Formas aditivas de grau 3^{τ}

Carlos Alirio Rico Acevedo

Brasília

2022

Carlos Alirio Rico Acevedo

Formas aditivas de grau 3^τ

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de DOUTOR EM MATEMÁTICA

Orientador:
Prof. Dr. Hemar Teixeira Godinho

Brasília

2022

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Formas Aditivas de Grau 3^tau
por

Carlos Alírio Rico Acevedo

Tese apresentada ao Departamento de Matemática da Universidade de Brasília como parte dos requisitos para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília, 03 de março de 2022.

Comissão Examinadora:

Hemar T. C. Godinho

Prof. Dr. Hemar Teixeira Godinho- MAT/UnB (Orientador)

Prof. Dr. Diego Marques Ferreira– MAT/UnB (Membro)

Ana Paula M. A. Chaves

Profa. Dra. Ana Paula Chaves – UFG (Membro)

Michael P. Knapp

Prof. Dr. Michael Knapp – Loyola University (Membro)

Victor Neumann

Prof. Dr. Victor Gonzalo Lopez Neumann - UFU (Membro)

Dedicado a Deus e à razão pela qual fui enviado, aos meus pais que sempre me apoiaram e aceitaram com amor a distância que surgiu na minha procura dos meus sonhos, espero estar mais presente e perto de vocês nos próximos anos. Também, este trabalho esta dedicado a minha avó Yolanda, quem me mostrou que não há idade para seguir os sonhos, e as minhas irmãs, Marcela e Angie, as quais tem-me brindado seu amor e carinho. Finalmente, aos meus sobrinhos, Luna e Samuel, que seu sonho de seguir o caminho da ciência esteja sempre cheio de sucesso.

Agradecimentos

... e você ainda ficará surpreso com você ... Coisas que eu nunca pensei fazer, e outras que pareciam surgir naturalmente, agradeço a Deus por elas.

Ao professor Hemar Godinho pela sua confiança, seu tempo e elegantes contribuições que viavilizaram este trabalho.

A Bruno de Paula Miranda, por todas suas contribuições e paciência e parceria no desenvolvimento deste trabalho.

Aos meus amigos no Brasil, em especial a Victor, Jeferson, Milton, Angie e Andres. Também, agradeço a aqueles que decidiram acolher algumas das minhas ideias.

À CNPq e à Capes pelo financiamento durante Doutorado.

Abstract

For any positive integer k, we define $\Gamma^*(k,p)$ to be the smallest integer s such that every additive form $a_1x_1^k + \cdots + a_sx_s^k$ in s variables with integers coefficients have a nontrivial zero in the p-adic field $\mathbb{Q}_p$. In this way, we define $\Gamma^*(k)$ to be the smallest integer s for which every additive form of degree k with integer coefficients in s variables have a nontrivial zero in every p-adic fields, i.e, $\Gamma^*(k) = \max_p\{\Gamma^*(k,p)\}$ for p prime. Now, we define

$$\gamma^* = \lfloor (\tau+1)\log_2(3) \rfloor + 1.$$

In [16] Knapp shows that for $k = 27$, them $\Gamma^*(27,3) \leq 27(\gamma^* - 3) + 1 = 109$, but, we will improve and generalize this bound, i.e, we should prove to

$$\Gamma^*(3^\tau, 3) \leq 3^\tau(\gamma^* - \tau - 1) + 1.$$

In addition, we give upper bounds for $\Gamma^*(k,p)$ when -1 is a kth power modulo $p^{\tau+1}$. Also, the exact value of $\Gamma^*(81) = 568$, and in an analogous way, we should prove that $\Gamma^*(243,p) \leq 1945$ for p different from 3889 or 4861, and that $\Gamma^*(729,p) \leq 7291$ for any $p \neq 2917$.

Keywords: Additive forms, p-adic solubility.

Resumo

Para quaisquer inteiro positivo k é definido $\Gamma^*(k,p)$ sendo o menor inteiro s tal que quaisquer forma aditiva $a_1x_1^k+\cdots+a_sx_s^k$ em s variáveis com coeficientes nos inteiros possui um zero não trivial no corpo p-ádico $\mathbb{Q}_p$. Por sua vez, define-se $\Gamma^*(k)$ sendo o menor inteiro s para o qual, quaisquer forma aditiva de grau k com coeficientes inteiros em s variáveis possui um zero não trivial em quaisquer corpo p-ádico, isto é, $\Gamma^*(k) = \max_p\{\Gamma^*(k,p)\}$ com o máximo percorrendo o conjunto dos números primos. Agora, defina

$$\gamma^* = \lfloor(\tau+1)\log_2(3)\rfloor + 1.$$

Em [16] Knapp mostra que quando $k = 27$, então $\Gamma^*(k,3) \leq 27(\gamma^* - 3) + 1 = 109$, mas em este trabalho é generalizada e melhorada esta limitante e mostra-se que

$$\Gamma^*(3^\tau,3) \leq 3^\tau(\gamma^* - \tau - 1) + 1.$$

Além disso, são dadas limitantes superiores para $\Gamma^*(k,p)$ quando -1 é uma k-ésima potencia modulo $p^{\tau+1}$. Também, é dado o valor exato de $\Gamma^*(81) = 568$, e, de maneira análoga, mostra-se que $\Gamma^*(243,p) \leq 1945$ para p diferente de 3889 ou 4861, e que $\Gamma^*(729,p) \leq 7291$ sempre que $p \neq 2917$.

Palavras-chave: Formas aditivas, solvibilidade p-ádica.

Notação

γ	Ver (1.20).
γ^*	Ver (2.2).
$\mathscr{F}, \mathscr{G}, \ldots$	Formas aditivas de grau k. Ver (1.16).
$\mathscr{F}_j$	Nível j de uma uma forma aditiva p-normalizada $\mathscr{F}$. Ver Lema 1.8 (1.18).
$\mathscr{F}^{(i)}$	Ver (1.19), (3.7), (3.8), (3.9).
m_j	Número de variáveis no nível j. Ver Lema 1.8 (1.18).
C	Configuração. Ver Definição 3.2.1 ou Definição 3.2.3
B	Bloco de uma configuração C. Ver Definição 3.2.2.
Σ_C	Número de variáveis em uma configuração C.
Σ_B	Número de variáveis em um Bloco B.
$\Theta(B, M)$	Ver Teorema 3.14.
$\Lambda(C)$	Ver (3.24).
$\Psi(t, n)$	Ver (3.25).
$\Psi(t, n, M)$	Ver (3.26).

Sumario

Introdução

Em 1920 Artin conjeturou que quaisquer polinômio homogêneo de grau k em s variáveis tem zeros p-ádicos desde que $s \leq k^2 + 1$ e, em 1924 os resultados de Hasse em [14] confirmaram os resultados para formas quadráticas. Isso estabeleceu o que hoje é conhecido como o principio Local-Global, o qual estabelece que: uma forma com coeficientes racionais, possui zeros racionais se, e somente se, possui zeros reais e p-ádicos. Em 1952 Lewis mostrou em [18] a validade da conjetura quando $k = 3$. Em 1957, Lewis [19] encontrou que 7 variáveis são suficientes para que toda forma aditiva (ou diagonal) de grau 3, possua um zero p-ádico, isto é, a forma

$$a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3,$$

possui um zero p-ádico sempre que $s \geq 7$.

De maneira geral, considere a forma aditiva de grau k

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \tag{1}$$

com coeficientes nos inteiros, e defina $\Gamma^*(k,p)$ como sendo o menor inteiro s para o qual (1) tem solução p-ádica para um primo p fixo, isto é, um zero p-ádico não trivial. Por sua vez, defina $\Gamma^*(k)$ como o menor número de variáveis, para o qual (1) tem solução p-ádica para todo primo p. Tem-se assim que

$$\Gamma^*(k) = \max_p\{\Gamma^*(k,p)\}.$$

Em 1963, Davenport e Lewis mostraram em [8] que $\Gamma^*(k) \leq k^2 + 1$, e a igualdade acontece quando $k+1$ é primo. Além disso, eles introduziram o método de contração de variáveis e a p-normalização, o qual é amplamente usado nos trabalhos sobre formas aditivas. O resultado de Davenport e Lewis, confirmou a conjetura de Artin para formas aditivas. Essa conjetura é falsa para formas em geral, pois em 1966 Terjanian [22], apresentou o seguinte polinômio

$$\mathcal{G}(\mathbf{x}) = x_1^4 + x_2^4 + x_3^4 - \left(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2\right) - x_1x_2x_3(x_1 + x_2 + x_3).$$

e mostrou que

$$\mathscr{G}(\mathbf{x_1}, \ldots, \mathbf{x_6}) = \mathcal{G}(\mathbf{x_1}) + \mathcal{G}(\mathbf{x_2}) + \mathcal{G}(\mathbf{x_3}) + 4\mathcal{G}(\mathbf{x_4}) + +4\mathcal{G}(\mathbf{x_5}) + 4\mathcal{G}(\mathbf{x_6}),$$

onde $\mathbf{x_i} = (x_{1,i}, x_{2,i}, x_{3,i})$, é uma forma em 18 variáveis que não possui zeros 2-ádicos.

No que diz respeito às formas aditivas, Chowla [6] mostrou que para formas aditivas de grau ímpar, o número de variáveis necessárias para garantir a solubilidade p-ádica é menor que $k^2 + 1$, a saber, da ordem $k \log(k)$, isto é,

$$\limsup_{k\to\infty} \left\{ \frac{\Gamma^*(k)}{k\log(k)} \right\} = \vartheta,$$

onde k é um inteiro ímpar. Neste sentido, Chowla e Shimura [7] mostraram que

$$\frac{1}{\log(2)} \leq \vartheta \leq \frac{2}{\log(2)}$$

e finalmente Tietäväinen [23] mostrou que $\vartheta = 1/\log(2)$. Outros resultados foram desenvolvidos na década dos 60's e inicio dos 70's do século anterior como por exemplo: $\Gamma^*(5) = 16$ por Gray [13], $\Gamma^*(7) = 22$ e $\Gamma^*(11) = 45$ por Bierstedt [1]. Também, Norton [21] mostra estes dois últimos resultados e, além disso, encontra que 37 variáveis são suficientes para uma forma aditiva de grau 9; De maneira independente, Dodson [9] encontra os valores $\Gamma^*(7)$ e $\Gamma^*(9)$. Em 1974, Bovey [3] mostrou que $\Gamma^*(8) = 39$.

Um longo tempo na apresentação de resultados para $\Gamma^*(k)$ ocorreu, e uma das causas de não ter avanços sobre o conhecimento dos valores exatos desta função desde os anos 70's do século anterior até hoje, deve-se à limitante de calculo computacional que é preciso em alguma parte dos métodos conhecidos. Não foi até 2011 que Knapp em [16] encontra $\Gamma^*(k)$ para os valores de k menores o iguais que 31 restantes, e no ano de 2018, em [17] encontra $\Gamma^*(32) = 524$. Por outra parte, Veras [24] em 2017 encontra $\Gamma^*(54) = 1049$ e mais recentemente Broll, Knapp, Kuiper, Rodrigues e Veras [4][1] dão os valores exatos de $\Gamma^*(k)$ para $33 \leq k \leq 64$.

São apenas conhecidas três fórmulas para o valor exato de $\Gamma^*(k)$: A primeira foi dada por Davemport e Lewis que é: $\Gamma^*(k) = k^2 + 1$ quando $k+1$ é primo. A segunda, foi dada por Dodson [9], sempre que $k+1$ é composto e $k \geq 7$, da forma $k = p(p-1)$, tem-se

$$\Gamma^*(k) = \frac{k^2}{2}\left(1 + \frac{1}{p}\right) + 1.$$

Knapp e Godinho [10] estabelecem uma fórmula exata quando $k = q^\tau(q-1)$ onde q é um número primo, com algumas restrições para q e τ, o que torna k muito grande.

Uma condição para encontrar zeros p-ádicos para uma forma aditiva, foi dada por Dodson [9]. Para isto, seja $k = p^\tau k_0$, com $(p, k_0) = 1$, sendo $(\cdot,\cdot)$ o máximo comum divisor. E seja

$$\gamma = \begin{cases} \tau + 1 & \text{se } \; p > 2, \;\; \text{ou} \;\; p = 2 \;\; e \;\; \tau = 0 \\ \tau + 2 & \text{se } \; p = 2. \end{cases} \tag{2}$$

Defina $\gamma^*(k, p^\gamma) = \gamma^*$ como o menor inteiro positivo s com a seguinte propriedade: Se $a_1, \ldots, a_s$ são inteiros primos relativos com p, então a congruência

$$a_1 x_1^k + \cdots + a_s x_s^k \pmod{p^\gamma}$$

possui uma solução primitiva, que é uma solução para a qual não todas as variáveis $x_1, \ldots, x_s$ são divisíveis por p. Daí, Dodson mostrou que

$$\Gamma^*(k, p) \leq k(\gamma^* - 1) + 1.$$

Por sua vez, Knapp em [16] mostra para $k = 27$ e $p = 3$ que

$$\Gamma^*(27, 3) \leq k(\gamma^* - 3) + 1 = 109.$$

Neste trabalho encontra-se que é possível generalizar este resultado como segue,

[1] Neste ponto, gostaria de agradecer aos autores por gentilmente me cederem uma cópia do seu trabalho para conhecer estes resultados.

Teorema 0.1. *Seja* $k = p^\tau(p-1)/2$. *Se* $\gamma^* - 4 \geq p$, *então*

$$\Gamma^*(k,p) \leq k(\gamma^* - 3) + 1. \tag{3}$$

Este resultado é mostrado no Capitulo 2. Surge de maneira natural para o caso $p = 3$ se perguntar: É possível diminuir a limitante superior para $\Gamma^*(27,3)$? E mais geralmente, dado que para $k = p^\tau(p-1)/2$, tem-se que -1 é uma potencia k-esima módulo p^γ, é possível obter melhores limitantes para $\Gamma^*(k,p)$? Da resposta a estas perguntas surge o desenvolvimento deste trabalho.

Para dar solução a estas perguntas seguem as seguintes considerações: Primeiro, fixa-se desde agora para este trabalho a hipótese especial de que -1 é sempre uma potencia k-ésima módulo p^γ. Por isso, ela é omitida no enunciado dos resultados, mas em alguns casos relembrada previamente.

Por outra parte, no capítulo 1 são estabelecidos resultados preliminares sobre formas aditivas e número de soluções das mesmas, os resultados deste capítulo são clássicos, e são apresentados por completude. A sua vez, na seção 2.1 do capítulo 2 encontra-se uma versão do Lema de Hensel 1.9, o Lema 2.1 dado por Godinho, Knapp, Rodriguez, Veras em [11], o qual junto com o Lema 2.4 constituem uma das ferramentas mais importantes no desenvolvimento deste trabalho. Consequência destes lemas, mostra-se neste mesmo capítulo o Teorema 0.1 e o seguinte resultado.

Teorema 0.2. *Para todo inteiro* $\tau \geq 1$ *existe um primo* q *ímpar, tal que para todo* $p \geq q$, *se* $k = p^\tau k_0$, *com* $(k_0, p) = 1$ *vale*

$$\Gamma^*(k,p) \leq k(\gamma^* - \gamma) + 1. \tag{4}$$

É em este momento no capítulo 2 que conjetura-se o seguinte: *Para todo* $\tau \geq 1$ *e para todo primo* $p \geq 3$ *é satisfeita a desigualdade (4).* Esta conjetura esta motivada tanto pelo Teorema 0.2, como pelo resultado principal deste trabalho, o qual é o seguinte.

Teorema A 1. *Seja* $\tau \geq 1$ *e* $k = 3^\tau$, *então*

$$\Gamma^*(k,3) \leq k(\gamma^* - \gamma) + 1.$$

Este resultado é mostrado no capítulo 4, mas para isso, no capítulo 3 estabelece-se o método de contração de variáveis para este trabalho, o qual pode ser achado na seção 3.1. Também, no capítulo 3 o uso do Lema 2.4 e a contração de variáveis, permitem desenhar algumas ferramentas combinatórias e de contagem de variáveis chamadas t-Blocos, os quais são necessários para o capítulo 4.

Finalmente, no Capitulo 5 é feita uma implementação do método de Knapp em [16] que, junto com o Teorema 1 permite mostrar que $\Gamma^*(81) = 568$. Além disso, mostra-se que $\Gamma^*(243, p) \leq 1945$, para todo primo $p \notin \{3889, 4861\}$, e também mostra-se que $\Gamma^*(729, p) \leq 72915$, para todo primo $p \neq 2917$. Para isto, é necessário a ajuda computacional, cujos comandos encontram-se no Apêndice A.

Capítulo 1

Preliminaries

1.1 Somas Exponenciais

Em Teoria de Números como em outras áreas, muitas vezes não é fácil estabelecer ou achar soluções explicitas para algumas equações, mas em muitos destes casos é apenas suficiente garantir a existência de pelo menos uma solução, e, é em este sentido que as somas exponenciais são frequentemente usadas. As componentes básicas da somas exponenciais são um grupo de homomorfismos chamados caracteres o quais se definem como segue.

Definição 1.1.1. *Seja $(G, \circ)$ um grupo abeliano finito e U o grupo multiplicativo das raízes da unidade em $\mathbb{C}$. Diz-se que χ é um carácter de G, se ele é um homomorfismo de G em U.*

Da definição é claro que se χ é um carácter, tem-se para todo $g_1, g_2 \in G$ que $\chi(g_1 \circ g_2) = \chi(g_1)\chi(g_2)$, isto implica que se 1_G é a identidade de G, obtém-se

$$\chi(1_G) = \chi(1_G)\chi(1_G),$$

do qual se conclui $\chi(1_G) = 1$. Ainda mais, se $|G|$ é a ordem de G, então

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1.$$

Do anterior, tem-se para todo $g \in G$ que os valores de χ são as $|G|$-ésimas raízes da unidade. Por outra parte, note que

$$\chi(g)\chi(g^{-1}) = \chi(g \circ g^{-1}) = \chi(1_G) = 1,$$

onde g^{-1} é o inverso de g pela operação de grupo. Isto implica que para todo $g \in G$

$$\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$$

onde do lado direito é a conjugação dos complexos.

Seja G^* o conjunto formado pelos caracteres de G, munido com a operação de produto de caracteres, isto é, para todo $g \in G$ e $\chi_1, \ldots, \chi_n$ caracteres de G

$$(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g).$$

Então o par $(G^*, \cdot)$ forma um grupo abeliano finito, com identidade $\chi_0(g) = 1$, para todo $g \in G$, chamado carácter trivial. E para cada carácter χ de G existe o conjugado associado definido por $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$. Com isto, tem-se as seguintes propriedades.

Teorema 1.1. *Seja G um grupo abeliano finito, então*

(i). $\displaystyle\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G^*| & \textit{se } g = 1_G, \\ 0 & \textit{se } g \neq 1_G. \end{cases}$

(ii). $\displaystyle\sum_{g \in G} \chi(g) = \begin{cases} |G| & \textit{se } \chi = \chi_0, \\ 0 & \textit{se } \chi \neq \chi_0. \end{cases}$

(iii). $|G| = |G^*|$

Demonstração. Por simplicidade, escreve-se de aqui em diante a operação de elementos do grupo G como $g_1 \circ g_2 = g_1 g_2$. Dado que todo carácter de G é um homomorfismo, tem-se que $\chi(1_G) = 1$, assim

$$\sum_{\chi \in G^*} \chi(1_G) = \sum_{\chi \in G^*} 1 = |G^*|.$$

De outra parte, se $g \neq 1_G$, então existe um carácter ψ de G, tal que $\psi(g) \neq 1$, logo

$$\psi(g) \sum_{\chi \in G^*} \chi(g) = \sum_{\chi \in G^*} (\psi\chi)(g) = \sum_{\chi \in G^*} \chi(g).$$

Logo, tem-se (i), dado que $\psi\chi \in G^*$ e G^* é um grupo abeliano finito.

Agora, se $\chi \neq \chi_0$, então existe $g_2 \in G$ tal que $\chi(g_2) \neq 0$, daí

$$\chi(g_2) \sum_{g_1 \in G} \chi(g_1) = \sum_{g_1 \in G} \chi(g_1 g_2) = \sum_{g_1 \in G} \chi(g_1).$$

Assim, fica mostrado (ii) quando $\chi \neq \chi_0$, pois G é um grupo abeliano finito. Caso $\chi = \chi_0$ o resultado é imediato. Finalmente, a prova de (iii), segue por (i) e (ii) que

$$|G| = \sum_{\chi \in G^*} \sum_{g \in G} \chi(g) = \sum_{g \in G} \sum_{\chi \in G^*} \chi(g) = |G^*|.$$

□

Usando as propriedades de grupo de G^* e as propriedades (i) e (ii) do anterior Teorema, obtém-se as relações ortogonais para caracteres como segue: Sejam χ, ψ caracteres de G. Então

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi}(g) = \begin{cases} 1 & \text{se } \chi = \psi \\ 0 & \text{se } \chi \neq \psi. \end{cases}$$

Por outra parte, para $g_1, g_2 \in G$

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1)\overline{\chi}(g_2) = \begin{cases} 1 & \text{se } g_1 = g_2 \\ 0 & \text{se } g_1 \neq g_2. \end{cases}$$

Estas relações ortogonais são a base para encontrar o número de soluções para funções definidas sobre G. Seja f um função do produto cartesiano $G^n = G \times \cdots \times G$ a G, então para um $h \in G$ o número de soluções $N(h)$ da equação $f(g_1, \ldots, g_n) = h$ esta dado por

$$N(h) = \frac{1}{|G|} \sum_{g_1 \in G} \cdots \sum_{g_n \in G} \sum_{\chi \in G^*} \chi(f(g_1, \ldots, g_n))\overline{\chi}(h). \tag{1.1}$$

Agora, considere $(G, +, \cdot)$ um corpo finito de ordem q, com 0_G o elemento neutro aditivo e 1_G o elemento neutro multiplicativo. Sejam ψ um carácter multiplicativo de G, isto é, um carácter do grupo multiplicativo $G^\times$, e χ um carácter do grupo aditivo de G, define-se a Soma Gaussiana como

$$\tau(\psi, \chi) = \sum_{g \in G^\times} \psi(g)\chi(g).$$

Teorema 1.2. *Seja ψ um carácter multiplicativo e χ um carácter aditivo de G. Então a soma Gaussiana $\tau(\psi, \chi)$ satisfaz*

$$\tau(\psi, \chi) = \begin{cases} q-1 & \text{se } \psi = \psi_0, \chi = \chi_0, \\ -1 & \text{se } \psi = \psi_0, \chi \neq \chi_0, \\ 0 & \text{se } \psi \neq \psi_0, \chi = \chi_0. \end{cases} \tag{1.2}$$

Além disso, se $\psi \neq \psi_0$ e $\chi \neq \chi_0$, então

$$|\tau(\psi, \chi)| = q^{1/2}. \tag{1.3}$$

Demonstração. Note que para o corpo finito $(G, +, \cdot)$, tem-se que a ordem do grupo multiplicativo $G^\times$ é $q-1$, assim se $\chi = \chi_0$, segue do Teorema 1.1.(ii) a primeira parte da igualdade (1.2). Agora, se ψ é o carácter multiplicativo trivial, então pelo Teorema 1.1.(ii)

$$\tau(\psi_0, \chi) = \sum_{g \in G^\times} \chi(g) = \sum_{g \in G} \chi(g) - \chi(0_G) = -1.$$

Da mesma forma, pela parte (ii) do Teorema 1.1 segue a terceira parte de (1.2). Finalmente, se $\psi \neq \psi_0$ e $\chi \neq \chi_0$, tem-se

$$\begin{aligned} |\tau(\psi, \chi)|^2 &= \overline{\tau(\psi, \chi)}\tau(\psi, \chi) \\ &= \sum_{g \in G^\times} \sum_{g_1 \in G^\times} \overline{\psi(g)\chi(g)}\psi(g_1)\chi(g_1) \\ &= \sum_{g \in G^\times} \sum_{g_1 \in G^\times} \psi(g^{-1}g_1)\chi(g_1 - g) \end{aligned}$$

fazendo $g^{-1}g_1 = h$, E usando novamente o Teorema 1.1.(ii), tem-se

$$\begin{aligned}
|\tau(\psi,\chi)|^2 &= \sum_{g\in G^\times}\sum_{h\in G^\times}\psi(h)\chi(g(h-1)) \\
&= \sum_{h\in G^\times}\psi(h)\left(\sum_{g\in G}\chi(g(h-1)) - \chi(0_G)\right) \\
&= \psi(1)q + \sum_{h\neq 1_G\in G^\times}\psi(h)\sum_{g\in G}\chi(g(h-1)) \\
&= q.
\end{aligned}$$

□

O seguinte lema usa-se em diferentes momentos no que segue relacionado a somas exponenciais(*ver [3]*).

