d_BPT: Os divisores dados não satisfazem as condições para esta
  cota";
end if;\\
```

B Algoritmo para Cotas Piso

```
//Cota LM
//definição dos divisores
A:=a1*Pl[1]+b1*Pl[2];
B:=a2*Pl[1]+b2*Pl[2];
Z:=a3*Pl[1]+b3*Pl[2];
//
G:=A+B+Z;
if (Dimension(A+Z) eq Dimension(A)) and
(Dimension(B+Z) eq Dimension(B)) then
 "d_LM: ", Degree(G-K) + Degree(Z);
else
 "d_LM: Os divisores dados não satisfazem as condições para esta
  cota";
end if;
//Cota GST
//definição dos divisores
AA:=a1*Pl[1]+b1*Pl[2];
BB:=a2*Pl[1]+b2*Pl[2];
CC:=a3*Pl[1]+b3*Pl[2];
ZZ:=a4*Pl[1]+b4*Pl[2];
//
GG:=AA+BB;
if (Dimension(AA-ZZ) eq Dimension(AA)) and
(Dimension(BB+ZZ) eq Dimension(BB)) and
(Dimension(BB) eq Dimension(CC))  then
 "d_GST: ", Degree(GG-K) + Degree(ZZ) + Dimension(K-AA)
 - Dimension(K-GG+CC);
else
 "d_GST: Os divisores dados não satisfazem as condições para esta
 cota";
end if;
//Cota ABZ
//definição dos divisores
AAA:=a1*Pl[1]+b1*Pl[2];
```

```
BBB:=a2*Pl[1]+b2*Pl[2];
ZZZ:=a3*Pl[1]+b3*Pl[2];
//
GGG:=AAA+BBB+ZZZ;
CCC:=GGG-K;
"d_ABZ: ", Dimension(AAA)-Dimension(AAA-CCC)+Dimension(BBB)
-Dimension(BBB-CCC);\\
```

C Algoritmo para Cotas Mistas

```
//Cota GST2
//definição dos divisores
A:=a1*Pl[1]+b1*Pl[2];
B:=a2*Pl[1]+b2*Pl[2];
Z:=a3*Pl[1]+b3*Pl[2];
//
G:=A+B;
if (Support(A-B) subset Support(Z)) and
   (Id(DivisorGroup(C1)) lt Z) and
   (Dimension(A-Z) eq Dimension(A)) and
   (Dimension(B+Z+1*Pl[1]) eq Dimension(B)) and
   (Dimension(B+Z+1*Pl[2]) eq Dimension(B)) and
   ((B+Z+1*Pl[1] lt A) or (B+Z+1*Pl[2] lt A)) then
 "d_GST2: ", Degree(G-K)+Degree(Z)+1;
else
 "d_GST2: Os divisores dados não satisfazem as condições para esta
 cota";
end if;
//Cota ABZ+
//definição dos divisores
AA:=a1*Pl[1]+b1*Pl[2];
BB:=a2*Pl[1]+b2*Pl[2];
ZZ:=a3*Pl[1]+b3*Pl[2];
A_:=a4*Pl[1]+b4*Pl[2];
B_:=a5*Pl[1]+b5*Pl[2];
//
```

```
GG:=AA+BB+ZZ;
CC:=GG-K;
if (Dimension(AA-CC) ne Dimension(AA-CC-1*Pl[1])) and
   (Dimension(AA-CC) ne Dimension(AA-CC-1*Pl[2])) and
   (Support(AA-A_) subset Support(ZZ)) and
   (((Dimension(A_-CC) ne Dimension(A_-CC-1*Pl[1])) and
   (Dimension(A_) eq Dimension(A_-1*Pl[1]))) or
   ((Dimension(A_-CC) ne Dimension(A_-CC-1*Pl[2])) and
   (Dimension(A_) eq Dimension(A_-1*Pl[2])))) then
   i:=true;
else
   i:=false;
end if;
if (Dimension(BB-CC) ne Dimension(BB-CC-1*Pl[1])) and
   (Dimension(BB-CC) ne Dimension(BB-CC-1*Pl[2])) and
   (Support(BB-B_) subset Support(ZZ)) and
   (((Dimension(B_-CC) ne Dimension(B_-CC-1*Pl[1])) and
   (Dimension(B_) eq Dimension(B_-1*Pl[1]))) or
   ((Dimension(B_-CC) ne Dimension(B_-CC-1*Pl[2])) and
   (Dimension(B_) eq Dimension(B_-1*Pl[2])))) then
   j:=true;
else
   j:=false;
end if;

if (i eq false) and (j eq false) then
     "d_ABZ+: ", Dimension(AA)-Dimension(AA-CC)+Dimension(BB)
     -Dimension(BB-CC);
elif ((i eq false) and (j eq true)) or
     ((i eq true) and (j eq false)) then
     "d_ABZ+: ", Dimension(AA)-Dimension(AA-CC)+Dimension(BB)
     -Dimension(BB-CC)+1;
else
     "d_ABZ+: ", Dimension(AA)-Dimension(AA-CC)+Dimension(BB)
     -Dimension(BB-CC)+2;
end if;
```

D Algoritmo para o Teorema Principal