Lema 1.3. *Sejam M um inteiro positivo e f uma função real positiva definida sobre os inteiros módulo M, para $c_1,\ldots,c_r$ inteiros primos relativos com M, tem-se*

$$\sum_{n=1}^{M} f(nc_1)\cdots f(nc_r) \leq \sum_{n=1}^{M} f(n)^r.$$

Demonstração. Dado que c_i é primo relativo com M para $i = 1,\ldots,r$, tem-se

$$\sum_{n=1}^{M} f(nc_i) = \sum_{n=1}^{M} f(n) \text{ para } i = 1,\ldots,r.$$

Usando a desigualdade de Hölder, tem-se

$$\sum_{n=1}^{M} f(nc_1)\cdots f(nc_r) \leq \left(\sum_{n=1}^{M} f(nc_1)^r\right)^{1/r}\cdots\left(\sum_{n=1}^{M} f(nc_r)^r\right)^{1/r} = \sum_{n=1}^{M} f(n)^r.$$

□

Agora, ajustando estes conceitos ao propósito deste trabalho, para um primo p assuma $G = \mathbb{Z}/p\mathbb{Z}$ e seja ζ uma raiz p-ésima da unidade, além disso defina para $y\in\mathbb{Z}$ e para todo $\overline{x}\in G$

$$\chi_t(\overline{x}) = \zeta^{ty} \tag{1.4}$$

onde $t = 0,\ldots,p-1$ e $y\in\overline{x}$, isto é, a igualdade (1.4) mantém-se se, e somente se, $y\equiv x \pmod p$. Particularmente, tem-se $x\in\overline{x}$, assim por simplicidade escreve-se

$\chi_t(\overline{x}) = \chi_t(x)$. Logo, não é difícil comprovar que χ_t é um carácter aditivo de $\mathbb{Z}/p\mathbb{Z}$, onde o carácter trivial é precisamente χ_0. Por outro lado, considere a função

$$F(x_1, \dots, x_n) = a_1 x_1^k + \cdots + a_n x_n^k,$$

com $a_i \not\equiv 0 \pmod{p}$. Daí, o número de soluções $N(0) = N$ da congruência

$$F(x_1, \dots, x_n) \equiv 0 \pmod{p} \tag{1.5}$$

esta dado pela equação (1.1), ou seja, com x_i no conjunto de resíduos módulo p para $i = 1, \dots, n$, tem-se

$$\begin{aligned} N &= \frac{1}{p} \sum_{x_1,\dots,x_n} \sum_{t=0}^{p-1} \prod_{j=1}^{n} \zeta^{t a_j x_j^k} \\ &= p^{n-1} + \frac{1}{p} \sum_{t=1}^{p-1} \prod_{j=1}^{n} \sum_{x_j} \zeta^{t a_j x_j^k}. \end{aligned} \tag{1.6}$$

Daí, para $a \not\equiv 0 \pmod{p}$ é de interesse o comportamento de

$$\sum_{y} \zeta^{a y^k}.$$

Se $m(x)$ é o número de soluções da congruência $y^k \equiv x \pmod{p}$, tem-se que $m(0) = 1$ e

$$\sum_{y} \zeta^{a y^k} = \sum_{x} m(x) \zeta^{a x}.$$

Logo, para $x \not\equiv 0 \pmod{p}$, tem-se que se g é uma raiz primitiva módulo p, então existe r tal que

$$x \equiv g^r \pmod{p}, \tag{1.7}$$

onde r é único módulo $p - 1$. Disto, considere $y \equiv g^u \pmod{p}$, então a congruência $y^k \equiv x \pmod{p}$ é equivalente à congruência

$$ku \equiv r \pmod{p-1}, \tag{1.8}$$

assim, pelo teorema das congruências de primeiro grau a congruência (1.8) possui

$d = (k, p-1)$ soluções em u se d divide r, caso contrário não possui soluções, portanto

$$m(x) = \begin{cases} d & \text{se } r \equiv 0 \pmod{d}, \\ 0 & \text{se } r \not\equiv 0 \pmod{d}. \end{cases} \tag{1.9}$$

Por outro lado considere ϵ a d-éssima raiz primitiva da unidade e para todo inteiro x primo relativo com p defina a função

$$\psi_l(x) = \epsilon^{rl}$$

onde r é determinado por (1.7) e $l = 0, 1, \ldots, d-1$, e, dado que $\epsilon^{p-1} = 1$ o valor de ϵ^{rl} não depende da escolha de r. Se $r \equiv 0 \pmod{d}$, então $\epsilon^{rl} = 1$ para todo $s = 0, 1, \ldots, d-1$, assim

$$\sum_{l=0}^{d-1} \psi_l(x) = d.$$

Caso contrário, se $r \not\equiv 0 \pmod{d}$, tem-se $\epsilon^r \neq 1$ e

$$\sum_{l=0}^{d-1} \psi_l(x) = \frac{\epsilon^{rd} - 1}{\epsilon^r - 1} = 0.$$

Comparando (1.9) com o anterior para $x \not\equiv 0 \pmod{p}$, obtém-se

$$m(x) = \sum_{l=0}^{d-1} \psi_l(x).$$

Por outra parte, ψ_l satisfaz $\psi_l(xy) = \psi_l(x)\psi_l(y)$ o que o faz um carácter multiplicativo módulo p, com ψ_0 o carácter trivial. Por (1.4)

$$\begin{aligned} \sum_y \zeta^{ay^k} &= 1 + \sum_{x=1}^{p-1} \sum_{l=0}^{d-1} \psi_l(x)\chi_a(x) \\ &= 1 + \sum_{x=1}^{p-1} \chi_a(x) + \sum_{x=1}^{p-1} \sum_{l=1}^{d-1} \psi_l(x)\chi_a(x) \\ &= \sum_{x=0}^{p-1} \chi_a(x) + \sum_{x=1}^{p-1} \sum_{l=1}^{d-1} \psi_l(x)\chi_a(x), \end{aligned}$$

pelo Teorema 1.1 (ii), tem-se

$$\begin{aligned}\sum_{y}\zeta^{ay^k} &= \sum_{x=1}^{p-1}\sum_{l=1}^{d-1}\psi_l(x)\chi_a(x)\\ &= \sum_{l=1}^{d-1}\tau(\psi_l,\chi_a),\end{aligned}$$

onde $\tau(\psi_l,\chi_a)$ é a soma Gaussiana para G. Por outro lado, note que a igualdade acima depende apenas do inteiro a, assim, defina

$$S(a)=\sum_{l=1}^{d-1}\tau(\psi_l,\chi_a).$$

Substituindo em (1.6), obtém-se

$$N=p^{n-1}+\frac{1}{p}\sum_{t=1}^{p-1}\prod_{j=1}^{n}S(ta_j).$$

Outros resultados sobre caracteres e somas Gaussianas podem ser consultados em [2], [15], [20] e [25]. O seguinte resultado encontra-se de maneira mais generalizada em [2].

Teorema 1.4. *Seja N o número de soluções da congruência (1.5). Então para cada número primo p que não divide $a_1,\ldots,a_n$, tem-se para $d=(k,p-1)$*

$$\left|N-p^{n-1}\right|\leq(d-1)^n p^{\frac{n}{2}} \tag{1.10}$$

Demonstração. Primeiro, note que pelo Lema 1.3 tem-se

$$\sum_{t=1}^{p-1}|S(ta_1)\cdots S(ta_n)|\leq\sum_{t=1}^{p-1}|S(t)|^n,$$

e dado que $|S\,(t)|\leq(d-1)p^{1/2}$ por (1.3), tem-se

$$\sum_{t=1}^{p-1}|S(ta_1)\cdots S(ta_n)|\leq(p-1)(d-1)^n p^{\frac{n}{2}}, \tag{1.11}$$

logo

$$\begin{aligned}\left|N - p^{n-1}\right| &\leq \frac{1}{p}\sum_{t=1}^{p-1}|S(ta_1)\cdots S(ta_n)| \\ &\leq (p-1)(d-1)^n p^{\frac{n}{2}-1} \\ &\leq (d-1)^n p^{\frac{n}{2}}.\end{aligned}$$

□

Note que (1.10) estabelece uma condição suficiente para garantir a solubilidade da congruência (1.5), isto é,

$$N \geq p^{n-1} - (d-1)^n p^{\frac{n}{2}} \geq 1.$$

Este resultado pode ser melhorado fazendo a seguinte consideração: Seja $(z_1, \ldots, z_n)$ uma solução para (1.5), onde não todo $z_i \equiv 0 \pmod p$ para $i = 1, \ldots, n$. Assuma, sem perda de generalidade, que $z_n \not\equiv 0 \pmod p$, então $(z_1 z_n^{-1}, \ldots, 1)$ é solução para

$$F(x_1, \ldots, 1) = a_1 x_1^k + \cdots + a_{n-1} x_{n-1}^k + a_n \equiv 0 \pmod p. \tag{1.12}$$

Portanto, (1.5) possui solução se, e somente se, (1.12) possui solução. Daí, Dodson [9] mostra o seguinte Lema, usando este arraçoamento e um argumento semelhante ao feito para calcular o número de soluções no Teorema 1.4.

Lema 1.5. *Considere a congruência (1.5). Se p é um primo que não divide k e $(a_i, p) = 1$ para $i = 1, \ldots, n$, então (1.5) possui uma solução primitiva, sempre que*

$$p > (d-1)^{(2n-2)/(n-2)} \tag{1.13}$$

onde $d = (k, p-1)$.

Agora, apresenta-se aqui um outro critério sob a existência de soluções primitivas de (1.5) dado por Bovey [3]. Para isto, note que (1.4) é independente da escolha da raiz primitiva, assim fazendo $\zeta^x = \exp(2\pi i x/p) = e_p(x)$, tem-se

$$S(a) = \sum_{x=0}^{p-1} e_p(ax^k)$$

Suponha que a congruência (1.5) só possui a solução trivial, isto implica

$$\sum_{x_1,\ldots,x_n}\sum_{t=0}^{p-1} e_p(ta_1x_1^k)\cdots e_p(ta_nx_n^k) = p$$

Substituindo em termos de $S(a)$, tem-se

$$\sum_{t=1}^{p-1} S(ta_1)\cdots S(ta_n) = p - p^n$$

Aplicando a norma à igualdade acima, e usando o Lema 1.3, tem-se

$$\sum_{t=1}^{p-1} |S(t)|^n \geq p^n - p$$

logo, obtém-se o seguinte Lema devido a Bovey [3], definindo para $n > 1$ a função

$$Q(k,p,n) := \sum_{t=1}^{p-1} \frac{|S(t)|^n}{p^n - p}. \tag{1.14}$$

Lema 1.6. *Sejam k, p e n inteiros positivos dados, com p um primo que não divide k. Além disso considere a congruência (1.5) com todos os coeficientes primos relativos a p. Se $Q(k,p,n) < 1$, então*

$$\Gamma^*(k,p) \leq k(n-1) + 1.$$

1.2 p-Normalização e Contração de Variáveis

Uma parte essencial do trabalho de Davenport e Lewis em [8], consiste em reescrever uma forma aditiva a fim de obter uma forma equivalente, para isto é necessário o seguinte Lema:

Lema 1.7. *Sejam $m_0, m_1, \ldots, m_{k-1}$ números reais, tais que $m_{k+j} = m_j$ para todo inteiro j. Além disso, considere*

$$\sum_{i=0}^{k-1} m_i = s.$$

Então, existe r tal que

$$\sum_{i=r}^{r+j} m_{r+i} \geq (j+1)\,\frac{s}{k}. \tag{1.15}$$

para todo $j = 0, \ldots, k-1$.

Assuma $s = 0$, pois caso contrário basta considerar $m_i^{'} = m_i - s/k$. Agora, assuma que não existe r satisfazendo o Lema, isto é, assuma que para quaisquer $a \in \mathbb{N}$ existe $b \geq a$ tal que $m_a + m_{a+1} + \cdots + m_b < 0$. Desta maneira, seja a_1, b_1 inteiros satisfazendo o anterior, além disso, considere $a_2 = b_1 + 1$, assim pode-se encontrar o correspondente b_2, desta maneira construi-se uma sequencia infinita $(a_1, b_1), (a_2, b_2), \ldots$ com $\sum m_i$ negativo. Desta maneira, pelo principio da casa dos pombos existe n tal que $a_1 \equiv a_n \pmod{k}$. Mas, isto é uma contradição, pois

$$\sum_{a_1}^{a_n - 1} m_i = \frac{a_n - a_1}{k} s = 0.$$

Lema 1.8. *Toda forma aditiva de grau k em s variáveis,*

$$\mathscr{F} = a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k, \tag{1.16}$$

com coeficientes inteiros, é equivalente a uma forma

$$\mathscr{F}_0 + p\mathscr{F}_1 + \cdots + p^{k-1}\mathscr{F}_{k-1}, \tag{1.17}$$

onde cada $\mathscr{F}_j$ é uma forma diagonal com coeficientes inteiros em m_j variáveis com todos os seus coeficientes não divisíveis por p. Ainda mais, tem-se

$$s = \sum_{i=0}^{k-1} m_i \quad e \quad m_0 + \cdots + m_j \geq (j+1)\frac{s}{k}, \tag{1.18}$$

para $j = 0, \ldots, k-1$. Uma forma satisfazendo estas propriedades é dita de p-normalizada, e para cada $0 \leq i \leq k$ diz-se que as variáveis da forma $\mathscr{F}_i$ estão no nível i.

Demonstração. Fatorizando a maior potencia prima p em cada um dos coeficientes de $\mathscr{F}$, tem-se

$$\mathscr{F} = \sum_{i \geq 0} p^i \mathscr{F}_i,$$

donde cada $\mathscr{F}_i$ é uma forma com coeficientes não divisíveis por p. Ainda mais, para $i \geq k$, tem-se $i = kt + r$ com $0 \leq r < k$, então basta fazer substituição das variáveis x do nível i, por $x = p^t x'$ para obter novas variáveis no nível r, desta forma obtém-se

$$\mathscr{F} = \mathscr{F}_0 + p\mathscr{F}_1 + \cdots + p^{k-1}\mathscr{F},$$

assim sem perda de generalidade, pode-se assumir que $x_1, \ldots, x_{s_j}$ são as variáveis dos níveis $0, 1, \ldots, j$, para $j = 0, 1, \ldots, k-1$. Agora, seja m_i o número de variáveis em $\mathscr{F}_i$ e note que

$$m_0 + m_1 + \cdots + m_{k-1} = s,$$

logo pelo Lema 1.7, existe r tal que é satisfeita a desigualdade (1.15). Daí, considere a forma

$$\mathscr{F}^{(r)} = \frac{1}{p^r} \cdot \mathscr{F}(px_1, px_2, \ldots, px_{s_{r-1}}, x_{s_{r-1}+1}, \ldots, x_s), \tag{1.19}$$

onde $x_1, \ldots, x_{s_{r-1}}$ são as variáveis do nível 0 até o nível $r-1$. Denotando $m_i^{(r)}$ como o número de variáveis da forma $\mathscr{F}^{(r)}$ no nível i, então tem-se

$$\sum_{i=0}^{j} m_i^{(r)} \geq (j+1)\left(\frac{s}{k}\right)$$

para $j = 0, \ldots, k-1$. De (1.19) é claro que $\mathscr{F}^{(r)}$ possui zeros p-ádicos se, e somente se, $\mathscr{F}$ os possui, portanto pode-se supor

$$\mathscr{F} = \mathscr{F}_0 + p\mathscr{F}_1 + \cdots + p^{k-1}\mathscr{F}_{k-1},$$

satisfazendo (1.18). □

A partir deste ponto fixa-se a seguinte notação: Denota-se $\mathscr{F}$ a forma aditiva p-normalizada de grau k em s variáveis escrita como em (1.16) e (1.18), e com todas as propiedades descritas no Lema 1.8. Alem disso, seja p um número primo e escreva $k = p^\tau k_0$ com $(p, k_0) = 1$. Defina

$$\gamma = \begin{cases} \tau + 1 & \text{se } \ p > 2, \ \text{ ou } \ p = 2 \ \ e \ \ \tau = 0. \\ \tau + 2 & \text{se } \ p = 2. \end{cases} \tag{1.20}$$

Se $\mathscr{F} = 0$ possui soluções nos inteiros, então a congruência $\mathscr{F} \equiv 0 \pmod{m}$ possui solução para todo m, mas a recíproca não é necessariamente verdadeira. Em este sentido, foram estabelecidos alguns métodos na procura de encontrar condições para que a recíproca seja satisfeita e um deles é o Lema de Hensel, como segue:

Lema 1.9 (Lema de Hensel)**.** *Sejam $\mathscr{F}$ uma forma como em (1.16) e p um primo, tal que $k = p^\tau k_0$, onde $p \nmid k_0$. Suponha que $\mathbf{z} \in \mathbb{Z}^s$ satisfaz $\mathscr{F}(\mathbf{z}) \equiv 0 \pmod{p^\gamma}$ com pelo menos uma variável no nível 0 não divisível por p. Então, $\mathscr{F}$ tem zeros p-ádicos* *não triviais, em outras palavras, existe* $\mathbf{y} \in \mathbb{Z}_p^s$ *tal que* $\mathbf{y} \equiv \mathbf{z} \pmod{p}$ *e* $\mathscr{F}(\mathbf{y}) = 0$ *em* $\mathbb{Q}_p$.

Em virtude do Lema de Hensel 1.9, se para uma forma aditiva $\mathscr{F}$ é possível fazer uma substituição das variáveis do nível 0, de tal maneira que o resultado de dita substituição seja um múltiplo de p^γ tem-se que $\mathscr{F}$ tem um zero p-ádico não trivial. Assim, apresenta-se a contração de variáveis, o qual consiste em um processo iterado de substituição de variáveis de um nível l, com $l \geq 0$ a um nível $l + j$ para j um inteiro positivo. Começa-se com o seguinte resultado.

Teorema 1.10 (Teorema de Warning)**.** *Se o grau do polinômio* $F(x_i, \ldots, x_n)$ *é menor que* n, *então o número de soluções da congruência* $F(x_i, \ldots, x_n) \equiv 0 \pmod{p}$ *é divisível por* p.

Demonstração. Suponha que a congruência $F(x_i, \ldots, x_n) \equiv 0 \pmod{p}$ possui s soluções $Y_i = (y_{1,i}, \ldots, y_{n,i})$ com $i = 1, \ldots, s$. Defina $H = 1 - F^{p-1}$, então H satisfaz para $X = (x_1, \ldots, x_n)$:

$$H(X) = \begin{cases} 1 & \text{se } \; X \equiv Y_i \pmod{p}, \\ 0 & \text{se } \; X \not\equiv Y_i \pmod{p}, \end{cases}$$

para algum $i = 1, \ldots, s$. Agora, para quaisquer $Y = (y_1, \ldots, y_n)$ defina

$$D_Y(x_1, \ldots, x_n) = \prod_{j=1}^{n} \left(1 - (x_j - y_j)^{p-1}\right).$$

Logo, pelo pequeno Teorema de Fermat, tem-se

$$D_Y(X) = \begin{cases} 1 & \text{se } \; X \equiv Y \pmod{p}, \\ 0 & \text{se } \; X \not\equiv Y \pmod{p}. \end{cases} \tag{1.21}$$

Assim, seja

$$H^*(X) = D_{Y_1}(X) + \cdots + D_{Y_s}(X),$$

de (1.21) resulta que $H^*(X) \equiv H(X) \pmod{p}$ para toda n-upla X com entradas nos inteiros. Logo, o grau de H^* não excede o grau de H que é menor que $n(p-1)$ e isto se deve, novamente, ao pequeno Teorema de Fermat. Em cada D_{Y_t} existe um termo de grau $n(p-1)$, a saber, o termo $(-1)^n (x_1 \cdots x_n)^{p-1}$. Como o grau de H^*

é estritamente menor que $n\,(p-1)$ necessariamente deve ter $s \equiv 0 \pmod p$, como queria ser mostrado. $\square$

Este teorema generaliza o Teorema de Chevalley [5] sobre a existência de soluções para funções polinomiais módulo primo. Um fato bem conhecido é: $x^k \equiv m \pmod p$ tem solução se, e somente se, $x^d \equiv m \pmod p$ possui solução, onde $d = (k, p-1)$. Usando o Teorema 1.10 e o fato anterior, segue o seguinte lema

Lema 1.11. *Seja $d = (k, p-1)$ e suponha que $a_1 \cdots a_n \not\equiv 0 \pmod p$. Então, a congruência*

$$a_1 x_1^k + \cdots + a_n x_n^k \equiv 0 \pmod p$$

possui solução com pelo menos uma variável não divisível por p, desde que $n > d$.

Uma prova do lema anterior, sem usar o Teorema 1.10 pode ser encontrada em [8]. Trata-se aqui o método de contração de variáveis, o qual faz uso do Lema 1.11 para substituir variáveis de um nível i da forma aditiva $\mathscr{F}$ a um nível $j > i$. Com isto, a forma de contrair variáveis acontece como segue: Se $k = p^\tau k_0$, e $\tau = 0$, então a congruência

$$a_1 x_1^k + a_{d+1} x_{d+1}^k \equiv 0 \pmod p,$$

com $a_1 a_2 \cdots a_{d+1} \not\equiv 0 \pmod p$, isto é, variáveis do nível 0, tem uma solução com $x_1 \not\equiv 0 \pmod p$. Agora, para $\tau > 0$, considere uma soma

$$b_1 y_1^k + \cdots + b_{d+1} y_{\delta+1}^k \tag{1.22}$$

onde $b_1 \cdots b_{d+1} \not\equiv 0 \pmod p$. Uma das variáveis $y_1, \ldots, y_{d+1}$ se distingue das outras, e vai-se supor que seja y_1. Pelo Lema 1.11, tem-se uma solução

$$b_1 c_1^k + \cdots + b_{d+1} c_{d+1}^k \equiv 0 \pmod p,$$

com $c_1 \not\equiv 0 \pmod p$. Ao escolher a solução adequadamente, pode-se supor que não é nula, e que pode ser escrita da forma

$$b_1 c_1^k + \cdots + b_{d+1} c_{d+1}^k = p^g e,$$

com $g \geq 1$ e $p \nmid e$. Substituindo $y_i = c_i z$ em (1.22), obtém-se um só termo da forma $p^g e z$, e é importante que $z \not\equiv 0 \pmod p$, pois implica que $y_1 \not\equiv 0 \pmod p$, onde y_1

é a variável distinguida.

É aplicada a contração, primeiro a grupos de $d+1$ termos no nível 0, e qualquer variável restante não contida nos diferentes grupos é igualada a zero. Isto da uma forma do tipo

$$p\mathscr{G}_1 + p^2\mathscr{G}_2 + \cdots$$

onde $\mathscr{G}_j$ tem os v_j termos originais de $\mathscr{F}_j$ mas alguns outros termos, resultado da contração. Os termos adicionais são chamados de variáveis derivadas.

A seguinte contração se aplica a $\mathscr{G}_1$, com a condição de que cada conjunto de $d+1$ termos, tenha pelo menos um termo derivado e dita variável é escolhida como a variável distinguida na contração. O processo segue sempre levando uma variável derivada da contração anterior, isto leva de maneira direta ou indireta uma variável do nível 0 da forma $\mathscr{F}$. Dado que o número de variáveis da forma aditiva $\mathscr{F}$ é finita, tem-se que o processo eventualmente para, e é achada uma forma aditiva

$$\mathscr{H} = p^{\mu}\mathscr{H}_{\mu} + p^{\mu+1}\mathscr{H}_{\mu+1} + \cdots \tag{1.23}$$

onde a congruência $\mathscr{H} \equiv 0 \pmod{p^{\gamma}}$ tem uma solução com pelo menos uma variável derivada não divisível por p. Em particular, para $j = 0, 1, \ldots$, quaisquer das formas $\mathscr{H}_{\mu+j}$ contem uma variável derivada, assim, pode-se tomar uma destas variáveis derivadas como 1, e todas as outras variáveis como zero. Isto implica que $\mathscr{F} \equiv 0 \pmod{p^{\gamma}}$ tem uma solução com pelo menos una variável do nível 0 não divisível por p, esta solução é chamada de solução primitiva.

Capítulo

2

Solubilidade, Teorema 0.1 e Teorema 0.2.

O propósito deste capítulo é estabelecer algumas condições para achar zeros p-ádicos não triviais de uma forma aditiva $\mathscr{F}$ de grau k em s variáveis, como também, mostrar os Teoremas 0.1 e 0.2. Para isto, neste trabalho é assumida a hipótese especial de que -1 é sempre uma k-ésima potência módulo p^{γ}.

2.1 Solubilidade.

Já tinha-se visto no método de contração de variáveis a importância do Lema 1.9, na procura de zeros p-ádicos não triviais, embora, isto implica a existência de uma variável coprima com p no nível 0. Uma versão mais geral é dada por Godinho, Knapp, Rodriguez, Veras em [11], como segue:

Lema 2.1. *Suponha que para algum $n \in \mathbb{N} \cup \{0\}$ existe um $\mathbf{z}_n \in \mathbb{Z}^s$ tal que*

$$\mathscr{F}(\mathbf{z}_n) \equiv 0 \pmod{p^{\gamma+n}} \tag{2.1}$$

com pelo menos uma entrada de $\mathbf{z}_n$ correspondendo a uma variável do nível j em (1.17), coprima com p, onde $j \leq n$. Então, $\mathscr{F}$ tem zeros p-ádicos não triviais e, esta solução será chamada de solução não singular módulo $p^{\gamma+n}$.

Demonstração. Se $n = 0$, o resultado é imediato do Lema 1.9. Agora, suponha que $n \geq 1$, por hipótese, $\mathbf{z}_n \in \mathbb{Z}^s$ possui uma entrada coprima com p para algum nível j, com $j \leq n$. Assim, assuma j como o menor inteiro para o qual é satisfeita a hipótese, e fazendo uma permutação cíclica como em (1.19) de $\mathscr{F}$ a $\mathscr{F}^{(j)}$, pode-se aplicar o Lema 1.9 a esta ultima forma aditiva e o resultado segue como no caso $n = 0$. $\square$

Agora, o objetivo é determinar soluções não singulares módulo $p^{\gamma+n}$, para algum $n \geq 0$. Para isto, defina

$$\gamma^* = \lfloor \gamma \log_2 (p) \rfloor + 1. \tag{2.2}$$

Começa-se com o seguinte lema.

Lema 2.2. *Se $m = m_0 + \cdots + m_{\gamma-1} \geq \gamma^*$, então a congruência*

$$\mathscr{F} \equiv 0 \pmod{p^\gamma} \tag{2.3}$$

tem soluções não triviais.

Demonstração. Escreva $\mathscr{F} = b_1 x_1^k + \cdots + b_m x_m^k \pmod{p^\gamma}$ e considere todas as somas possíveis parciais de seus coeficientes, ou seja,

$$b_i, b_i + b_j, b_i + b_j + b_l, \ldots, b_1 + b_2 + \cdots + b_m.$$

Observe que há $2^m - 1$ possíveis somas. Se uma dessas somas for congruente com 0 módulo p^γ, tem-se o resultado. Se duas dessas somas, $\sum_i b_i$ e $\sum_j b_j$, são congruentes módulo p^γ, então removendo as parcelas iguais de ambas somas, obtém-se duas somas, $\sum_i' b_i$ e $\sum_j' b_j$, onde todo $b_i \neq b_j$. Logo, como é assumido que -1 é uma k-ésima potência, basta substituir $x_i^k = 1$ se b_i é uma parcela de $\sum_i' b_i$ e $x_j^k = -1$ se b_j é uma parcela de $\sum_j' b_j$, obtendo assim uma solução para (2.3). Agora, se todas as parcelas são distintas e não nulas módulo p^γ, isso implica que $2^m - 1 < p^\gamma$, mas isso contradiz a hipótese que $m \geq \gamma^*$. O que completa a demonstração. $\square$

O Lema anterior, fornece apenas soluções não triviais, em este sentido, o seguinte Lema proporciona um critério para encontrar soluções não singulares módulo p^γ de uma forma aditiva, e portanto, zeros p-ádicos não triviais.

Lema 2.3. *Seja $m_0 + \cdots + m_{\gamma-1} \geq \gamma^*$ e escreva (ver (1.17))*

$$\mathscr{F} \equiv \mathscr{F}_0 + p\mathscr{G} \pmod{p^\gamma}.$$

Se $\mathscr{G} \equiv 0 \pmod{p^\gamma}$ somente tem solução trivial, então a congruência (2.3) tem solução não singular módulo p^γ.

Demonstração. Do Lema 2.2 segue que a congruência (2.3) tem soluções não triviais. Como por hipótese $\mathscr{G} \equiv 0 \pmod{p^\gamma}$ tem somente a solução trivial, então esta solução não trivial da congruência (2.3) deve necessariamente incluir variáveis não nulas do nível 0, ou seja, é uma solução não singular módulo p^γ. □

A ideia de encontrar soluções não singulares módulo p^γ podem ser usadas para encontrar soluções não singulares módulo $p^{\gamma+n}$ com n um inteiro positivo, em virtude do Lema 2.1 como segue.

Lema 2.4. *Seja $\mathscr{F}$ uma forma aditiva p-normalizada de grau k em s variáveis. Em cada um dos seguintes casos $\mathscr{F}$ tem zeros p-ádicos não triviais.*

(i). $m_i \geq \gamma^*$ *para algum* $i \in \{0, 1, \dots, k-1\}$;

(ii). *Existe* $r \in \{1, 2, \dots, \gamma - 1\}$ *tal que pode-se escolher* $i \in \{0, 1, \dots, k-r-1\}$ *e* r *índices distintos* $j_l \in \{i+1, i+2, \dots, i+\gamma-1\}$ *com* $m_i \geq \gamma^* - r$ *e* $m_{j_l} \geq 1$ *para* $l = 1, 2, \dots, r$.

Demonstração. Se $m_i \geq \gamma^*$ segue do Lema 2.2 que $\mathscr{F}_i \equiv 0 \pmod{p^\gamma}$ tem solução não trivial com $\mathbf{x}_i = (x_1, \dots, x_m)$ módulo p^γ, cujas entradas são coprimas com p. Agora, considere $\mathbf{0}_j$ a m_j-upla de zeros para $0 \leq j \leq k-1$ e $j \neq i$, daí considere $\mathbf{x} = (\mathbf{0}_0, \dots, \mathbf{x}_i, \mathbf{0}_{i+1}, \dots, \mathbf{0}_{k-1}) \in \mathbb{Z}^s$, e observe que

$$\mathscr{F}(\mathbf{x}) = \mathscr{F}_0(\mathbf{0}_0) + \cdots + p^i \mathscr{F}_i(\mathbf{x_i}) + \cdots + p^{k-1}\mathscr{F}_{k-1}(\mathbf{0}_{k-1}) \equiv 0 \pmod{p^{\gamma+i}}.$$

Logo, o resultado segue do Lema 2.1. Agora, para caso (ii), seja $m_i \geq \gamma^* - r$ e suponha que existem níveis $j_l \in \{i+1, i+2, \dots, i+\gamma-1\}$ como na hipótese. Escreva $j_l - i = t_l$ para $l = 1, \dots, r$ e a $\mathscr{G}$ como sendo uma forma aditiva com uma variável de cada um dos níveis j_l, assim,

$$\mathscr{G} = p^{t_1-1} a_{j_1} x_{j_1}^k + \cdots + p^{t_r-1} a_{j_r} x_{j_r}^k,$$

assim, a congruência $\mathscr{G} \equiv 0 \pmod{p^{\gamma-1}}$ somente possui soluções triviais, então pelo Lema 2.2 a congruência

$$\mathscr{F}_i + p\mathscr{G} \equiv 0 \pmod{p^\gamma}$$

possui soluções não singulares módulo p^γ, o que implica por um argumento semelhante ao caso anterior, que $\mathscr{F}$ possui soluções não singulares módulo $p^{\gamma+i}$, como queria ser mostrado. □

Note que fazendo $i = 0$ no caso (i) do Lema anterior, obtém-se o Lema 3.2.1 de [9]. Além disso, o seguinte Lema, o qual é o Lema 5 de Knapp [16], é uma consequência direta do Lema 2.4.

Lema 2.5. *Seja $\mathscr{F}$ uma forma aditiva p-normalizada de grau k, com -1 sendo uma k-ésima potência módulo p^γ. Se existem n variáveis no nível 0, tais que $2^n > p^\gamma$, então $\mathscr{F}$ tem zeros p-adicos não triviais.*

2.2 Teorema 0.1.

De maneira preliminar, mostra-se o seguinte Lema que permite demonstrar o Teorema 0.1

Lema 2.6. *Sejam p um primo, $t = p^r + 1$ e $a_1, \dots, a_t$ uma sequência de inteiros coprimos com p. Suponha que para todo par i, j com $1 \leq i < j \leq t$ tem-se*

$$a_i \equiv a_j \pmod{p^{\gamma-r}} \quad \textit{ou} \quad a_i \equiv -a_j \pmod{p^{\gamma-r}}. \tag{2.4}$$

Então, existem $i, j \in \{1, \dots, t\}$ com $i \neq j$ tal que

$$a_i \equiv a_j \pmod{p^\gamma} \quad \textit{ou} \quad a_i \equiv -a_j \pmod{p^\gamma}.$$

Demonstração. Fixando a_1 considere o conjunto $C = \{a_2, a_3, \dots, a_t\}$. Por (2.4), tem-se que C é a união disjunta dos conjuntos

$$A = \{a_i \in C;\ a_i \equiv a_1 \pmod{p^{\gamma-r}}\}$$

e

$$B = \{a_i \in C;\ a_i \equiv -a_1 \pmod{p^{\gamma-r}}\}.$$

Ainda mais, $a_i \in A$ se, e somente se,

$$a_i \equiv a_1 + b_i p^{\gamma-r} \pmod{p^\gamma}$$

com $b_i \in \{0, 1, 2, \dots, t-2\}$. Similarmente, $a_i \in B$ se, e somente se,

$$a_i \equiv -a_1 + b_i p^{\gamma-r} \pmod{p^\gamma},$$

com $b_i \in \{0, 1, 2, \dots, t-2\}$. Se para algum $a_i \in C$, tem-se $b_i = 0$ o problema já está resolvido, portanto, assuma $b_i \neq 0$ para todo $a_i \in C$. Assim, são analisados os seguintes casos:

- Se $|A| = t-1$ (ou $|B| = t-1$), então pelo principio da casa dos pombos pode-se escolher $a_i, a_j \in A$ com $b_i = b_j$, logo $a_i \equiv a_j \pmod{p^\gamma}$.
- Se $1 \leq |A| \leq t-2$, então $|B| = |C| - |A| \geq 1$. Se acontece que é possível escolher $a_i = a_j \in A$ (ou B) com $b_i = b_j$ procede-se como no anterior caso. Caso contrário, novamente pelo principio da casa dos pombos, existem $a_i \in A$ e $a_j \in B$ tais que $b_i \equiv -b_j \pmod{p^r}$, tem-se assim $a_i + a_j \equiv 0 \pmod{p^\gamma}$, ou seja,
$$a_i \equiv -a_j \pmod{p^\gamma}.$$

Daí, em quaisquer dos casos obtém-se

$$a_i \equiv a_j \pmod{p^\gamma} \;\text{ ou }\; a_i \equiv -a_j \pmod{p^\gamma}.$$

□

Teorema 0.1. *Seja $k = p^\tau (p-1)/2$. Se $\gamma^* - 4 \geq p$ então,*

$$\Gamma^*(k,p) \leq k(\gamma^* - 3) + 1.$$

Demonstração. Seja $\mathscr{F}$ uma forma aditiva de grau k em s variáveis. Suponha que $s \geq k(\gamma^* - 3) + 1$, $\gamma^* \geq p + 4$ e $d = (k, p-1) = (p-1)/2$. Dado que $d = (p-1)/2$, tem-se que o conjunto $\mathbb{K}$ das k-ésimas potências módulo p^γ é igual a $\mathbb{K} = \{-1, 0, 1\}$. Alem disso, pode-se assumir que $\mathscr{F}$ é p-normalizada, com as propriedades descritas no Lema 1.8. Logo, tem-se que

$$m_0 + \cdots + m_j \geq (j+1)(\gamma^* - 3) + 1. \tag{2.5}$$

Se $m_0 \geq \gamma^*$, segue do Lema 2.4 que $\mathscr{F}$ possui zeros p-ádicos não triviais . Por outra parte, se $m_0 = \gamma^* - 1$, então de (2.5) segue que $m_0 + m_1 \geq 2(\gamma^* - 3) + 1$, assim, por hipótese $m_1 \geq \gamma^* - 4 \geq p$, em particular $m_1 \geq 1$, e novamente o resultado segue do caso (ii) do Lema 2.4. Finalmente, assuma que $m_0 = \gamma^* - 2$, logo, de (2.5) tem-se que $m_1 \geq \gamma^* - 3 \geq p + 1$. Considere a seguinte congruência, com $t = p + 1$

$$\mathscr{F}_0 + p\left(b_1 x_1^k + \cdots + b_t x_t^k\right) \equiv 0 \pmod{p^\gamma} \tag{2.6}$$

com $b_1, \ldots, b_t$ inteiros coprimos com p. Se existem índices i, j tais que a congruência $p\left(b_i x_i^k + b_j x_j^k\right) \equiv 0 \pmod{p^\gamma}$ não tem soluções não triviais, segue assim do Lema 2.3 que a congruência (2.6) possui soluções não singulares módulo p^γ. Agora, suponha que para todo $i, j \in \{1, \ldots, t\}$, a congruência (2.6) tem soluções não triviais. Como $\mathbb{K} = \{-1, 0, 1\}$, implica que, $b_i \equiv b_j \pmod{p^{\gamma-1}}$ ou $b_i \equiv -b_j \pmod{p^{\gamma-1}}$. Assim segue do Lema 2.6 que existe i, j tal que

$$b_i \equiv b_j \pmod{p^\gamma} \quad \text{ou} \quad b_i \equiv -b_j \pmod{p^\gamma},$$

ou seja,

$$p\mathscr{F}_1 = p\left(b_1 x_1^k + \cdots + b_t x_t^k\right) \equiv 0 \pmod{p^{\gamma+1}}$$

tem solução não trivial. Mas, isso é suficiente para obter um zero p-ádico não trivial para $\mathscr{F}$, pelo Lema 2.1. Com isto, tem-se que

$$\Gamma^*(k, p) \leq k(\gamma^* - 3) + 1.$$

Como se queria mostrar. □

2.3 Teorema 0.2.

O objetivo desta secção é mostrar o Teorema 0.2, para isso é essencial o Lema 2.4 o que implica assumir que -1 é uma k-ésima potência modulo p^γ. Também, são importantes as condições de p-normalização dadas pelo Lema 1.8. Assim, daqui em diante para $\tau \geq 1$ assuma $\mathscr{F}$ uma forma aditiva p-normalizada de grau $k = p^\tau k_0$ em s variáveis, com $p \nmid k_0$ e $s \geq k(\gamma^* - \gamma) + 1$. Logo, $\mathscr{F}$ satisfaz (1.18), isto é,

$$m_0 + \cdots + m_j \geq (j + 1)(\gamma^* - \gamma) + 1. \tag{2.7}$$

Agora, assuma que $m_0 = \gamma^* - t$ para $0 \leq t \leq \tau$, é claro pelo Lema 2.4 que se $m_i \geq \gamma^*$ para algum $0 \leq i \leq k-1$, a forma $\mathscr{F}$ possui uma solução não singular módulo $p^{\gamma+i}$, portanto de aqui em diante é assumido $1 \leq t$.

Proposição 2.1. *Seja $\mathscr{F}$ uma forma aditiva de grau $k = p^\tau k_0$ em s variáveis, com $s \geq k(\gamma^* - \gamma) + 1$ e tal que -1 é uma potência k-ésima modulo p^γ. Se $\tau \in \{1, 2\}$, então*

$$\Gamma^*(k, p) \leq k(\gamma^* - \gamma) + 1.$$

Demonstração. Para mostrar a primeira parte da Proposição, se $\tau = 1$ e $m_0 = \gamma^* - 1$, tem-se de (2.7) que $m_1 \geq \gamma^* - 2 \geq 1$, pois $p \geq 3$. Do Lema 2.4 tem-se que $\mathscr{F}$ possui zeros p-ádicos não triviais. Isto implica que

$$\Gamma^*(k,p) \leq k(\gamma^* - 2) + 1.$$

Agora, para $\tau = 2$ e $m_0 = \gamma^* - 1$, tem-se de (2.7) $m_1 \geq \gamma^* - 4 \geq 1$ e novamente, pelo Lema 2.4 a forma aditiva $\mathscr{F}$ possui zeros p-ádicos não triviais. Se $m_0 = \gamma^* - 2$ obtém-se de (2.7)

$$m_1 + m_2 \geq 2\,(\gamma^* - 3) > \gamma^* - 1, \tag{2.8}$$

para $p \geq 5$, isto implica que existem pelo menos dois níveis com pelo menos uma variável, portanto, pelo Lema 2.4 a forma $\mathscr{F}$ possui solução não singular módulo p^3. Dado que $\mathscr{F}$ possui solução para $m_0 = \gamma^* - t$ quando $t \in \{0, 1, 2\}$ tem-se

$$\Gamma^*(k,p) \leq k(\gamma^* - 3) + 1. \tag{2.9}$$

Agora, quando $p = 3$, tem-se $\gamma^* = 5$ e $m_0 = 3$. Se existem dois níveis com variáveis o resultado segue do Lema 2.4, assim, assuma que apenas um nível possui pelo menos $2\,(\gamma^* - 3) = 4$ variáveis, dado que pela 3-normalização $m_0 + m_1 \geq 5$, segue que $m_2 \geq 2$ e portanto as 4 variáveis anteriormente mencionadas devem estar no nível 1. Por outra parte, note que a condição $\gamma^* \geq p - 4$ no Teorema 0.1 serve assegurar a existência de $p + 1$ variáveis no nível 1, a qual em este caso pode ser omitida, já que $m_1 = 4$. Portanto, pelo Teorema 0.1 tem-se uma solução 3-ádica não trivial, isto implica que para $p = 3$ também é satisfeito (2.9). $\square$

Proposição 2.2. *Seja $\mathscr{F}$ uma forma aditiva de grau $k = p^\tau k_0$ em s variáveis, com $s \geq k(\gamma^* - \gamma) + 1$ e tal que -1 é uma k-ésima potência modulo p^γ. Se $m_0 = \gamma^* - t$, com $t \in \{1, 2\}$, então $\mathscr{F}$ tem um zero p-ádico quando $\tau \geq 3$.*

Demonstração. Assuma-se que $\tau \geq 3$, $\mathscr{F}$ uma forma aditiva como na hipótese e $\gamma^* - 1 \leq m_0 \leq \gamma^* - 2$. Primeiro, tome $\tau = 3$, e considere o número de variáveis do nível 1 ao nível 3 assim, tem-se que

$$\begin{aligned}\sum_{i=1}^{3} m_i &\geq 4\left(\gamma^* - \gamma\right) + 1 - m_0 \\ &\geq 3\gamma^* - 4\gamma + 2 \\ &\geq \gamma^* - 1,\end{aligned}$$

A ultima desigualdade é mantida para todo $p \geq 3$, isto implica que, existem pelo menos dois níveis, com pelo menos uma variável e, portanto, do Lema 2.4, tem-se que $\mathscr{F}$ tem um zero 3-ádico não trivial. Agora, tome $\tau \geq 4$, de maneira análoga ao caso anterior, considere os níveis 1 a 4. Da p-normalização, tem-se que

$$\begin{aligned}\sum_{i=1}^{4} m_i &\geq 5\left(\gamma^* - \gamma\right) + 1 - m_0 \\ &\geq 4\gamma^* - \gamma + 2 \\ &\geq \gamma^* - 1,\end{aligned}$$

esta ultima desigualdade é satisfeita para todo primo $p \geq 3$, portanto, existem pelo menos dois níveis, com pelo menos uma variável e o resultado segue pelo Lema 2.4.