```
//Cálculo de cotas para gamma(C;S,S')
A:=[DivisorGroup(C1)|];
P:=[DivisorGroup(C1)|];

//pontos racionais
for i in [1..100] do
P[i]:=Pl[1];
end for;
C:=a*Pl[1]+b*Pl[2]; //divisor C
AA:=c*Pl[1]+d*Pl[2]; //divisor inicial
A[1]:=AA+P[1];

//definição dos demais divisores
for i in [2..#P] do
A[i]:=A[i-1]+P[i];
end for;

//conjunto S
S:=[DivisorGroup(C1)|Pl[1]];
//conjunto S'
SS:=[DivisorGroup(C1)|Pl[1]];
//conjunto Delta
D:={i: i in [1..#P]|(Dimension(A[i]) ne Dimension(A[i]-P[i]))
and (Dimension(A[i]-C) eq Dimension(A[i]-C-P[i]))};
"Delta: ",D;
//conjunto Delta'
E:={i: i in [1..#P]|(Dimension(A[i]) eq Dimension(A[i]-P[i]))
and (Dimension(A[i]-C) ne Dimension(A[i]-C-P[i]))};
"Delta': ",E;
//conjunto I
I:={i:i in [1..#P]|P[i] in S};
//conjunto I'
J:={i:i in [1..#P]|P[i] in SS};
"gamma(C;S,S') >=", #(D meet J)+#(E meet I)-#(E);
```

Referências

[1] Beelen, Peter. *The order bound for general algebraic geometric codes.* Finite Fields and Their Applications 13.3 (2007): 665-680.

[2] Duursma, Iwan, e Radoslav Kirov. *An extension of the order bound for AG codes.* International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Springer, Berlin, Heidelberg, 2009.

[3] Duursma, Iwan, Radoslav Kirov, e Seungkook Park. *Distance bounds for algebraic geometric codes.* Journal of Pure and Applied Algebra 215.8 (2011): 1863-1878.

[4] Duursma, Iwan M., e Seungkook Park. *Coset bounds for algebraic geometric codes.* Finite Fields and Their Applications 16.1 (2010): 36-55.

[5] Garcia, Arnaldo, Seon Jeong Kim, e Robert F. Lax. *Consecutive Weierstrass gaps and minimum distance of Goppa codes.* Journal of pure and applied algebra 84.2 (1993): 199-207.

[6] Garcia, Arnaldo, e R. F. Lax. *Goppa codes and Weierstrass gaps.* Coding Theory and Algebraic Geometry. Springer, Berlin, Heidelberg, 1992. 33-42.

[7] Goppa, Valerii Denisovich. *Codes associated with divisors.* Problemy Peredachi Informatsii 13.1 (1977): 33-39.

[8] Güneri, Cem, Henning Stichtenoth, e İhsan Taşkın. *Further improvements on the designed minimum distance of algebraic geometry codes.* Journal of Pure and Applied Algebra 213.1 (2009): 87-97.

[9] Lundell, Benjamin, e Jason McCullough. *A generalized floor bound for the minimum distance of geometric Goppa codes.* Journal of Pure and Applied Algebra 207.1 (2006): 155-164.

[10] Magma Computational Algebra System, Online disponível em `http://magma.maths.usyd.edu.au`.

[11] Maharaj, Hiren, Gretchen L. Matthews, e Gottlieb Pirsic. *Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences.* Journal of Pure and Applied Algebra 195.3 (2005): 261-280.

[12] Robles, Diogo. *Lacunas de Weierstrass e Códigos de Goppa.* Dissertação de Mestrado, Unicamp-São Paulo (1997).

[13] Salvador, Gabriel Daniel Villa. *Topics in the theory of algebraic function fields.* Springer Science and Business Media, 2006.

[14] Stichtenoth, Henning. *Algebraic function fields and codes.* Vol. 254. Springer Science and Business Media, 2009.

[15] Van Lint, J., and R. Wilson. *On the minimum distance of cyclic codes.* IEEE Transactions on Information Theory 32.1 (1986): 23-40.