□

Pelas Proposições 2.1 e 2.2, assume-se $\tau \geq 3$, $t \geq 3$ e mostra-se o seguinte Lema.

Lema 2.7. *Seja $\mathscr{F}$ uma forma aditiva de grau $k = p^\tau k_0$ em s variáveis, com $s \geq k(\gamma^* - \gamma) + 1$ e tal que -1 é uma k-ésima potência modulo p^γ. Para $\tau \geq 3$, se $m_0 = \gamma^* - t$ e*

$$t \leq \frac{\gamma(\gamma^* - \gamma) - 1}{\gamma^* - 3}, \tag{2.10}$$

então $\mathscr{F}$ possui um zero p-ádico não trivial.

Demonstração. Considere $\mathscr{F}$ uma forma $p-$normalizada e $m_0 = \gamma^* - t$, com t satisfazendo (2.10). Se existem t níveis com pelo menos uma variável o resultado segue do Lema 2.4. Da p-normalização (*ver* 2.7) segue que o número de variáveis entre os níveis 1 e τ satisfaz

$$\sum_{i=1}^{\tau} m_i \geq \gamma\left(\gamma^* - \gamma\right) + 1 - m_0 = \gamma\left(\gamma^* - \gamma\right) + 1 - \left(\gamma^* - t\right).$$

Por sua vez, de (2.10), tem-se que pode ser garantida a desigualdade

$$\gamma\left(\gamma^{*}-\gamma\right)+1-\left(\gamma^{*}-t\right) \geq (t-1)\left(\gamma^{*}-2\right). \tag{2.11}$$

Isto implica que podem ser distribuídas pelo menos $(t-1)\left(\gamma^{*}-2\right)$ variáveis em não mais que $t-1$ níveis. Relembrando que da Proposição 2.2, tem-se $t \geq 3$, sejam $i_1, i_2, \ldots, i_{t-1}$ os níveis onde são distribuídas estas variáveis, os quais satisfazem

$$1 \leq i_1 < i_2 < \ldots < i_{t-1} \leq \tau.$$

Inicialmente considere $\tau \geq 4$, $t \geq 4$ e

$$m_{i_1} + \cdots + m_{i_{t-1}} = (t-1)\left(\gamma^{*}-2\right).$$

Se estes $t-1$ níveis tem $\gamma^{*}-2$ variáveis cada um, o resultado segue do Lema 2.4 aplicado ao nível i_1. Agora, se existe $1 \leq s \leq t-1$, tal que $m_{i_s} < \gamma^{*}-2$, então $m_{i_s} \geq \gamma^{*}-3$, caso contrario existe $1 \leq r \leq t-1$, com $r \neq s$, tal que $m_{i_r} \geq \gamma^{*}$, ou existem dois níveis $i_{r_1} < i_{r_2}$ cada um com pelo menos $\gamma-1$ variáveis e portanto, tem-se solução novamente pelo Lema 2.4.

Quando $t > 4$ o resultado segue aplicando o Lema 2.4 ao menor nível i_s, satisfazendo $m_{i_s} \geq \gamma^{*}-2$. Por outra parte, se $t = 4$, tem-se os casos

$$\left(m_{i_1}, m_{i_2}, m_{i_3}\right) \in \left\{\left(\gamma^{*}-a, \gamma^{*}-b, \gamma^{*}-c\right);\ (a, b, c) \in P_{\{1,2,3\}}\right\},$$

onde $P_{\{1,2,3\}}$ é o conjunto das permutações de dos elementos 1, 2 e 3. Logo, do Lema 2.4, tem-se solução quando $m_{i_1} = \gamma^{*}-1$ ou $m_{i_1} = \gamma^{*}-2$. Portanto, considere

$$\left(m_{i_1}, m_{i_2}, m_{i_3}\right) \in \left\{\left(\gamma^{*}-3, \gamma^{*}-b, \gamma^{*}-c\right);\ (b, c) \in P_{\{1,2\}}\right\}.$$

Se $(b, c) = (1, 2)$ o resultado é imediato pelo Lema 2.4 aplicado ao nível i_2. Portanto, considere $(b,c) = (2,1)$. Segue de (2.7) e (2.11)

$$\begin{aligned}
\sum_{\substack{i=1 \\ i\neq i_1,i_2,i_3}}^{\tau+1} m_i &\geq (\gamma+1)(\gamma^*-\gamma)+1-m_0-m_{i_1}-m_{i_2}-m_{i_3} \\
&= (\gamma+1)(\gamma^*-\gamma)-4\gamma^*+11 \\
&> 0.
\end{aligned} \tag{2.12}$$

Dado que $\gamma = \tau+1$ e $\gamma^* = \lfloor \gamma \log_2(p) \rfloor + 1$ (*ver* (1.20) e (2.2)), esta desigualdade é satisfeita para todo $\tau \geq 4$ e para todo $p \geq 3$, exceto para os casos

$$(p,\tau) \in \{(3,4),(3,5)\}.$$

Note que para o caso $(p,\tau) = (3,4)$, tem-se da desigualdade (2.10) que $t \leq 2$, o que não esta no assumido para t. Logo, considere $\tau \geq 4$ e $p \geq 3$, com $(p,\tau) \neq (3,5)$, de (2.12), tem-se que que existe pelo menos uma variável no nível $\tau+1$, assim, aplicando o Lema 2.4 ao nível i_1, obtém-se um zero p-ádico não trivial.

Quando $(p,\tau) = (3,5)$, tem-se que $\gamma^* = 10$ e $m_0 = 6$, dado que $\mathscr{F}$ é p-normalizada, segue de (2.7) que $m_0 + m_1 \geq 9$, portanto o nível i_1 é o nível 1, obtendo assim $m_1 = \gamma^* - 3 = 7$, com isto $i_2 \geq 2$. Novamente, de (2.7) tem-se

$$\sum_{\substack{i=2 \\ i\neq i_2,i_3}}^{\tau+2} m_i \geq (\gamma+2)(\gamma^*-\gamma)-4\gamma^*+12 = 3.$$

Portanto, pelo menos um dos níveis, $\tau+1$ ou $\tau+2$, possui pelo menos uma variável, daí aplicando o Lema 2.4 ao nível i_2, obtém-se um zero p-ádico não trivial. Agora, quando $\tau \geq 4$, $t \geq 4$ e são distribuídas mais que $(t-1)(\gamma^*-2)$ em $t-1$ níveis, o resultado segue aplicando o Lema 2.4 ao menor nível i_s, tal que $m_{i_s} \geq \gamma^* - 2$.

Para $\tau \geq 3$ seja $t = 3$, por (2.11), tem-se que existem dois níveis, com pelo menos $2\gamma^* - 4$ variáveis. Se $m_{i_1} + m_{i_2} \geq 2\gamma^* - 2$ tem-se que quaisquer destes níveis tem pelo menos $\gamma^* - 1$ variáveis e o resultado segue do Lema 2.4. Portanto, assuma

$$2\gamma^* - 3 \geq m_{i_1} + m_{i_2} \geq 2\gamma^* - 4.$$

Assim, obtém-se de (2.7)

$$\begin{aligned}\sum_{\substack{i=1\\ i\neq i_1,i_2}}^{\tau+1} m_i &\geq (\gamma+1)(\gamma^*-\gamma)+1-m_0-m_{i_1}-m_{i_2}\\ &=(\gamma+1)(\gamma^*-\gamma)-3\gamma^*+7\\ &\geq 1.\end{aligned} \tag{2.13}$$

Isto implica que o nível γ possui pelo menos uma variável, e, novamente o resultado segue ao aplicar o Lema 2.4 ao nível i_1. Finalmente, se para um t satisfazendo (2.10), e portanto (2.11), tem-se que são distribuídas pelo menos $(t-1)(\gamma^*-2)$ variáveis em h níveis, com $1 \leq h < t-1$, segue que um ou mais destes níveis possuem pelo menos γ^*-1, caso este nível seja o nível τ, fazendo um raciocínio semelhante ao feito no caso anterior, obtém-se uma solução pelo Lema 2.4, o qual conclui a prova. □

Como uma consequência imediata da Lema 2.7, tem-se a prova do Teorema 0.2.

Prova do Teorema 0.2

Teorema 0.2. *Para todo inteiro $\tau \geq 1$ existe um primo q ímpar, tal que para todo $p \geq q$, se $k = p^\tau k_0$ vale*

$$\Gamma^*(k,p) \leq k(\gamma^*-\gamma)+1.$$

Demonstração. Pela Proposição 2.1, tem-se que $q=3$ para $\tau = 1,2$. Agora, fixando $\tau \geq 3$ defina

$$F_\tau(p) := \frac{(\tau+1)\left(\lfloor(\tau+1)\log_2(p)\rfloor-\tau\right)-1}{\lfloor(\tau+1)\log_2(p)\rfloor-2} \tag{2.14}$$

Observe que $F_\tau(p)$ é uma função crescente em p com assintota horizontal $\tau+1$ pois,

$$\frac{(\tau+1)^2(\log_2(p)-1)-1}{(\tau+1)\log_2(p)-2} \leq F_\tau(p) \leq \frac{(\tau+1)\left((\tau+1)\log_2(p)+\tau\right)-1}{(\tau+1)\log_2(p)-2}. \tag{2.15}$$

Seja q o menor primo tal que $\tau \leq F_\tau(q)$ e considere $\mathscr{F}$ uma forma aditiva de grau k em s variáveis, com $p \geq q$, $k = p^\tau k_0$ e $s \geq k(\gamma^*-\gamma)+1$. Observe que τ satisfaz (2.10), pois $F_\tau(p)$ não é mais que o lado direito de dita desigualdade em termos de τ e p. Daí, se $m_0 = \gamma^*-t$, segue do Lema 2.7 que $\mathscr{F}$ possui um zero p-ádico não trivial para $1 \leq t \leq \tau$. Isto implica que

$$\Gamma^*(k,p) \leq k(\gamma^*-\gamma)+1.$$

$\square$

A Tabela 2.1 mostra os primeiros primos q resultantes da prova do Teorema 0.2 quando $\tau \neq 3$, deve ser esclarecido que, quando $\tau = 3$ o valor de q pelo Teorema anterior é $q = 5$, mas como um resultado do Teorema 1 este valor é $q = 3$. Por outra parte, da Proposição 2.1 tem-se que para $\tau \in \{1, 2\}$, tem-se que $q \geq 3$.

τ	q	τ	q	τ	q
1	3	11	613	21	576287
2	3	12	1213	22	1147819
3	3	13	2377	23	2286961
4	7	14	4721	24	4558097
5	13	15	9337	25	9087079
6	23	16	18517	26	18120413
7	43	17	36781	27	36141247
8	83	18	73121	28	72097633
9	163	19	145441	29	143851009
10	311	20	289439	30	287059441

Tabela 2.1: Primeiros 30 valores de q para os quais é satisfeito o Teorema 0.2.

Note que da parcela direita da desigualdade (2.15) os primos q para os quais é satisfeito o Teorema 0.2 crescem exponencialmente e, embora estes valores podem ser um pouco melhorados como na Tabela 2.1 (*ver* A.3), ditos valores seguem tendo um comportamento exponencial, ainda assim, conjetura-se o seguinte:

Conjetura 2.1. *O primo q no Teorema 0.2 é $q = 3$, isto é, que para todo $\tau \geq 1$ e para todo primo $p \geq 3$ tem-se*

$$\Gamma^*(k, p) \leq k(\gamma^* - \gamma) + 1.$$

Capítulo

3

Contração de Variáveis e Blocos

Como foi visto na demonstração do Teorema 0.1 é usado o Lema 2.6, o qual não é mais que uma contração de variáveis do nível 1 ao nível $\gamma + 1$ a fim de encontrar uma solução não singular módulo $p^{\gamma+1}$, e, o caminho para encontrar dita solução é o Lema 2.1.

Neste capítulo estes conceitos são adaptados com o objetivo de estabelecer as ferramentas necessárias que serão usadas no capítulo 4 para dar solução ao problema principal, ou seja, a prova do Teorema 1. Isto implica, que no que segue do trabalho será estudado a detalhe o caso $k = 3^\tau$, principalmente quando é considerado o primo p=3. Nesse caso, tem-se que

$$(k, p-1) = (3^\tau, 2) = 1 = \frac{3-1}{2},$$

ou seja, tem-se que -1 é uma 3^γ-ésima potência módulo 3^γ.

Os resultados são organizados como segue: Na seção 3.1 é estabelecida a maneira em que são contraídas as variáveis. A sua vez, o Lema 3.6 é a versão do Lema 2.4 para $k = 3^\tau$. Tanto do Lema 2.1, como do Lema 3.6 surge a limitante do método, pois ele prevê a existência de variáveis nos τ-níveis seguintes de um nível i dado. Agora, como é assumida uma forma p-normalizada $\mathscr{F}$ de grau k com $s \geq k(\gamma^* - \gamma) + 1$ variáveis, decorre daí, na seção 3.2 uma forma de distribuir este número de variáveis nos τ-níveis a fim de que toda forma $\mathscr{F}$ com o número de variáveis já dito, possua solução não singular módulo p^γ.

3.1 Lemas de Contração

Uma parte essencial no trabalho de Davenport e Lewis em [8], foi estabelecer um método para contrair variáveis do nível 0 para obter uma nova variável no nível pelo menos γ em uma forma aditiva p-normalizada, como foi visto no capítulo 1, esta nova variável é obtida através de um procedimento acumulativo, o qual após achar uma solução, permite achar variáveis não nulas no nível 0 para aplicar o Lema de Hensel 1.9. Apresenta-se aqui uma forma de contrair variáveis que, em conjunção com o Lema 3.6 e outras ferramentas, fornecem um caminho propicio para a aplicação do Lema 2.1. Começa-se com alguns lemas sobre contração de variáveis de maneira mais geral, isto, porque no desenvolvimento deste trabalho observa-se que estas generalizações abrem a porta para possíveis novos trabalhos a partir destes lemas, mas no decorrido do trabalho, os esforços focam-se no caso $p = 3$.

Seja $k = p^{\tau} k_0$, com k_0 coprimo a p. Considere $\mathscr{F}$ uma forma aditiva p-normalizada de grau k em s variáveis, satisfazendo as condições do Lema 1.8.

$$\mathscr{F} = a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k, \tag{3.1}$$

Por outra parte, seja $\alpha \in \mathbb{Z}$ escrito na base p

$$\alpha = \alpha_0 + \alpha_1 \cdot p + \cdots + \alpha_n \cdot p^n,$$

Diz-se que α_i é o *zerotermo* de α, se i é o primeiro índice tal que $\alpha_i \neq 0$. Além disso, se uma variável x de $\mathscr{F}$ esta no nível l, então o zero termo de x é definido como sendo o zerotermo de α/p^l, onde α é o coeficiente de x.

Nos seguintes lemas assume-se $k = p^{\tau}(p-1)/2$,

$$d = (k, p-1) = \frac{p-1}{2},$$

portanto, tem-se que -1 é uma potencia k-ésima módulo p^{γ}.

Lema 3.1. *Se $x_1, x_2, \ldots, x_r$ com $r \geq (p+1)/2$ são variáveis no nível l, elas podem ser contraídas em novas variáveis y, no nível pelo menos $l+1$.*

Demonstração. Sem perda de generalidade assume-se $l = 0$, além disso, o trabalho é feito módulo p^2. Para $i = 1, 2, \ldots, r$, sejam

$$\alpha_i = a_i + pb_i,$$

com $a_i \in \{1, 2, \ldots, p-1\}$ e $b_i \in \{0, 1, 2, \ldots, p-1\}$ os coeficientes das r variáveis. Se existem i, j tais que $a_i = a_j$, fazendo $x_i = y_{i,j}$ e $x_j = -y_{i,j}$, obtém-se uma nova variável $y_{i,j}$ com coeficientes $p(b_i - b_j)$. Por outra parte, se $a_i \neq a_j$, para todo i, j então, fazendo $x_i = y_{i,j} = x_j$ com $a_i + a_j = p$, tem-se uma nova variável $y_{i,j}$ com coeficiente $p\,(1 + b_i + b_j)$. Em cada um dos casos, obteve-se novas variáveis da forma $y_{i,j}$ em pelo menos no nível 1. □

Lema 3.2. *Se tem-se p variáveis no nível l com o mesmo zerotermo, então é possível contrair dois ou p de estas variáveis para uma nova variável no nível precisamente $l+1$.*

Demonstração. Novamente, seja considerado $l = 0$ e, o trabalho é feito módulo p^2. Assuma-se os coeficientes $\alpha_i = a + pb_i$, com $p \nmid a$ e $b_i \in \{0, 1, 2, \ldots, p-1\}$ para $i = 1, 2, \ldots p$. Se $b_1 = b_i$ para $i = 2, \ldots p$, fazendo $x_i = y$ para $i = 1, 2, \ldots, p$, obtém-se uma nova variável y com coeficiente $a \cdot p \not\equiv \pmod{p^2}$. Caso contrário, é possível escolher índices i, j tais que $b_i \neq b_j$ então, fazendo $x_i = y$ e $x_j = -y$, tem-se uma nova variável y cujo coeficiente é $p(b_i - b_j) \not\equiv 0 \pmod{p^2}$, isto é, em quaisquer dos casos obtém-se uma nova variável precisamente no nível 1. □

Lema 3.3. *Se tem-se $(p-1)^2 + 1$ variáveis no nível l, então é possível contrair dois ou p destas variáveis em uma nova variável no nível precisamente $l+1$.*

Demonstração. Sem perda de generalidade, considere $l = 0$, e novamente o trabalho é feito módulo p^2. Com $(p-1)^2 + 1$ variáveis no nível zero, pelo princípio da casa dos pombos, é possível escolher p destas variáveis tendo o mesmo zerotermo e o resultado segue diretamente do Lema 3.2. □

O seguinte Lema é uma aplicação direta do Lema 3.3 e da seguinte propriedade para a função piso: Sejam n um inteiro e x, m reais arbitrários, então

$$\left\lfloor \frac{\lfloor x/m \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{mn} \right\rfloor. \tag{3.2}$$

A demonstração deste fato pode ser encontrado em [12, p.72].

Lema 3.4. *Seja M o número de variáveis no nível j, então é possível contrair estas variáveis para obter*

$$\max\left\{0, \left\lfloor \frac{M-(p^l-1)(p-2)}{p^l} \right\rfloor\right\}$$

novas variáveis precisamente no nível $j+l$.

Demonstração. O objetivo da prova é assegurar a existência de variáveis contraídas exatamente no nível $j+l$ provenientes da contração de variáveis do nível j, usando recursivamente o Lema 3.3. Em este sentido, o Lema 3.3 providencia um número mínimo de variáveis onde isto acontece. Assim, sem perda de generalidade, assuma $j=0$. Se $l=1$ e $M<(p-1)^2+1$, não é possível garantir a existência de variáveis exatamente no nível 1, pois pelo Teorema da Casa dos Pombos não podem ser garantidas p variáveis com o mesmo zerotermo. Portanto, considere $M \geq (p-1)^2+1$, e observe que pelo menos $(p-1)(p-2)$ não serão contraídas, obtendo

$$M-(p-1)(p-2) \geq p.$$

Logo o número máximo de variáveis contraídas do nível 0 ao nível 1, esta dado por

$$\left\lfloor \frac{M-(p-1)(p-2)}{p} \right\rfloor.$$

Agora, assuma valido para l e mostra-se para $l+1$. Da hipótese de indução, se o nível l possui zero variáveis contraídas desde o nível 0, o resultado é imediato assim, se o nível l tem pelo menos

$$\left\lfloor \frac{M-(p^l-1)(p-2)}{p^l} \right\rfloor$$

variáveis contraídas desde nível 0, estas variáveis podem ser contraídas ao nível $l+1$ como no caso $l=1$, pois

$$\begin{aligned}\left\lfloor \frac{\left\lfloor \frac{M-(p^l-1)(p-2)}{p^l} \right\rfloor - (p-1)(p-2)}{p} \right\rfloor &= \left\lfloor \frac{\left\lfloor \frac{M-(p-2)\left(p^{l+1}-1\right)}{p^l} \right\rfloor}{p} \right\rfloor \\ &= \left\lfloor \frac{M-(p^{l+1}-1)(p-2)}{p^{l+1}} \right\rfloor.\end{aligned} \tag{3.3}$$

□

Assume-se de agora em diante que $k = 3^\tau$, e relembra-se que $\gamma^* = \lfloor \gamma \log_2(3) + 1 \rfloor$ (*ver* (2.2)). Com isto, o Lema 3.4 reescreve-se para este caso como segue:

Lema 3.5. *Seja M o número de variáveis no nível j, então é possível contrair estas variáveis para obter*

$$\max\left\{0, \left\lfloor \frac{M-(3^l-1)}{3^l} \right\rfloor\right\}. \tag{3.4}$$

novas variáveis no nível $j + l$.

Apresenta-se agora um dos resultados fundamentais deste trabalho, o qual é uma dedução do Lema 2.4. Grande parte dos futuros esforços, focam-se em satisfazer as hipóteses do seguinte lema para mostrar o Teorema 1. É em virtude desta ideia que são desenvolvidos os conceitos.

Lema 3.6. *Seja $\mathscr{F}$ uma forma aditiva 3-normalizada de grau $k = 3^\tau$ em s variáveis. Em cada um dos seguintes casos $\mathscr{F}$ tem zeros 3-ádicos não triviais.*

(i). $m_i \geq \gamma^*$ *para algum* $i \in \{0, 1, \ldots, k-1\}$;

(ii). *Existe* $r \in \{1, 2, \ldots, \gamma - 1\}$ *tal que pode-se escolher* $i \in \{0, 1, \ldots, k - r - 1\}$ *e* r *índices distintos* $j_l \in \{i+1, i+2, \ldots, i+\gamma-1\}$ *com* $m_i \geq \gamma^* - r$ *e* $m_{j_l} \geq 1$ *para* $l = 1, 2, \ldots, r$.

Demonstração. A prova segue do Lema 2.4. □

Apesar que o Lema 3.5 oferece uma quantia sobre o número de variáveis que podem ser contraídas de um nível j até o nível $j + l$, dito Lema não considera as interações com outras variáveis em um processo iterado de contração de variáveis de um nível ao imediato seguinte, e deste último com uma nova quantidade de variáveis ao que segue. Por isto, apresenta-se dita iteração em um caso particular, onde a notação assumida facilita a prova do Lema 3.8.

Lema 3.7. *Suponha $\mathscr{F}$ como em (3.1) e seja $N = \lfloor (m_0 - 2)/3 \rfloor$. Por outra parte, considere G, h e H inteiros positivos, com $h < H$ e, alem disso, sejam $m_0 = G + h$ e*

$$m_i = G + H - N + \delta_{i-1} - \delta_i, \tag{3.5}$$

onde $\delta_0 = 0$ e $\delta_i \geq 0$ para $i = 1, 2, \ldots, l$. Então, é possível contrair variáveis em ordem para garantir pelo menos $N - \left\lceil \frac{\delta_l}{3} \right\rceil$ novas variáveis no nível $l + 1$.

Demonstração. A prova é feita por indução sobre l. Quando $l = 0$ segue do Lema 3.5 que o número de variáveis contraídas do nível 0 ao nível 1 esta dado pelo Lema 3.5, ou seja,

$$N = \left\lfloor \frac{m_0 - 2}{3} \right\rfloor,$$

dado que $\delta_0 = 0$ segue que são contraídas exatamente N variáveis ao nível 1. Agora, para $l = 1$, fazendo uso do Lema 3.5 para as variáveis do nível 0 e depois de contração para o nível 1 obtém-se

$$\begin{aligned}
\left\lfloor \frac{\left(m_1 + \left\lfloor \frac{m_0-2}{3} \right\rfloor\right) - 2}{3} \right\rfloor &= \left\lfloor \frac{(m_1 + N) - 2}{3} \right\rfloor \\
&= \left\lfloor \frac{(G + H - N - \delta_1 + N) - 2}{3} \right\rfloor \\
&= \left\lfloor \frac{G + H - 2}{3} - \frac{\delta_1}{3} \right\rfloor \\
&\geq N - \left\lceil \frac{\delta_1}{3} \right\rceil
\end{aligned}$$

novas variáveis no nível 2. Assuma-se que o resultado é valido para l e prova-se para $l + 1$. Da hipótese de indução e do Lema 3.5, o número de novas variáveis no nível $l + 2$ é

$$\begin{aligned}
\left\lfloor \frac{\left(m_{l+1} + N - \left\lceil \frac{\delta_l}{3} \right\rceil\right) - 2}{3} \right\rfloor &= \left\lfloor \frac{\left((G + H - N + \delta_l - \delta_{l+1}) + N - \left\lceil \frac{\delta_l}{3} \right\rceil\right) - 2}{3} \right\rfloor \\
&= \left\lfloor \frac{G + H - 2}{3} + \frac{\delta_l - \left\lceil \frac{\delta_l}{3} \right\rceil}{3} - \frac{\delta_{l+1}}{3} \right\rfloor \\
&\geq N - \left\lceil \frac{\delta_{l+1}}{3} \right\rceil
\end{aligned}$$

□

Considere $\mathscr{F}$ uma forma aditiva 3-normalizada de grau $k = 3^\tau$ em $s \geq 3^\tau(\gamma^* - \gamma) + 1$ variáveis. Observe, que para obter a desigualdade

$$\Gamma^*(3^\tau, 3) \leq 3^\tau(\gamma^* - \gamma) + 1,$$

é suficiente mostrar que $\mathscr{F}$ possui zeros 3-ádicos não triviais para todo

$$\gamma^* - \tau \leq m_0 < \gamma^*,$$

pois, quando $m_0 \geq \gamma^*$ sempre se tem zeros 3-ádicos pelo Lema 3.6. Com isto, suponha que existe H, tal que $\mathscr{F}$ possui zeros 3-adicos não triviais sempre que $m_0 = \gamma^* - \gamma + h$, com

$$H \leq h \leq \gamma - 1.$$

O objetivo é usar estas soluções para mostrar que a forma aditiva $\mathscr{F}$ tem zeros 3-ádicos não triviais quando $m_0 = \gamma^* - \gamma + h'$, com $1 \leq h' < H$. Para isto, o seguinte Lema usa a 3-normalização e os valores de m_0 para os quais já se tem uma solução, para garantir a existência de variáveis nos níveis $1 \leq i \leq i - h'$ para assim usar o Lema 3.6. Em este processo, o Lema 3.7 tem um papel fundamental, e é aqui onde é justificada a notação adotada para dito lema.

Lema 3.8. *Seja $\mathcal{S}$ o conjunto das formas aditivas 3-normalizadas de grau $k = 3^\tau$ em*

$$s \geq 3^\tau(\gamma^* - \gamma) + 1$$

variáveis, onde $m_0 = (\gamma^* - \gamma) + h$, com $1 \leq h \leq \gamma - 1$. Seja $2 \leq H \leq \gamma - 1$ tal que para toda $\mathscr{F} \in \mathcal{S}$, com $H \leq h \leq \gamma - 1$ tem um zero 3-ádico. Se

$$H \leq \left\lfloor \frac{m_0 - 2}{3} \right\rfloor = N, \tag{3.6}$$

então toda forma $\mathscr{F} \in \mathcal{S}$ com $m_0 = (\gamma^* - \gamma) + h$ e $1 \leq h \leq \gamma^* - \gamma$, também tem um zero 3-ádico não trivial.

Demonstração. Seja $G = \gamma^* - \gamma$, pela hipótese sobre H, assume-se $h < H$. Dado que $\mathscr{F}$ é 3-normalizada, tem-se

$$\begin{aligned} m_1 &\geq 2G + 1 - m_0 \\ &= 2G + 1 - (G + h) \\ &= G + 1 - h \\ &> 0. \end{aligned}$$

Fazendo uso do Lema 3.5 para contrair as variáveis do nível zero, é possível criar N

variáveis no nível 1. Primeiro, assuma $m_1 \geq G + H - N$, então considere a forma

$$\mathscr{F}^{(1)} = \frac{1}{3} \cdot \mathscr{F}(3x_1, 3x_2, \ldots, 3x_{s_0}, x_{s_0+1}, \ldots, x_s) \tag{3.7}$$

onde as variáveis $x_1, \ldots, x_{s_0}$ são as variáveis do nível zero que não foram contraídas. Denota-se $m_i^{(1)}$ como o número de variáveis da forma $\mathscr{F}^{(1)}$ que estão no nível i, assim, tem-se

$$\begin{aligned} m_0^{(1)} = m_1 + N &\geq (G + H - N) + N \\ &= G + H \end{aligned}$$

e por outra parte,

$$\begin{aligned} \sum_{i=0}^{j} m_i^{(1)} &= m_1 + N + m_2 + \cdots + m_{j+1} \\ &= \sum_{i=0}^{j+1} m_i - (m_0 - N) \\ &\geq (j+2)G + 1 - (G + h - N) \\ &= (j+1)G + 1 + (N - h) \\ &> (j+1)G + 1 \end{aligned}$$

para $j = 1, 2, \ldots, k-1$ e conclui-se que $\mathscr{F}^{(1)}$ satisfaz as propriedades de uma forma 3-normalizada (*ver* Lema 1.8), logo por hipótese, tem-se que $\mathscr{F}^{(1)}$ possui zeros 3-ádicos não triviais. Portanto, assuma $m_1 = G + H - N - \delta_1$ com $\delta_1 > 0$, e tem-se

$$\begin{aligned} m_2 &= 3G + 1 - m_0 - m_1 \\ &= 3G + 1 - (G + h) - (G + H - N - \delta_1) \\ &= G + 1 - h + (N - H) + \delta_1 \\ &> 0. \end{aligned}$$

Suponha que $m_2 \geq G + H - N + \delta_1$, pelo Lema 3.7 é possível contrair variáveis dos níveis 0 e 1 e obter pelo menos $N - \left\lceil \frac{\delta_1}{3} \right\rceil$ novas variáveis no nível 2. Assim, considere a forma

$$\mathscr{F}^{(2)} = \frac{1}{3^2} \cdot \mathscr{F}(3x_1, 3x_2, \ldots, 3x_{s_1}, x_{s_1+1}, \ldots, x_s) \tag{3.8}$$

onde as variáveis $x_1, \ldots, x_{s_1}$, são as variáveis dos níveis 0 e 1 que não foram contraídas. Denote $m_i^{(2)}$ como o número de variáveis no nível i da forma $\mathscr{F}^{(2)}$, assim,

$$\begin{aligned} m_0^{(2)} &= m_2 + N - \left\lceil \frac{\delta_1}{3} \right\rceil \\ &\geq (G + H - N + \delta_1) + N - \left\lceil \frac{\delta_1}{3} \right\rceil \\ &\geq G + H \end{aligned}$$

e

$$\begin{aligned} \sum_{i=0}^{j} m_i^{(2)} &= m_2 + N + m_3 + \cdots + m_{j+2} \\ &= \sum_{i=0}^{j+2} m_i - (m_0 + m_1 - N) \\ &\geq (j+3)G + 1 - ((G+h) + (G + H - N - \delta_1) - N) \\ &= (j+1)G + 1 + (2N - h - H) + \delta_1 \\ &> (j+1)G + 1, \end{aligned}$$

para $j = 1, 2, \ldots, k-2$ e conclui-se que $\mathscr{F}^{(2)}$ é uma forma 3-normalizada. Logo por hipótese, tem-se que $\mathscr{F}^{(2)}$ possui zeros 3-ádicos não triviais. Dessa maneira, assume-se $m_2 = G + H - N + \delta_1 - \delta_2$ com $\delta_2 > 0$.

Agora, assume-se para todo $j < n$

$$1 < m_j = G + H - N + \delta_{j-1} - \delta_j$$

com $\delta_i > 0$ para todo $i = 1, 2, \ldots, j$. dado que a forma é 3-normalizada, tem-se

$$\begin{aligned} m_n &= (n+1)G + 1 - \sum_{i=0}^{n-1} m_i \\ &= (n+1)G + 1 - (G+h) - (G + H - N - \delta_1) \\ &\quad - \sum_{i=2}^{n-1} (G + H - N + \delta_{i-1} - \delta_i) \\ &= G + 1 - h + (n-1)(N - H) + \delta_{n-1} \\ &> 0. \end{aligned}$$

Suponha que $m_n \geq G + H - N + \delta_{n-1}$, pelo Lema 3.7 é possível contrair variáveis dos níveis $0, 1, \ldots, n-1$ e obter pelo menos $N - \left\lceil \frac{\delta_{n-1}}{3} \right\rceil$ novas variáveis no nível n. Novamente, considerando a forma

$$\mathscr{F}^{(n)} = \frac{1}{3^n} \cdot \mathscr{F}(3x_1, 3x_2, \ldots, 3x_{s_{n-1}}, x_{s_{n-1}+1}, \ldots, x_s), \tag{3.9}$$

onde as variáveis $x_1, \ldots, x_{s_{n-1}}$ são as variáveis que não foram contraídas dos níveis $0, 1, \ldots, n-1$. Denota-se $m_i^{(n)}$ como o número de variáveis da forma $\mathscr{F}^{(n)}$ no nível i, o que satisfaz

$$\begin{aligned} m_0^{(n)} &= m_n + N - \left\lceil \frac{\delta_{n-1}}{3} \right\rceil \\ &\geq (G + H - N + \delta_{n-1}) + N - \left\lceil \frac{\delta_{n-1}}{3} \right\rceil \\ &\geq G + H, \end{aligned}$$

e análogo aos casos anteriores, tem-se

$$\begin{aligned} \sum_{i=0}^{j} m_i^{(n)} &= \sum_{i=0}^{n+j} m_i - \left(\sum_{i=0}^{n-1} m_i - N \right) \\ &\geq (n + j + 1)G + 1 + N - (G + h) \\ &\quad - (G + H - N - \delta_1) - \sum_{i=2}^{n-1} (G + H - N + \delta_{i-1} - \delta_i) \\ &> (j + 1)G + 1, \end{aligned}$$

para $j = 1, 2, \ldots, 3^\tau - n$, assim, $\mathscr{F}^{(n)}$ é uma forma 3-normalizada com o qual são obtidos zeros 3-adicos não triviais. Disto, assume-se

$$m_n = G + H - N + \delta_{n-1} - \delta_n$$

para $\delta_n > 0$. Daí, aplicando este processo de maneira recursiva é possível obter uma forma $\mathscr{F}^{(n+r)}$ com $r \geq 1$ para a qual ou tem zeros 3-adicos não triviais, ou tem-se

$$\prod_{i=1}^{\gamma^* - m_0} m_i \neq 0$$

e aplicando o Lema 3.6 obtém-se o resultado desejado. $\square$

Corolário 3.1. *Seja $\mathcal{S}$ o conjunto das formas 3-normalizadas e $\mathscr{F} \in \mathcal{S}$ uma forma aditiva como no Lema 3.8. Se $\mathscr{F}$ possui zeros 3-ádicos não triviais quando*

$$m_0 = \gamma^* - \gamma + h, \tag{3.10}$$

com $H < h \leq \gamma - 1$ e

$$H = \left\lfloor \frac{\gamma^* - \gamma - 2}{2} \right\rfloor, \tag{3.11}$$

então toda forma $\mathscr{F} \in \mathcal{S}$ também tem zeros 3-adicos quando $m_0 = \gamma^* - \gamma + h$, e $1 \leq h \leq H$.

Demonstração. Da equação (3.6) obtém-se o valor de H. Fazendo $h = H$ em (3.10) obtém-se pelo Lema 3.8 uma solução não singular para uma forma $\mathscr{F} \in \mathcal{S}$ com $\gamma^* - \gamma^* + H$ variáveis no nível 0. Agora, assuma $h = H - 1$ em (3.10), dado que uma forma 3-normalizada com $\gamma^* - \gamma^* + H$ no nível 0 possui um zero 3-adico não trivial pelo Lema 3.8 a forma com $m_0 = \gamma^* - \gamma + H - 1$ tem zeros 3-adicos não triviais. O resultado segue até $h = 1$ iterando este raciocínio. □

Embora o pareça, cada um dos passos do Lema 3.8 não são necessariamente lineares no sentido de apenas obter uma solução, é dizer, o Lema 3.8 encontra todas as soluções não singulares possíveis, e ditas soluções estão apenas reguladas pelos valores que podem assumir os δ_i's respeitando a 3-normalização, isto é, o Lema 3.8 encontra todos os zeros 3-ádicos não triviais, para todos os valores que podem assumir os m_i com $i = 1, 2, \ldots, \gamma^* - m_0$, limitados tanto pela 3-normalização como pelas soluções anteriores.

Exemplo 3.9. Seja $k = 3^8$, e considere $\mathcal{S}$ o conjunto das formas 3-normalizadas com $3^8 \cdot 6 + 1$ variáveis como no Lema 3.8. Do Corolário 3.1 tem-se que $H = 2$, assim, suponha-se que para todo $4 \leq h \leq 8$ a forma $\mathscr{F} \in \mathcal{S}$ com $6 + h$ variáveis no nível zero possui solução não singular, isto é, para

$$9 \leq m_0 \leq 14,$$

a equação

$$\mathscr{F} \equiv 0 \pmod{3^\gamma} \tag{3.12}$$

possui soluções não triviais. Agora, seja $m_0 = 8$, como $\mathscr{F} \in \mathcal{S}$, implica que $m_1 \geq 5$. Se $m_1 \geq 7$, tem-se pelo Lema 3.5 que é possível contrair duas variáveis do nível

0 ao nível 1, isto implica, que após de contrações $m_1 \geq 9$, portanto, a forma $\mathscr{F}$ pode ser reordenada à forma $\mathscr{F}^{(1)}$ como em (3.7) e assim a equação (3.12) possui soluções não triviais, daí, tem-se que $5 \leq m_1 \leq 6$. Se $m_1 = 5$ do Lema 3.7 contrai-se variáveis do nível 0 ao nível 2, de tal forma que obtém-se 1 nova variável no nível 2, assim, por um argumento semelhante ao anterior tem-se $6 \leq m_2 \leq 7$ logo, se $m_2 = 6$ pelo Lema 3.7 tem-se $6 \leq m_3 \leq 7$. Por outra parte, se $m_2 = 7$ segue que $5 \leq m_3 \leq 6$. O procedimento segue desta maneira para os níveis i com $i = 4, 5, 6, 7$. Desta maneira, é possível aplicar o Lema 3.6, e tem-se portanto uma solução não singular para (3.12). O raciocino é semelhante quando $m_1 = 6$, obtendo da mesma maneira uma solução não singular para (3.12). Isto exemplifica o razoamento do Lema 3.8 e na Figura 3.1 apresenta-se em resumo estas ideias.

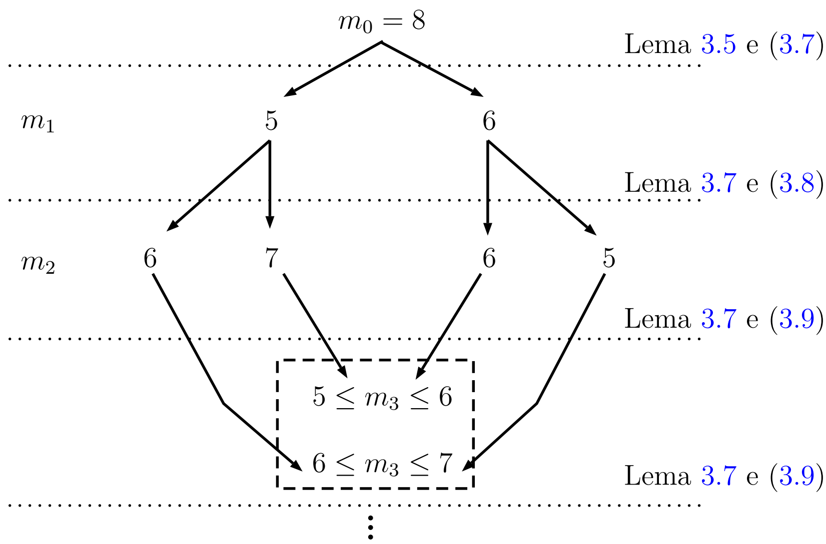

Figura 3.1: Casos para $m_0 = 8$ quando $k = 3^8$.

Finalmente, seja $m_0 = 7$. Tem-se $m_1 \geq 6$, dado que é possível contrair varáveis do nível zero a uma nova variável no nível 1, assim, se $m_1 \geq 7$ após da contração de variáveis, teria pelo menos 8 variáveis, o que já possui uma solução, portanto $m_1 = 6$. Agora, $m_2 \geq 6$, contraindo variáveis pelo Lema 3.7 do nível zero ao nível 2, tem-se pelo menos uma nova variável em dito nível, assim se $m_2 \geq 7$, obtém-se uma solução não singular, portanto $m_2 = 6$. Estes argumentos seguem de maneira iterada até o nível 8, daí, usando o Lema 3.6 tem-se uma solução não singular.

Portanto, quaisquer forma aditiva com $3^8 \cdot 6 + 1$ possui uma solução não singular, isto é, representa um zero 3-ádico.

3.2 Blocos e t-configurações

Como foi visto na seção 3.1, o Lema 3.8 permite obter soluções para uma forma p-normalizada a partir de soluções anteriores, mas para isto, a forma aditiva $\mathscr{F}$ precisa satisfazer a condição que: após de contrair variáveis do nível zero a um nível i e reordenar a forma, de tal maneira que dito nível agora seja o nível 0, $\mathscr{F}^{(i)} \in \mathcal{S}$, isto é, $\mathscr{F}^{(i)}$ deve ser p-normalizada. Precisamente, o valor de H obtido em (3.11) providencia uma limitante para m_0 e as formas aditivas que tem valores $h \geq H$ em (3.6) as quais, após de contração não necessariamente são p-normalizadas. Nesse sentido, fornece-se um método que consiste em considerar o número de variáveis que tem-se desde o nível zero até o nível τ por conta da p-normalização, ou seja, pelo menos $\gamma\left(\gamma^* - \gamma\right) + 1$ variáveis, e novamente o que se quer é distribuir essas variáveis de tal maneira que sejam satisfeitas as hipóteses do Lema 3.6, sem importar em que níveis encontrem-se possivelmente distribuídas as variáveis.

Seja $\mathscr{F}$ uma forma 3-normalizada de grau $k = 3^\tau$ em s variáveis. Segue de (1.18) que $s = m_0 + \cdots + m_{k-1}$. Defina

$$\mathcal{N} = \{i; \;\; m_i \neq 0\},$$

o qual é chamado de conjunto de níveis de $\mathscr{F}$.

Definição 3.2.1. *Seja $t < \gamma$ um inteiro positivo. Define-se uma t-configuração como qualquer subconjunto de níveis $C = \{i_1, i_2, \ldots, i_t\} \subseteq \mathcal{N}$ onde $1 \leq i_1 < \cdots < i_t < \gamma$*

Dada uma t-configuração C o seguinte lema estabelece uma limitante superior para m_i, com $i \in C$. Esta limitante esta dada pelo Lema 3.6 como segue:

Lema 3.10. *Seja $C = \{i_1, \ldots, i_t\}$ uma t-configuração, então*

$$m_{i_j} \leq \gamma^* - t - 1 + j, \tag{3.13}$$

ou então, $\mathscr{F}$ tem um zero 3-ádico

Demonstração. Segue do Lema 3.6 que $m_{i_j} \leq \gamma^* - 1$ para $1 \leq j \leq t$, disto tem-se que quando $j = t$, $m_{i_t} \leq \gamma^* - 1$, satisfazendo (3.13). Agora, se $m_{i_{t-1}} \geq \gamma^* - 1$, tem-se um zero 3-adico não trivial pelo Lema 3.6, pois existe pelo menos una variável no nível i_t, portanto $m_{i_{t-1}} \leq \gamma^* - 2$, com o qual tem-se (3.13). De maneira geral, para $1 \leq j \leq t-3$, se $m_{i_j} \geq \gamma^* - t + j$, seguindo o mesmo raciocínio usado no caso $t-2$ segue que

$$m_{i_j} \leq \gamma^* - t - 1 + j,$$

como queria ser provado. □

Relembrando que neste trabalho, tem-se particular interesse nos subconjuntos do conjunto de níveis $\mathcal{N}_\tau = \{1 \leq i \leq \tau; \quad m_i \neq 0\}$ que formam uma t-configuração, segue o seguinte exemplo.

Exemplo 3.11. Seja $\mathscr{F}$ uma forma aditiva 3-normalizada de grau $k = 3^9$ em $s \geq k(\gamma^* - \gamma) + 1$ variáveis, com $\gamma = 10$ e $\gamma^* = \lfloor 10 \log_2(3) \rfloor + 1 = 16$. Alem disso, considere uma 6-configuração, e observe que se $10 \leq m_0$, então $\mathscr{F}$ representa um zero 3-ádico não trivial. Do anterior, e do Lema 1.8, segue que $7 \leq m_0 \leq 9$. Por outra parte, do Lema 3.10 tem-se que

$$m_{i_j} \leq 9 + j \tag{3.14}$$

Na Figura 3.2 mostra-se o dito anteriormente

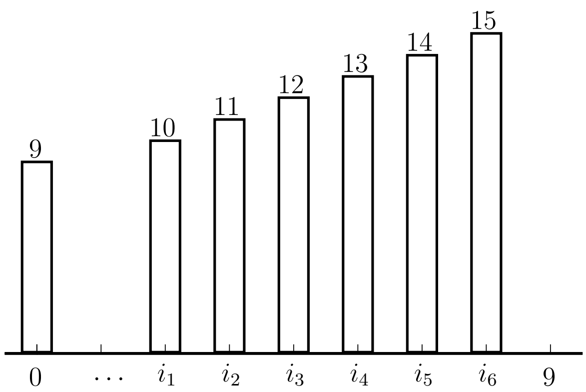

Figura 3.2: *Caso $\tau = 9$ com uma 6-configuração. Aqui $\gamma^* = 16$, $m_0 = 9$ e os valores acima de cada barra são o número máximo de variáveis que pode ter este nível.*

Agora, considere $C = \{i_1, \ldots, i_t\}$ uma t-configuração, e considere o subconjunto de índices consecutivos $\{i_j, i_{j+1} \ldots, i_t\} \subseteq C$, de cardinalidade r, com $r \geq 2$, além disso, suponha que $m_{i_j} \geq \gamma^* - t + j$. O conjunto que satisfaz estas condições é chamado de

r-conjunto não singular. Observe que se uma t-configuração contem um r-conjunto não singular, então segue do Lema 3.6 que a forma $\mathscr{F}$ possui um zero 3-ádico não trivial.

Dependendo da configuração C, ela possui subconjuntos que satisfazem uma serie de propriedades. Estes subconjuntos são chamados Blocos, os quais se definem como segue.

Definição 3.2.2. *Dada uma t-configuração $C = \{i_1, i_2, \ldots, i_t\}$, um subconjunto $B = \{i_j, i_{j+1}, \ldots, i_l\} \subseteq C$ é chamado Bloco de tamanho $|B|$ se são satisfeitas as seguintes propriedades :*

(i). $i_{r+1} = i_r + 1$ *para* $r = j, j+1, \ldots, l-1$.

(ii). $i_j \geq i_{j-1} + 2$;

(iii). $i_l \leq i_{l+1} - 2$;

com uma clara restrição para $j = 1$ e $l = t$. Se $|B| = 1$ é dito que B é um bloco unitário.

Da definição acima, tem-se que qualquer t-configuração pode ser expressada como a união disjunta de blocos, isto é,

$$C = B_1 \cup \cdots \cup B_m. \tag{3.15}$$

Observe que as propriedades (i), (ii), e (iii) da Definição acima, garantem que a representação (3.15) é única, a menos de ordem. Outro fato que é relevante no desenvolvimento do método é o conjunto de subconjuntos de C, cujos elementos são Blocos, tais que a união é C. Estes conjuntos são classificados segundo a sua cardinalidade, para isto começa-se com a seguente definição:

Definição 3.2.3. *Dada uma t-configuração $C = B_1 \cup \cdots \cup B_m$ e um inteiro n tal que $0 \leq n \leq t-1$, diz-se que C é uma (t, n)-configuração se*

$$\sum_{i=1}^{m} (|B_i| - 1) = n. \tag{3.16}$$

Para uma t-configuração C, o valor de $n \geq 0$ tem um papel central na classificação pelo número de Blocos, e são satisfeitas as seguintes propriedades:

Lema 3.12. *Seja C uma (t,n)-configuração e $n \geq 0$, então o número n representa a quantidade de níveis que satisfazem $i_j \in C$ com $i_{j+1} = i_j + 1$.*

Demonstração. Seja $C = B_1 \cup \cdots \cup B_m$ uma (t,n)-configuração, observe para B_i, com $i = 1, \ldots, m$, tem-se que $|B_i| - 1$ representa o número de níveis em B_i tais que se $i_j \in B_i$, então $i_{j+1} = i_j + 1$. $\square$

Proposição 3.1. *Quaisquer duas (t,n)-configurações possuem o mesmo número de blocos.*

Demonstração. Sejam C_0 e C_1 duas (t,n)-configurações, com $C_0 = B_1 \cup \cdots \cup B_m$ e $C_1 = D_1 \cup \cdots \cup D_r$. Observe que

$$\sum_{i=1}^{m} |B_i| = \sum_{j=1}^{r} |D_j| = t,$$

pois C_0 e C_1 são t-configurações. Agora, de (3.16), tem-se

$$t - m = \sum_{i=1}^{m} (|B_i| - 1) = n = \sum_{j=1}^{r} (|D_j| - 1) = t - r,$$

do qual se conclui que $m = r$ como queria ser provado. $\square$

Neste trabalho tem especial relevância as seguintes (t,n)-configurações.

Definição 3.2.4. *A (t,n)-configuração, com $n \geq 0$ e*

$$C = \bigcup_{i=1}^{m} B_i,$$

é chamada minimal, se $|B_1| = n + 1$ e $|B_j| = 1$ para $j = 2, 3, \ldots, m$.

Da 3-normalização (*ver* (1.18)), tem-se como estimar o número de variáveis nos níveis $0, 1, \ldots, \tau$, logo, existem varias maneiras possíveis de distribuir este número de variáveis nos diferentes níveis i, com $i \geq 1$, e cada uma de estas possibilidades resulta em uma (t,n)-configuração C, dessa forma, o que segue é encontrar o número de variáveis necessárias de C, de tal jeito que ela seja um t-conjunto não singular ou que contenha um r-conjunto não singular. De maneira introdutória para o que segue, considere o seguinte exemplo:

Exemplo 3.13. Seja $\mathscr{F}$ uma forma 3-normalizada como no Exemplo 3.11 e C uma 9-configuração. Observe que no Exemplo 3.11 não foram consideradas as possíveis contrações entre níveis de um mesmo bloco que podem ser feitas segundo o Lema 3.7. Assim, suponha inicialmente, para algum $1 < j \leq t$ que $i_{j-1}, i_j \in B$ um bloco de C, pelo Lema 3.10 tem-se $m_{i_j} \leq 9 + j$ (*ver* 3.13), mas do nível i_j é possível contrair um número de variáveis do nível i_{j-1} ao nível i_j, do que obtém-se pelo Lema 3.5 que *(ver Figura 3.3)*

$$\begin{aligned} m_{i_j} &\leq \gamma^* - t - 1 + j - \left\lfloor \frac{m_{i_{j-1}} - 2}{3} \right\rfloor \\ &= \gamma^* - t - 1 + j - \left\lfloor \frac{\gamma^* - t + j - 4}{3} \right\rfloor \\ &= 9 + j - \left\lfloor \frac{5 + j}{3} \right\rfloor. \end{aligned}$$

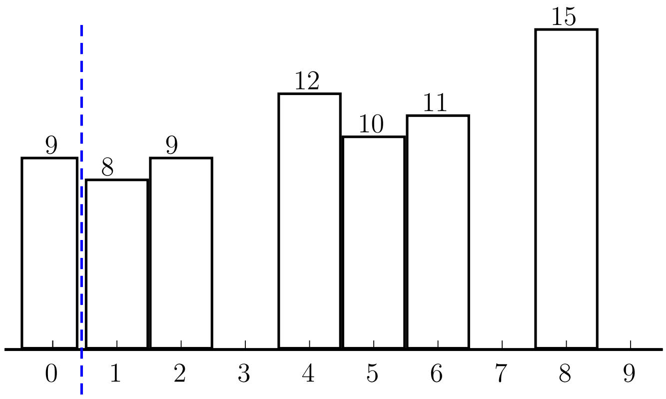

Figura 3.3: *Uma $(6,3)$-configuração (a partir da linha pontilhada) para o caso $\tau = 9$ considerando contrações entre níveis.*

Observe que pelo Lema 3.10 o nível 1 deve ter no máximo 10 variáveis (*ver* (3.14)), mas dado que podem ser contraídas variáveis do nível 0 ao nível 1, ele tem no máximo 8 variáveis. Por outra parte, os níveis 4 e 9, são o primeiro nível de seus blocos respetivos, portanto em eles não é alterada a limitante, mantendo assim, (3.14). Por outra parte, as limitantes expostas nos outros níveis, são consequência das contrações consecutivas entre níveis entre os blocos, segundo o Lema 3.7. Por exemplo, dado que o nível 4, tem no máximo 12 variáveis, então após contração, podem ser obtidas até 3 variáveis contraídas no nível 5, portanto o nível 5, tem no máximo 10 variáveis. Agora, contraindo variáveis do nível 5 ao nível 6 obtém-se que o nível 6 agora possui no máximo 13 variáveis, das quais podem se obter até 3 variáveis contraídas no nível 7, portanto o número máximo de variáveis em este nível é 11.

A partir de agora, se no Bloco B tem-se uma certa quantidade de variáveis, essa quantidade será denotada por Σ_B. Da mesma forma, denota-se por Σ_C o número de variáveis distribuídas nos níveis que constituem a configuração C.

Por outra parte, observe que na figura 3.3 o primeiro nível de cada bloco, determina as possíveis contrações nos níveis seguintes, e que naturalmente cada bloco possui um valor diferente; este valor depende da configuração e do número de níveis que há nos níveis inferiores ao bloco. Com isto, é introduzida a variável M, para dizer que certo bloco B de uma configuração, tem no máximo M variáveis no seu primeiro nível.

Teorema 3.14. *Seja $B = \{i_1, \cdots, i_l\}$ um bloco e fixe $M \in \mathbb{N}$. Se*

$$\Sigma_B > \Theta(B, M) = \sum_{i=0}^{l-1}(M+i) - \delta_B \sum_{i=0}^{l-2} \left\lfloor \frac{M+i-2}{3} \right\rfloor \tag{3.17}$$

onde

$$\delta_B = \begin{cases} 1, & se \quad l > 1 \\ 0, & caso\ contrário, \end{cases}$$

então podem-se contrair variáveis com a finalidade de obter um nível $i_j \in B$ com pelo menos $M + j$ variáveis.

Demonstração. Sem perda de generalidade assuma-se $B = \{1, 2, 3, \ldots, l\}$, e a prova é feita por indução sobre l. Para $l = 1$, tem-se $\delta_B = 0$ e diretamente de (3.17)

$$m_1 = \Sigma_B > M.$$

Agora, para $l = 2$, segue $B = \{1, 2\}$ com

$$\Sigma_B = m_1 + m_2 > M + (M+1) - \left\lfloor \frac{M-2}{3} \right\rfloor. \tag{3.18}$$

Se $m_1 > M$ nada a fazer, então, assuma $m_1 = M - \delta$ para algum $\delta \geq 0$ e isto junto com (3.18) implica

$$m_2 > M + 1 - \left\lfloor \frac{M-2}{3} \right\rfloor + \delta,$$

fazendo uso do Lemma 3.5 para as variáveis do nível 1, obtém-se

$$\begin{aligned} M + 1 - \left\lfloor \frac{M-2}{3} \right\rfloor + \delta + \left\lfloor \frac{M-\delta-2}{3} \right\rfloor &= M + 1 - \left\lfloor \frac{M-2}{3} \right\rfloor + \left\lfloor \frac{M-2}{3} + \frac{2\delta}{3} \right\rfloor \\ &\geq M + 1 \end{aligned} \tag{3.19}$$

variáveis no nível 2, portanto mantém-se o resultado.

Agora, suponha que o resultado é valido para $|B| < l$. Segue mostrar $|B| = l$, para cada $j \in \{1, 2, 3, \ldots, l-1\}$ defina-se

$$B_j = \{1, 2, \ldots, j\},$$

pela hipótese de indução, assuma-se

$$\Sigma_{B_j} = \Theta(B_j, M) = \left(\sum_{i=0}^{j-1} (M+i) - \delta_{B_j} \sum_{i=0}^{j-2} \left\lfloor \frac{M+i-2}{3} \right\rfloor \right) - \delta_j \tag{3.20}$$

para algum $\delta_j \geq 0$. Em particular de (3.17) e (3.20), tem-se

$$m_l > M + (l-1) - \left\lfloor \frac{M + (l-2) - 2}{3} \right\rfloor + \delta_{l-1}; \tag{3.21}$$

e dado que

$$\begin{aligned} m_j &= \Sigma_{B_j} - \Sigma_{B_{j-1}} \\ &= M + (j-1) - \left\lfloor \frac{M + (j-2) - 2}{3} \right\rfloor - \delta_j + \delta_{j-1} \end{aligned} \tag{3.22}$$

para $j = 2, 3, \ldots, l-1$ e $j = 1$ tem-se

$$m_1 = M - \delta_1, \tag{3.23}$$

para algum $\delta_1 \geq 0$, aplicando o Lema 3.5 para as variáveis do nível 1, além disso, por (3.22) e (3.23), tem-se pelo menos

$$M + 1 - \left\lfloor \frac{M-2}{3} \right\rfloor - \delta_2 + \delta_1 + \left\lfloor \frac{M - \delta_1 - 2}{3} \right\rfloor \geq M + 1 - \delta_2$$

variáveis no nível 2. Novamente, aplicando o Lema 3.5 para as variáveis do nível 2 e por (3.22) tem-se pelo menos $M + 2 - \delta_3$ variáveis no nível 3. Procedendo desta maneira, garanta-se após de sucessivas contrações que pelo menos existem $M + (l-2) - \delta_{l-1}$ no nível $l - 1$. Finalmente, fazendo uso do Lema 3.5 para as variáveis do nível $l-1$ o resultado segue por (3.21) de maneira semelhante ao caso $l = 2$. □

Em concordância com a procura do conjunto não singular, para uma t-configuração, tem-se que os níveis são da forma $\gamma^* - t + r$ para r algum inteiro (não necessariamente positivo, como se viu no exemplo da Figura 3.2). Assim, enquadrado este conceito no Teorema acima, tem-se o seguinte resultado.

Corolário 3.2. *Seja $C = B_1 \cup \cdots \cup B_m$ para quaisquer t-configuração. Denote-se $L_0 = 0$ e*

$$L_j = \sum_{i=1}^{j} |B_i|,$$

para cada $j \in \{1, 2, \cdots, m\}$. Se existe $j \in \{1, 2, \ldots, m\}$ tal que

$$\Sigma_{B_j} > \Theta(B_j, \gamma^* - t + L_{j-1}),$$

então a forma aditiva admite um zero não trivial.

Demonstração. Seja B_j com

$$\begin{aligned}\Sigma_{B_j} &> \Theta(B_j, \gamma^* - t + L_{j-1}) \\ &= \sum_{i=0}^{|B_j|-1} ((\gamma^* - t) + L_{j-1} + i) - \delta_{B_j} \sum_{i=0}^{|B_j|-2} \left\lfloor \frac{(\gamma^* - t) + L_{j-1} + i - 2}{3} \right\rfloor.\end{aligned}$$

Aplicando o Teorema 3.14 ao bloco B_j e fazendo $M = (\gamma^* - t) + L_{j-1}$, é possível concluir que existe $l \in \{1, 2, \ldots, |B_j|\}$ tal que o l-ésimo nível de B_j tem mais que $M + l = \gamma^* - (t - L_{j-1} - l)$ variáveis. Dado que existem $t - (L_{j-1} + l)$ níveis adiante que possuem variáveis, pois B_j é o bloco da t-configuração C, o resultado segue do Lema 3.6, isto é, este é um $(t - L_{j-1} - l)$ conjunto não singular. □

De maneira natural este resultado é estendido a qualquer bloco de uma configuração C, como segue.

Corolário 3.3. *Seja $C = B_1 \cup \cdots \cup B_m$ uma t-configuração e defina-se o número*

$$\begin{aligned}\Lambda(C) &= \sum_{i=1}^{m} \Theta(B_i, \gamma^* - t + L_{i-1}) \\ &= \sum_{i=0}^{t-1} (\gamma^* - t + i) - \sum_{i=0}^{t-2} \delta_i \left\lfloor \frac{(\gamma^* - t + i) - 2}{3} \right\rfloor,\end{aligned} \tag{3.24}$$

onde para $j = 1, 2, \ldots, m$ define-se

$$\delta_i = \begin{cases} 1, & se\ L_{j-1} \leq i < L_j\ e\ \ L_j - L_{j-1} > 1 \\ 0, & caso\ contrario. \end{cases}$$

Se $\Sigma_C > \Lambda(C)$, então a forma admite um zero não trivial.

Demonstração. Observe que o valor $\Lambda(C)$ em (3.24) não é mais que a reescrita de (3.17) para todos os blocos em C, assim, a prova segue diretamente do Corolário 3.2. □

Fixando $t \in \{1, \ldots, \tau\}$ e $n \in \{0, 1, \ldots, t-1\}$ o número de (t, n)-configurações esta dado por $\binom{t-1}{n}$. Logo, não seria só desgastante, senão ineficiente, provar (ou comprovar) para cada uma destas (t, n)-configurações o Corolário 3.3. Claramente, uma solução para uma (t, n)-configuração dada com um determinado número de variáveis, não é suficiente para obter uma solução para as outras. Assim, procura-se uma (t, n)-configuração que possua o maior número de variáveis em virtude da equação (3.24), para a qual a existência de uma solução não trivial garanta a existência de soluções não triviais para quaisquer outra (t, n)-configuração. Denota-se por $\Psi(t, n)$ o somatório em (3.24) quando C é uma (t, n)-configuração minimal, isto é,

$$\Psi(t, n) = \sum_{i=0}^{t-1} (\gamma^* - t + i) - \delta_n \sum_{i=0}^{n-1} \left\lfloor \frac{(\gamma^* - t + i) - 2}{3} \right\rfloor, \tag{3.25}$$

com

$$\delta_n = \begin{cases} 1, & \text{se} \quad n > 0 \\ 0, & \text{se} \quad n = 0 \end{cases}.$$

Da mesma forma que foi feito para os blocos e a função Θ, a definição acima pode ser ainda mais geral introduzindo a variável M que depende da configuração, e em virtude disto e, sempre que não exista ambiguidade, será usada a mesma letra Ψ para a seguinte função: Seja $M \in \mathbb{N}$ defina-se

$$\Psi(t,n,M) = \sum_{i=0}^{t-1}(M+i) - \delta_n \sum_{i=0}^{n-1} \left\lfloor \frac{(M+i)-2}{3} \right\rfloor \tag{3.26}$$

Desta forma, segue que $\Psi(t,n) = \Psi(t,n,\gamma^*-t)$. A introdução do termo M facilitará a notação e as operações feitas no capítulo 4, e da mesma maneira que foi introduzida na definição da função . Por outra parte, observe que se C é uma (t,n)-configuração minimal, então

$$\Psi\left(t,n\right) = \Lambda\left(C\right).$$

Corolário 3.4. *Se C é qualquer (t,n)-configuração e $\Sigma_C > \Psi(t,n)$, então a forma aditiva possui um zero não trivial.*

Demonstração. Seja C_0 uma (t,n)-configuração, segue do Lema 3.12 que no sumátorio (3.24), precisamente n dos $\delta_i's$ são iguais a 1, dado que a função $\lfloor x/3 \rfloor$ é não decrescente, o maior valor de $\Lambda(C_0)$ acontece quando $\delta_i = 1$, para todo $i = 0, 1, \ldots, n-1$, e isto acontece se, e somente se, C_0 é uma (t,n)-configuração minimal. Daí, tomando C_0 como uma (t,n)-configuração minimal, tem-se que para quaisquer (t,n)-configuração C,

$$\Lambda(C_0) = \Psi(t,n) \geq \Lambda(C),$$

e o resultado segue do Corolário 3.3. □

Agora, seja C uma t-configuração e suponha que existe r um inteiro positivo, tal que $m_0 = \gamma^* - r$, com $r > t$. Isto implica, que o número de níveis que possui C não é suficiente para satisfazer as condições do Lema 3.6, a saber, são necessários pelo menos $r-t$ níveis a mais, com pelo menos uma variável. Se existem $r-t$ blocos de tal maneira que após de contrações dentro dos níveis destes blocos ou mesmo, se seu último nível tem um número suficiente de variáveis para contrair aos $r-t$ níveis vazios que seguem a cada um destes blocos, então podem ser satisfeitas as condições do Lema 3.6 e portanto, tem-se uma solução não singular. Claramente, se o nível τ é um destes níveis, esta afirmação não é mantida.

Do dito acima, o que se quer é precisamente trabalhar no caso quando não é possível obter estes $r-t$ novos níveis a partir dos blocos da t-configuração. Isto que em um primeiro olhar parece desfavorável, é por demais uma grande vantagem pois, é obtido um novo somatório de termos negativos na equação (3.24).

Definição 3.2.5. *Um bloco $B=\{i_1,i_2,\ldots,i_n\}$ de uma t-configuração C é chamado de l-bloco se no nível i_n existem pelo menos l variáveis. Se o último nível do bloco B tem no máximo l variáveis, diz-se B é um l-bloco limitado.*

Exemplo 3.15. Seja $k=3^9$ e considere uma forma aditiva $\mathscr{F}$ como no Exemplo 3.11. Alem disso, considere $m_0=10$, e C uma $(4,2)$-configuração como na Figura 3.4 e suponha que $i_4<\tau$. Neste caso, os dois blocos, são blocos 4-limitados. Por outra parte, observe que se i_j possui pelo menos 5 variáveis para $j=2,4$ ou seja, B_1 e B_2, então pelo lema 3.5, pode ser obtida pelo menos uma variável nos níveis i_{j+1}, e portanto teria-se pelo Lema 3.6 aplicado ao nível 0, uma zero não trivial.

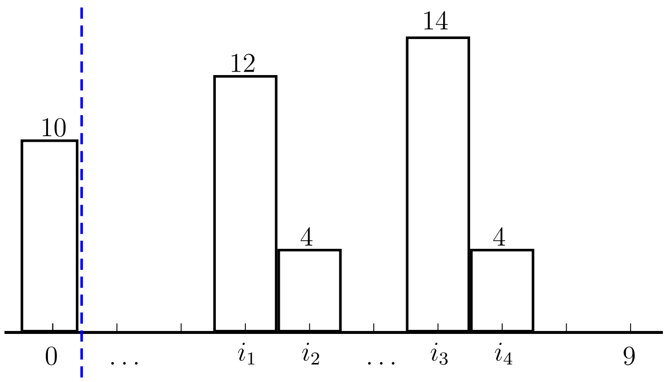

Figura 3.4: *Uma $(4,2)$-configuração (a partir da linha pontilhada) para o caso $\tau=9$ com dois 4-blocos limitados.*

Proposição 3.2. *Seja $B=\{i_1,i_2,\ldots,i_n\}$ um bloco l-limitado não unitário e fixe $M\in\mathbb{N}$. Se*

$$\Sigma_B>\Theta(B,M)-\left((M+n-1)-\left\lfloor\frac{M+(n-2)-2}{3}\right\rfloor-l\right),$$

então é possível contrair variáveis e obter pelo menos um nível $i_j\in B-\{i_n\}$ com mais que $M+j$ variáveis.

Demonstração. Sem perda de generalidade assuma-se $B=\{1,2,\ldots,n\}$. Além disso, considere $B'=\{1,2,\ldots,n-1\}$, dado que B é um bloco l-limitado, tem-se

$$
\begin{aligned}
\Sigma_{B'} &\geq \Sigma_B - l\\
&> \Theta(B,M) - \left((M+n-1) - \left\lfloor \frac{M+(n-2)-2}{3} \right\rfloor - l\right) - l\\
&= \Theta(B,M) - \left((M+n-1) - \left\lfloor \frac{M+(n-2)-2}{3} \right\rfloor\right)\\
&= \Theta(B',M).
\end{aligned}
$$

e o resultado segue do Teorema 3.14. □

Desta maneira, obtém-se uma reformulação do Corolário 3.3, sempre que seja necessário considerar a quantidade de blocos l-limitados em uma configuração.

Corolário 3.5. *Considere uma t-configuração $C = B_1 \cup B_2 \cup \cdots \cup B_m$, e assuma que os blocos $B_{i_1}, B_{i_2}, \ldots, B_{i_p}$ são blocos l-limitados. Seja*

$$
b_{i_j} = \begin{cases} \left((\gamma^* - t + L_{i_j} - 1) - \left\lfloor \frac{(\gamma^* - t + L_{i_j} - 2) - 2}{3} \right\rfloor\right) - l, & \textit{se} \quad |B_{i_j}| \geq 2,\\ (\gamma^* - t + L_{i_j} - 1) - l, & \textit{se} \quad |B_{i_j}| = 1. \end{cases} \tag{3.27}
$$

Se $\Sigma_C > \Lambda(C) - \sum_{j=1}^{p} b_{i_j}$, então tem-se um zero não trivial.

Demonstração. Sejam C uma t-configuração e $\mathcal{L} = \{i_1, \ldots, i_p\}$. Tem-se que

$$
\Lambda(C) - \sum_{j=1}^{p} b_{i_j} = \sum_{\substack{i=1\\ i \notin \mathcal{L}}}^{m} \Theta\left(B_i, \gamma^* - \gamma\right) + \sum_{j=1}^{p} \Theta\left(B_{i_j}, \gamma^* - \gamma\right) - b_{i_j}.
$$

Dado que por hipótese $\Sigma_C > \Lambda(C) - \sum_{j=1}^{p} b_{i_j}$, isto implica que existe pelo menos um bloco l-limitado B_{i_j}, tal que

$$
\Sigma_{B_{i_j}} > \Theta\left(B_{i_j}, \gamma^* - \gamma\right) - b_{i_j},
$$

portanto o resultado segue da Proposição 3.2. Caso contrario, existe B_i para $i \notin \mathcal{L}$ tal que

$$
\Sigma_{B_i} > \Theta\left(B_i, \gamma^* - \gamma\right),
$$

e o resultado segue pelo Teorema 3.14. □

Como resultado do Corolário 3.4, daqui em diante é assumido o termo t-configuração, como t-configuração minimal, sempre que não seja ambíguo.

As que seguem, são propriedades que serão fortemente usadas na seção 4.2. Em virtude do Corolário 3.4, é usada a representação minimal e por tanto, todas as igualdades abaixo são usadas as equações (3.25) e (3.26). Estas propriedades vistam de relacionar as quantidades de variáveis que possuem as diferentes t-configurações, e ainda mais, as (t, n)-configurações, com a finalidade de expressar ditas quantidades em termos de uma (t, n)-configuração dada. São estabelecidas duas relações, ou por número de blocos dentro de uma mesma t-configuração, como em *(a)* e *(c)*, ou por igual número de blocos entre diferentes t-configurações. Por exemplo: a propriedade 3.3.*(b)*, estabelece a variação do número de variáveis para configurações que tem o mesmo número de blocos, ou seja, para $h \in \mathbb{Z}^+$, se m é o número de blocos de uma (t, n)-configuração, então m é o número de blocos de uma $(t-h, n-h)$-configuração, mas o número de variáveis não é necessariamente o mesmo, esta diferencia esta dada por *(b)* da seguinte proposição.

Proposição 3.3. *Para t, n, ε e M inteiros positivos as seguintes são satisfeitas as seguintes propriedades:*

(a). $\Psi(t, n, M)$ *é estritamente crescente como função de t e estritamente decrescente como função de n.*

(b). $$\Psi(t, n, M) - \Psi(t-\omega, n-\omega, M+\omega) = \begin{cases} \displaystyle\sum_{i=0}^{\omega-1} M + i - \left\lfloor \frac{M+i-2}{3} \right\rfloor, & se \;\; \omega > 0; \\ 0, & se \;\; \omega = 0. \end{cases}$$

(c). $$\Psi(t, n-\varepsilon, M) - \Psi(t, n, M) = \begin{cases} \displaystyle\sum_{i=0}^{\varepsilon-1} \left\lfloor \frac{M+n-\varepsilon+i-2}{3} \right\rfloor, & se \;\; \varepsilon > 0; \\ 0, & se \; \varepsilon = 0 \end{cases}$$

(d). $$\Psi(t, n, M) - \Psi(t, n, M-1) = t + \left\lfloor \frac{M}{3} \right\rfloor - \left\lfloor \frac{M+n}{3} \right\rfloor \text{ para quaisquer } M \geq 1.$$

Demonstração. A prova de *(a)* decorre de maneira imediata de (3.26). Agora, para *(b)*, se $\omega = 0$ nada a fazer, portanto tome $\omega \geq 1$, de (3.26), tem-se

$$\begin{aligned}
\Psi(t,n,M) - \Psi(t-\omega, n-\omega, M+\omega) &= \sum_{i=0}^{t-1}(M+i) - \sum_{i=0}^{n-1}\left\lfloor \frac{M+i-2}{3} \right\rfloor \\
&\quad - \sum_{i=0}^{t-\omega-1}(M+\omega+i) + \sum_{i=0}^{n-\omega-1}\left\lfloor \frac{M+\omega+i-2}{3} \right\rfloor \\
&= \sum_{i=0}^{\omega-1}(M+i) - \sum_{i=0}^{n-1}\left\lfloor \frac{M+i-2}{3} \right\rfloor \\
&\quad + \sum_{i=\omega}^{n-1}\left\lfloor \frac{M+i-2}{3} \right\rfloor \\
&= \sum_{i=0}^{\omega-1}(M+i) - \sum_{i=0}^{\omega-1}\left\lfloor \frac{M+i-2}{3} \right\rfloor.
\end{aligned}$$

As propriedades *(c)* e *(d)*, seguem de maneira semelhante. $\square$

Capítulo

4

Limitante Superior para $\Gamma^*(3^\tau, 3)$

Neste Capitulo mostra-se o Teorema 1, para isto lembra-se que é assumido sempre $\mathscr{F}$ como uma forma aditiva 3-normalizada de grau $k = 3^\tau$ em $s \geq k(\gamma^* - \gamma) + 1$ variáveis, satisfazendo as propriedades do Lema 1.8, onde $\gamma^* = \lfloor \gamma \log_2(3) \rfloor + 1$ e $\gamma = \tau + 1$. Por outra parte sempre que seja falado de *solução não singular*, se faz referencia a solução não singular modulo p^γ da congruência

$$\mathscr{F} \equiv 0 \pmod{p^\gamma}.$$

Começa-se enunciando o Teorema

Teorema 1. *Seja $\tau \geq 1$ e $k = 3^\tau$, então*

$$\Gamma^*(k, 3) \leq k(\gamma^* - \gamma) + 1. \tag{4.1}$$

4.1 O método para $\tau \leq 7$

A prova do Teorema 1 para o caso $\tau \leq 7$ divide-se em cada um dos valores de $3 \leq \tau \leq 7$. A estrutura da prova em cada um dos casos varia segundo o valor de τ, mas essencialmente, tomam-se cada um dos valores que pode assumir o nível m_0 pela 3-normalização e o Lema 3.6, ou seja, $\gamma^* - \gamma + 1 \leq m_0 \leq \gamma^* - 1$, junto com a possibilidade de variáveis no nível $\tau + 1$ (e $\tau + 2$ em alguns casos) e é feita uma contagem de variáveis, para depois analisar sua distribuição. Finalmente, em todos os casos usa-se o Lema 3.6.

Caso $\tau = 3$.

Para $\tau = 3$ tem-se que $\gamma^* = 7$, assim, tome $m_0 = \gamma^* - t$ com $1 \leq t \leq 3$. Pela Proposição 2.2 tem-se solução não trivial quando $t = 1, 2$ portanto considere $t = 3$, isto é, $m_0 = 4$. Se $m_4 = 0$ pela 3-normalização, tem-se

$$m_1 + m_2 + m_3 + m_4 \geq 12,$$

logo se estes três níveis possuem pelo menos uma variável, o resultado segue do Lema 3.6, portanto assuma que apenas dois níveis possuem variáveis, mas isto implica que cada nível possui pelo menos $\gamma^* - 1 = 6$ variáveis e novamente pelo Lema 3.6 a forma possui uma solução não singular. Agora, se $m_4 \geq 1$ pelo Lema 3.6 implica que $m_i \leq 5$ para $i = 1, 2, 3$, daí, se $m_1 = 5$, pela 3-normalização, tem-se $m_2 + m_3 \geq$, logo pelo menos um dos níveis 2 ou 3 possui pelo menos uma variável, portanto o resultado segue do Lema 3.6 aplicado desde o nível 1 ate o nível 4. Finalmente, quando $3 \leq m_1 \leq 4$, se $m_2 = 5$ pelo Lema 3.5 é possível contrair variáveis do nível 2 e obter uma nova variável no nível 3, e se $m_2 \leq 4$ pela 3-normalização obtém-se 3 níveis com variáveis. Portanto, em qualquer dos dois casos anteriores o resultado segue ao aplicar o Lema 3.6. Assim, em quaisquer dos casos obtém-se uma solução não singular, do que se conclui (4.1).

Caso $\tau = 4$

Quando $\tau = 4$, tem-se $\gamma^* = 8$, deste modo, tome $m_0 = \gamma^* - t$ com $3 \leq t \leq 4$. Para $t = 3$ se tem $m_0 = 5$, assim, assuma primeiro que $m_5 = 0$, isto implica que

$$\sum_{i=1}^{5} m_i \geq 14$$

o que implica a existência de dois níveis com variáveis com pelo menos 7 variáveis, logo pelo Lema 3.6 implica uma solução não singular. Agora, quando $m_5 \geq 1$ implica que $m_i \leq 6$ para quaisquer $i = 1, 2, 3, 4$; por outra parte, pela 3-normalização, tem-se 11 variáveis entre os nível 1 e o nível 4, se estas variáveis estão distribuídas em 3 ou 4 níveis, o resultado segue do Lema 3.6, portanto, assuma que estas variáveis são distribuídas em só dois níveis, isto é, para $i_1, i_2 \in \{1, 2, 3, 4\}$ (sem perda de generalidade assuma $i_1 < i_2$) tem-se $m_{i_1} = r$ e $m_{i_2} = 11 - r$ com $4 \leq r \leq 7$, mas dado que quaisquer dos níveis tem no máximo 6 variáveis, segue que ou, $m_{i_1} = 6$ e

$m_{i_2} = 5$ ou, $m_{i_1} = 5$ e $m_{i_2} = 6$. No primeiro caso, dado que $m_{i_1} = 6$ e existem dois níveis com variáveis até o nível 5, o resultado segue do Lema 3.6 portanto, assuma $m_{i_1} = 5$. Pela 3-normalização $i_1 = 1$ e $2 \leq i_2 \leq 3$, logo pelo Lema 3.5 é possível contrair duas ou três variáveis do nível i_2 para ter uma nova variável no nível i_2+1 e assim tem-se 3 níveis com variáveis e, obtém-se uma solução não singular pelo Lema 3.6.

Agora, suponha que o nível 0 possui $\gamma^* - 4 = 4$ variáveis assim, se $6 \leq m_1 \leq 7$ como

$$\sum_{i=2}^{5} m_i \geq 8,$$

então existem pelo menos dois níveis com pelo menos uma variável no conjunto de níveis $\{2, 3, 4, 5\}$, e é suficiente aplicar o Lema 3.6 ao nível 1. Por outra parte, se $m_1 = 5$ e $6 \leq m_2 \leq 7$, tem-se

$$\sum_{i=3}^{6} m_i \geq 6,$$

logo se existem dois níveis com pelo menos uma variável, a forma aditiva possui uma solução não singular, portanto, assuma que existe apenas um nível i_1 com este número de variáveis daí, pela 3-normalização, dito nível pertence a $\{3, 4, 5\}$ e pelo Lema 3.5 pode-se contrair duas ou três variáveis do nível i_1 para obter uma nova variável no nível $i_1 + 1$ e o resultado segue do Lema 3.6.

Se $1 \leq m_2 \leq 5$, então

$$\sum_{i=3}^{5} m_i \geq 5.$$

Novamente, se estas variáveis são distribuídas em dois níveis, o resultado segue aplicando o Lema 3.6 ao nível 1. Assim, se estas 5 variáveis estão apenas em um nível i_1 e este nível pertence a $\{3, 4\}$, logo usando o Lema 3.5 para contrair variáveis do nível i_1 ao nível $i_1 + 1$ o resultado segue do Lema 3.6 aplicado ao nível 1.

Com o anterior, seja $3 \leq m_1 \leq 4$, se $6 \leq m_2 \leq 7$, obtém-se solução não singular como no caso de 5 variáveis no nível 1. Agora, se $m_1 = 4$ obtém-se

$$\sum_{i=2}^{4} m_i \geq 8.$$

Daí, se estas variáveis estão distribuídas nos 3 seguintes níveis, basta usar o Lema 3.6. Portanto, assuma que estas 8 variáveis estão apenas em dois níveis, isto é, $m_{i_1} = r$ e $m_{i_2} = 8 - r$ com $2 \leq r \leq 5$, pela 3-normalização $i_1 = 2$ e se $r = 2, 3$ o resultado segue do Lema 3.5 contraindo variáveis do nível 3 ao nível 4, obtendo assim 4 níveis com variáveis. Agora, se $m_2 = 4$ pela 3-normalização e o Lema 3.5, obtém-se $m_3 = 4$ e $m_5 \geq 1$ daí, pelo Lema 3.1 podem-se contrair duas variáveis do nível 0 a um nível $l \geq 1$; Se $l \geq 5$ o resultado segue do Lema de Hensel 1.9, logo assuma $1 \leq l < 4$, segue do Lema 3.5 aplicando contrações desde nível l até obter pelo menos uma variável no nível 4 e o resultado segue aplicando o Lema 3.6 ao nível 1. Quando $l = 4$ é imediato.

Por outra parte, se $m_2 = 5$ e $m_3 = 0$ basta contrair pelo Lema 3.5 variáveis do nível 2 para obter uma variável no nível 3, e assim ter pelo menos uma variável em cada um dos níveis desde o primeiro nível até o quarto nível portanto, $m_3 = 3$ e o análise é semelhante ao caso $m_2 = 4$. Finalmente, se $m_1 = 3$, tem-se $m_2 = r$ e $m_3 = 9 - r$ com $3 \leq r \leq 5$. Pela 3-normalização tem-se $3 \leq m_2 \leq 5$ e $4 \leq m_3 \leq 6$ daí, usando o Lema 3.5 para contrair variáveis do nível 3 ao nível 4 ou, fazendo de maneira iterada contrações desde o nível 2 a fim de obter uma variável no nível 4, obtém-se em quaisquer caso 4 níveis com variáveis e o resultado segue do Lema 3.6.

Dado que para cada $m_0 = 4, 5, 6, 7$ obtém-se uma solução não singular, segue que quaisquer forma aditiva de grau 3^4 com $3^5 + 1$ variáveis possui um zero 3-ádico.

Caso $\tau = 5$.

Quando $\tau = 5$ tem-se $\gamma^* = 10$, e do Lema 2.7, tem-se solução não singular para $m_0 = \gamma^* - t$ com $t \leq 3$. Assim, seja $t = 4$ portanto $m_0 = 6$ e $1 \leq m_1 \leq 9$, Se $7 \leq m_1 \leq 9$, então da 3-normalização tem-se

$$\sum_{i=2}^{5} m_i \geq 10,$$

logo, existem pelo menos dois níveis com pelo menos uma variável entre o conjunto de níveis $\{2, 3, 4, 5\}$ daí, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 1 de tal maneira que $m_1 \geq 8$ e o resultado segue do Lema 3.6. Agora, para

$3 \leq m_1 \leq 6$ se, $8 \leq m_2 \leq 9$, tem-se

$$\sum_{i=3}^{7} m_i \geq 12.$$

Portanto, existem pelo menos dois níveis no conjunto $\{3, 4, \ldots, 7\}$ que possuem pelo menos uma variável, e o resultado segue do Lema 3.6 aplicado ao nível 2. Desse modo, assuma $1 \leq m_2 \leq 7$ do que obtém-se

$$\sum_{i=3}^{5} m_i \geq 6.$$

Se este número de variáveis é distribuído em dois níveis, o resultado é imediato pelo Lema 3.6 portanto, assuma que as 6 variáveis estão somente em um nível, tem-se pela 3-normalização que este nível deve ser ou, o nível 3 ou, o nível 4, e em quaisquer dos casos pelo Lema 3.5 podem-se contrair duas ou 3 variáveis ao nível seguinte, obtendo 4 níveis além do nível 0, com pelo menos uma variável e novamente, o resultado segue do Lema 3.6. Portanto, a forma aditiva com 6 variáveis no nível 0 possui solução não singular.

Já foi mostrado que existe solução para $m_0 = \gamma^* - t$ com $1 \leq t \leq 4$, o que reescrito em forma do Corolário 3.1 é: A forma aditiva possui solução não singular para (3.12) quando $m_0 = \gamma^* - \gamma + t$ para

$$H = 1 < t \leq \gamma - 1 = 5.$$

Daí, quando $m_0 = \gamma^* - \gamma + 1 = 5$, a congruência (3.12) possui solução não singular. Com isto conclui-se que, quaisquer forma aditiva com $3^5 \cdot 5 + 1$ variáveis possui uma solução não singular módulo 3^6, como se queria mostrar.

Caso $\tau = 6$.

Se $\tau = 6$, tem-se $\gamma^* = 12$ assim, seja $m_0 = 12 - t$ com $3 \leq t \leq 6$. Pelo Lema 2.7 tem-se solução não singular quando $t \geq 3$, e por outra parte, se é mostrado que a forma aditiva possui solução quando o nível 0 possui $12 - t$ variáveis com $1 \leq t \leq 5$ pelo Corolário 3.1 tem-se imediatamente o caso $m_0 = 6$. Daí, mostra-se os casos quando $4 \leq t \leq 5$.

Se $t = 4$, tem-se $m_0 = 8$ e, portanto $3 \leq m_1 \leq 11$. Se $8 \leq m_1 \leq 11$, tem-se

$$\sum_{i=2}^{6} m_i \geq 17,$$

isto implica que existem dois níveis com pelo menos uma variável daí, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 1, tem-se $m_1 \geq 10$ e o resultado segue do Lema 3.6. Agora, se $3 \leq m_1 \leq 7$, tem-se

$$\sum_{i=2}^{6} m_i \geq 21,$$

o resultado é imediato se este número de variáveis esta distribuído em 3 níveis diferentes. Desta maneira, suponha que apenas são distribuídas em 2 níveis, assim, $m_{i_j} \geq 10$, com $j = 1, 2$ e $2 \leq i_1 < i_2 \leq 6$. Com isto, assuma $m_{i_1} + m_{i_2} \geq 21$, dado que $m_0 + m_1 \leq 15$, tem-se $m_2 > 1$, portanto $i_1 = 2$ e $3 \leq i_2 \leq 5$. Daí, o resultado segue de usar o Lema 3.5 para contrair variáveis do nível i_2 ao nível $i_2 + 1$, e posteriormente usar o Lema 3.6.

Quando $t = 5$, tem-se $m_0 = 7$ e $4 \leq m_1 \leq 11$. Se $9 \leq m_1 \leq 11$, então

$$\sum_{i=2}^{6} m_i \geq 18.$$

Daí, existem pelo menos dois níveis com pelo menos uma variável, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 1, tem-se $m_i \geq 10$ e o resultado segue do Lema 3.6. Por outra parte, se $4 \leq m_1 \leq 8$, tem-se $9 \leq m_2 \leq 11$, isto implica

$$\sum_{i=3}^{7} m_i \geq 15,$$

portanto, existem pelo menos dois níveis entre em $\{3, \ldots, 7\}$ com pelo menos uma variável. Daí, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 2, tem-se $m_2 \geq 10$ e o resultado segue do Lema 3.6.

Agora, suponha que $1 \leq m_2 \leq 8$, isto implica que

$$\sum_{i=3}^{6} m_i \geq 13.$$

Se ditas variáveis estão distribuídas em 3 níveis, o resultado é imediato. Então, assuma que se distribuam em apenas dois níveis, daí $m_{i_1} + m_{i_2} \geq 13$. Dado que $m_0 + m_1 + m_2 \leq 23$, isto implica que $i_1 \in \{3, 4\}$. Se $m_{i_1} = 11$ tem-se $m_{i_2} \geq 2$ e o resultado segue do Lema 3.6. Se $8 \leq m_{i_1} \leq 10$, então $m_{i_2} \geq 3$. Daí, se $m_{i_2} = m_{i_1+1}$, pelo Lema 3.5 pode-se contrair variáveis do nível i_1 ao nível i_2 de tal maneira que $m_{i_2} \geq 5$ e de novo é possível usar o Lema 3.5 no nível i_2 para obter uma variável no nível seguinte, e o resultado segue do Lema 3.6. Caso contrario basta usar o Lema 3.5 no nível i_1 para contrair variáveis ao nível $i_1 + 1$ seguido do Lema 3.6. Finalmente, se $1 \leq m_{i_1} \leq 7$, tem-se $m_{i_2} \geq 6$ assim, $m_0 + m_1 + m_2 + m_{i_1} \leq 30$, portanto, $i_1 < i_2 \leq 5$. Assim, é suficiente usar o Lema 3.5 para contrair variáveis do nível i_2 de tal maneira $m_{i_2+1} \geq 1$, e o resultado segue do Lema 3.6.

Logo, pelo mostrado anteriormente e pelo Corolário 3.1 toda forma aditiva $\mathscr{F}$ de grau $k = 3^6$ satisfaz

$$\Gamma^*(k, 3) \leq 3^6 \cdot 5 + 1.$$

Caso $\tau = 7$.

Quando $\tau = 7$ tem-se que $\gamma^* = 13$, considerando $m_0 = 13 - t$, tem-se pelo Lema 2.7 que existe solução quando $1 \leq t \leq 3$. Assim, inicialmente seja $t = 4$, isto é, $m_0 = 9$ o que implica que $2 \leq m_1 \leq 12$. Mas,

$$\sum_{i=2}^{7} m_i \geq 20,$$

isto implica que existem 2 níveis com pelo menos uma variável (se for 3 níveis, já tem solução). Daí, tem-se $m_{i_1} + m_{i_2} \geq 20$ com $m_{i_j} \geq 8$ para $j = 1, 2$. Logo pelo Lema 3.5, podem ser contraídas 2 ou três variáveis a um nível vazio ou, após de sucessivas contrações entre níveis obter uma variável em um nível vazio o que dão 3 níveis com pelo menos uma variável, e o resultado segue do Lema 3.6.

Se $t = 5$, tem-se $m_0 = 8$ e $3 \leq m_1 \leq 12$. Se $8 \leq m_1 \leq 12$, tem-se da 3-normalização a existencia de pelo menos 21 variáveis no conjunto de níveis $\{2, \ldots, 7\}$. Assuma que dito número de variáveis é distribuído em apenas dois níveis, assim $m_{i_j} \geq 9$ para $j = 1, 2$, isto é, $m_{i_1} = r$ e $m_{i_2} = 21 - r$ para $9 \leq r \leq 12$, isto, junto com a 3-normalização, implica que podem ser obtidos 3 níveis contraindo variáveis de maneira iterada entre níveis consecutivos até um nível vazio, ou bem contraindo diretamente a um nível vazio. Daí, usando o Lema 3.5 para contrair variáveis do nível 0, obtém-se duas novas variáveis no nível 1, de tal forma que $m_1 \geq 10$ e o resultado segue do Lema 3.6. Por outra parte, se $3 \leq m_1 \leq 7$, implica que $1 \leq m_2 \leq 12$, logo

$$\sum_{i=3}^{7} m_i \geq 14.$$

Assim, existem pelo menos dois níveis tais que $m_{i_1} + m_{i_2} \geq 14$ com $3 \leq i_1 \leq 5$, e $m_{i_j} \geq 2$ para $i = 1, 2$ e segue um razoamento semelhante ao caso anterior para obter 3 níveis com pelo menos uma variável, e novamente, o resultado segue do Lema 3.6.

Se $t = 6$, então $m_0 = 7$ e $4 \leq m_1 \leq 12$. Assim, se $8 \leq m_1 \leq 12$, da 3-normalização tem-se

$$\sum_{i=2}^{8} m_i \geq 27,$$

portanto existem 3 níveis entre os níveis no conjunto $\{2, \ldots, 8\}$ com pelo menos 3 variáveis, o que implica, por um razoamento semelhante ao caso $t = 6$, que destes três níveis podem-se obter 4 níveis com pelo menos uma variável e pelo Lema 3.5, contraindo variáveis do nível 0 ao nível 1, tem-se $m_1 \geq 9$. Agora, seja $m_1 = 7$ e $7 \leq m_2 \leq 12$, segue

$$\sum_{i=3}^{9} m_i \geq 25.$$

Daí, existem pelo menos 3 níveis não vazios entre o níveis $\{3, 4, \ldots, 9\}$ e, o resultado segue o bem do Lema 3.6 aplicado a estes 3 níveis ou obtendo 4 níveis usando contrações (iteradas se for o caso) destes três níveis e depois usando o Lema 3.5 desde o nível 0 ao nível 2 tal que $m_2 \geq 9$. Por outra parte, se $2 \leq m_2 \leq 6$ implica $1 \leq m_3 \leq 12$ e obtém-se assim

$$\sum_{i=4}^{8} m_i \geq 14$$

com o qual, tem-se pelo menos dois níveis não vazios nos níveis $\{4, 5, \ldots, 8\}$ com os quais é possível obter mais um nível com pelo menos uma variável, daí, usando o Lema 3.5 para contrair variáveis desde o nível 0 ao nível 1, obtém-se $m_1 \geq 8$, e o resultado segue do Lema 3.6. Se $4 \leq m_1 \leq 6$ e $8 \leq m_2 \leq 12$, tem-se

$$\sum_{i=3}^{9} m_i \geq 26,$$

isto implica que existem pelo menos 3 níveis não vazios nos níveis $\{3, \ldots, 9\}$, com o que após de contrações obtém-se pelo menos mais um nível com variáveis, isto é, 4 níveis com pelo menos uma variável. Com isto, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 2 de tal maneira que $m_2 \geq 9$, o resultado segue do Lema 3.6. Agora, se $4 \leq m_2 \leq 7$ implica que $1 \leq m_3 \leq 12$ assim, para $9 \leq m_3 \leq 12$ existem pelo menos 2 níveis não vazios entre os níveis $i_1, i_2 \in \{4, 5, \ldots, 8\}$ tais que $m_{i_1} + m_{i_2} \geq 14$, com o qual, obtém-se pelo menos mais um nível com variáveis e, usando o Lema 3.5 para contrair variáveis do nível 0 ao nível 3 de tal forma que $m_i \geq 10$ o resultado segue do Lema 3.6. Por outra parte, se $2 \leq m_3 \leq 8$ tem-se

$$m_0 + m_1 + m_2 + m_3 \leq 28,$$

isto implica que existem pelo menos dois níveis não vazios $i_1, i_2 \in \{4, 5, \ldots, 8\}$ tais que $m_{i_1} + m_{i_2} \geq 18$ daí, o bem aplicando o Lema 3.6 a estes dois níveis ou, usando contrações de variáveis destes níveis para obter mais um nível com pelo menos uma variável, o resultado segue do Lema 3.6.

Finalmente se $m_2 = 3$, tem-se $m_0 = 7$ e $m_1 = 6$ com isto existem pelo menos 3 níveis não vazios entre os níveis $\{3, 4, \ldots, 7\}$ os quais somam pelo menos 25 variáveis, isto implica que cada nível tem pelo menos 3 variáveis e, usando o Lema 3.5 para contrair variáveis entre níveis consecutivos ou, de um nível com variáveis ao seguinte nível vazio, é possível obter 4 níveis com pelo menos uma variável, daí, usando o Lema 3.6 conclui a prova para o caso $t = 6$. Com isto, e com o Corolário 3.1 segue para uma forma aditiva de grau 3^7 que

$$\Gamma(3^7, 3) \leq 3^7 5 + 1.$$

4.1.1 Prova do Teorema 1 para $1 \leq \tau \leq 7$

Pela Proposição 2.1, tem-se para $\tau = 1, 2$ que

$$\Gamma^* \left(3, 3\right) \leq 7 \quad \text{e} \quad \Gamma^* \left(3^2, 3\right) \leq 19$$

Logo, com isto e com em todos os casos já vistos para $3 \leq \tau \leq 7$ conclui-se que é satisfeita (4.1), isto é, para $1 \leq \tau \leq 7$,

$$\Gamma^*(3^\tau, 3) \leq 3^\tau(\gamma^* - \gamma) + 1. \tag{4.2}$$

4.2 O método para $\tau \geq 8$

Para estruturar o método da prova no caso $\tau \geq 8$ precisa-se da seguinte definição: Se t representa o número de níveis que pertencem $\{1, 2, 3, \ldots, \tau\}$ contendo variáveis, pelo Corolário 3.1 define-se

$$t_1 = \gamma - \left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor - 1$$

como a maior t-configuração para a qual o corolário não é aplicável. De maneira geral define-se para $1 \leq h \leq \gamma - \left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor$,

$$t_h = \gamma - \left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor - h \tag{4.3}$$

e

$$m(h) = \gamma^* - t_h - 1 \tag{4.4}$$

Observe que se é mostrado a existência de soluções não singulares para as formas que no nível 0 possuem $m(h)$ variáveis para cada um dos h no intervalo já mencionado, segue do Corolário 3.1 a existência de soluções não singulares para as formas com $m_0 = \gamma^* - r$ com $t_1 \leq r \leq \tau$, isto é, para as formas com $m_0 \geq \gamma^* - \gamma + 1$, e com isto, obtém-se a desigualdade (4.2).

O esquema da prova para o caso $\tau \geq 8$ divide-se em três partes: A primeira, consiste em fazer um análise sobre as t_h-configurações com exatamente h blocos, o qual permite estabelecer uma condição necessária para obter um zero não trivial em ditas configurações e, além disso, esta condição serve como base para introduzir condições necessárias para os outros tipos de t_h-configurações; Cabe aclarar, que este análise é feito para os casos quando $m_1 \geq 1$, pois para o caso $m_1 = 0$, dito análise não é necessário como será visto na prova do Teorema 1. A segunda parte, consiste em uma serie de propriedades que relacionam as (t_h, n)-configurações para diferentes h e n com as (t_1, t_2)-configurações e as condições necessárias para obter um zero não trivial sempre que $m_1 \geq 1$, mas neste sentido existe certo paralelo em ditas propriedades quando $m_1 = 0$ e as provas são em sua maioria semelhantes. Finalmente, a terceira parte consiste no uso das propriedades obtidas para executar a prova do teorema, e é tratado de maneira especial os casos para $\tau = 8, 9$. Começa-se definindo o seguinte:

Seja C uma configuração, onde $m_1 \geq 1$ e defina

$$S_C = \gamma(\gamma^* - \gamma) + 1 - m_0 + \left\lfloor \frac{m_0 - 2}{3} \right\rfloor. \tag{4.5}$$

Por outra parte, denota-se Σ_C como o número de variáveis distributivas nos níveis que conformam a configuração C. Após contrações de variáveis do nível 0 ao nível 1, tem-se

$$\Sigma_C = S_C + X, \tag{4.6}$$

onde X é uma variável que depende do número de variáveis nos níveis i, com $i \geq \gamma$. Agora, para um h fixo, considere $m(1) \leq m_0 \leq m(h)$ e defina

$$S_C(h) = (\gamma^* - \gamma)\gamma + 1 - m(h) + \left\lfloor \frac{m(h) - 2}{3} \right\rfloor. \tag{4.7}$$

Com isto, é claro que

$$S_C \geq S_C(h),$$

e portanto $\Sigma_C \geq S_C(h) + X$. De maneira semelhante, define-se por Σ_C' quando $m_1 = 0$, e para este caso, não é considerado a possível existência de variáveis nos níveis maiores que τ, tendo assim

$$\Sigma_C' = \gamma(\gamma^* - \gamma) + 1 - m_0. \tag{4.8}$$

Por uniformidade na notação vai-se notar $\Sigma_C' = S_C'$ e de maneira análoga ao caso $m_1 \geq 1$, para $m(1) \leq m_0 \leq m(h)$ define-se

$$S_C'(h) = (\gamma^* - \gamma)\gamma + 1 - m(h). \tag{4.9}$$

tendo assim $S_C^{'} \geq S_C^{'}(h)$.

A seguinte é uma limitante para h quando $m_1 = 0$, a qual faz parte importante na demonstração do resultado principal.

Lema 4.1. *Seja $\mathscr{F}$ uma forma aditiva 3-normalizada de grau $k = 3^\tau$ em s variáveis, com $s \geq k(\gamma^* - \gamma) + 1$. Então, $m_1 \geq 0$ sempre que*

$$\gamma^* - 2\gamma + t_1 + 3 \leq h. \tag{4.10}$$

Demonstração. Dado que $\mathscr{F}$ é uma forma 3-normalizada em $s \geq k(\gamma^* - \gamma) + 1$ variáveis, e $m(1) \leq m_0 \leq m(h)$, tome o maior número de variáveis que pode assumir o nível 0, ou seja, $m(h)$. Segue da 3-normalização, que o nível 1 possui uma limitante inferior, pois

$$m(h) + m_1 \geq 2(\gamma^* - \gamma) + 1.$$

Daí, se $m_1 \geq 1$, não há nada a fazer. Logo, $m_1 = 0$ sempre que

$$m(h) - (2(\gamma^* - \gamma) + 1) \geq 0,$$

isto é, que o nível 0 possua tantas variáveis de tal maneira que a condição de 3-normalização, $m(h) + m_1 \geq 2(\gamma^* - \gamma) + 1$, seja mantida quando $m_1 = 0$. Assim, usando a definição de $m(h)$ (*ver* (4.4)) e substituindo $t_h = t_1 - h + 1$, tem-se

$$\begin{aligned} 2(\gamma^* - \gamma) + 1 - m(h) &= 2(\gamma^* - \gamma) + 1 - (\gamma^* - t_h - 1) \\ &= \gamma^* - 2\gamma + t_1 + 3 - h \\ &\leq 0. \end{aligned}$$

Assim, isolando h, obtém-se a desigualdade (4.10) como queria ser mostrado. □

4.2.1 Considerações Iniciais.

Na prova para $\tau \leq 7$, são usados recorrentemente dois conceitos: A 3-normalização e o Lema 3.6. O primeiro passo, é escolher um nível l e, junto com a 3-normalização, determinar o número de variáveis entre o nível l e o nível τ, além de considerar a possível existência de variáveis nos níveis maiores que τ. Logo, o que segue é analisar a forma em que distribuíam-se dito número de variáveis, as quais podem estar entre os níveis l e $l+\tau$ ou, os níveis l e τ para assim aplicar o Lema 3.6 desde o nível l. Esta ideia é usada seguindo as condições particulares de cada subcaso. No que segue, retoma-se esta ideia e, a forma de analisar a distribuição das variáveis esta orientada a satisfazer as condições do Corolário 3.4 e em consequência o Corolário 3.5, com a diferencia que o método é estabelecido apenas para o nível 0 e a possível existência ou não de variáveis nos níveis 1 e 2, com tudo, a aplicação final do Lema 3.6 acontece desde o nível 0. Levando isto em consideração, começa-se avaliando o que acontece quando os níveis $\tau+1, \tau+2$ e $\tau+3$ possuem variáveis e, para isso é precisa a seguinte proposição.

Proposição 4.1. *Seja $h \geq 1$, então para todo $M \geq 1$ as seguintes são satisfeitas desigualdades*

$$\Psi(t_h - 1, t_{2h}, M) - \Psi(t_h - 1, t_{2h}, M-1) < \gamma^* - \gamma \tag{4.11}$$

e

$$\Psi(t_h - 1, t_{2h} - 1, M) - \Psi(t_h - 1, t_{2h} - 1, M-1) < \gamma^* - \gamma. \tag{4.12}$$

Demonstração. Dado que $\tau \geq 8$, tem-se que

$$1 \leq 2\gamma\left(2\log_2(3) - 3\right) < 4\gamma^* - 6\gamma,$$

com isto, dado que por hipótese $h \geq 1$, a desigualdade $-h+2 < 4\gamma^* - 6\gamma$ é mantida. Por outra parte, da definição de t_h (*ver* (4.3)), tem-se $2t_1 \leq 3\gamma - \gamma^*$ assim,

$$2t_1 - h + 2 < 3\gamma - \gamma^* - h + 2 < 3\gamma^* - 3\gamma.$$

Agora, da Proposição 3.3, tem-se

$$\Psi(t, n, M) - \Psi(t, n, M-1) \leq t - \frac{n}{3} + 1,$$

daí, substituindo $t = t_h - 1$ e $n = t_{2h}$, obtém-se

$$\Psi(t_h - 1, t_{2h}, M) - \Psi(t_h - 1, t_{2h}, M-1) \leq \frac{2t_1 - h + 2}{3}, \tag{4.13}$$

o qual completa a prova para (4.11). De maneira similar mostra-se a desigualdade (4.12). $\square$

Agora, para uma (t,n)-configuração foi definido $\Psi(t,n,M)$ em (3.26) e, embora o valor de M pode ser qualquer inteiro positivo, ajustado ao problema, dito valor depende da (t,n)-configuração e da existência de variáveis nos níveis posteriores a τ, isto é, para uma (t,n)-configuração minimal C o valor de M é $\gamma^* - t_h$ como em (3.26), mas se por exemplo $m_\gamma \geq 1$, então $M = \gamma^* - t_h - 1$ em virtude do Lema 3.6 e o conjunto não singular. Daí, estabelecer as condições para a existência de um zero não trivial precisa um análise mais detalhado.

Seja C uma (t,n)-configuração, pelos Corolários 3.3 e 3.4 quando $m_1 \geq 1$, o objetivo é encontrar desigualdades da forma

$$\Sigma_C = S_C + X > \Psi(t,n,M), \tag{4.14}$$

onde, X e M são inteiros positivos que depende da existência de variáveis nos níveis maiores a τ. Assim, tem-se que a desigualdade (4.14) é valida se, e somente se,

$$S_C > \Psi(t,n,M) - X. \tag{4.15}$$

Assim, sempre que seja satisfeita a desigualdade (4.15), então a forma $\mathscr{F}$ admite um zero não trivial. De aqui em diante, adota-se a desigualdade (4.15), por efeitos de notação e simplicidade operacional.

Considere agora os níveis $\tau+1 = \gamma$, $\tau+2 = \gamma+1$ e $\tau+3 = \gamma+2$, divide-se o análise em dois grandes casos: O primeiro quando $m_2 = 0$, e o segundo caso quando $m_2 \geq 1$. No que segue, alguns dos argumentos são obtidos de maneira análoga a casos anteriores, assim, explana-se apenas aqueles que precisam de algumas considerações especificas. Por outra parte, para um $h \geq 1$ dado, se tem interesse nas t_h-configurações com exatamente h blocos, pois estas carecem da aplicabilidade de um argumento que usa blocos limitados que serão usado na prova do Teorema 1 quando $\tau \geq 8$. Por isto, assuma-se C como uma (t_h, t_{2h})-configuração (não necessariamente minimal).

Para $m_2 \geq 1$: Dado que o nível 2 possui variáveis, a quantidade de blocos segue sendo a mesma que os da configuração C, assim, considere $C' = C - \{1\}$ uma $(t_h - 1, t_{2h} - 1)$-configuração. Daí, contraindo as variáveis do nível 0 ao nível 2, tem-se

$$\begin{aligned} S_{C'}(h) &= \gamma\left(\gamma^* - \gamma\right) + 1 - m(h) - m_1 + \left\lfloor \frac{m(h)-1}{3} \right\rfloor + \left\lfloor \frac{m_1 - 2}{3} \right\rfloor \\ &= S_C(h) - \gamma^* + t_h + \left\lfloor \frac{\gamma^* - t_h - 2}{3} \right\rfloor. \end{aligned} \tag{4.16}$$

Sejam $\chi = \gamma^* - \gamma$, $M = \gamma^* - t_h$, e para efeitos de simplificar a notação e manter a relação com a configuração C', toma-se o par $(t_h, t_{2h}) = C'$, na função Ψ, ou seja

$$\Psi(t_h, t_{2h}, M) = \Psi\left(C', M\right).$$

Dado que $2 \in C'$, então apenas são considerando os níveis m_γ e $m_{\gamma+1}$, com o qual obtém-se as seguintes desigualdades, as quais são necessárias para obter uma zero não trivial.

I). Se $m_\gamma = m_{\gamma+1} = 0$, da 3-normalização existem pelo menos $S_{C'}(h) + 2\chi$ variáveis na configuração C' daí, deve ser satisfeito

$$S_{C'}(h) \geq \Psi(C', M) - 2\chi = \beta_1. \tag{4.17}$$

II). Se $m_\gamma = 0$ e $m_{\gamma+1} \geq 1$, segue que do Lema 3.6 que se $m_2 \geq M$, obtém-se um zero não trivial, isto é, C' é um conjunto não singular, portanto $m_2 \leq M - 1$. Com isto, para obter um zero não trivial é necessário que

$$S_{C'}(h) > \Psi(C', M-1) - \chi = \beta_2. \tag{4.18}$$

III). Se $1 \leq m_\gamma \leq 4$ e $m_{\gamma+1} \geq 0$, tem-se da 3-normalização que na C' existem pelo menos $S_{C'}(h) + (\chi - 4) + \chi$ variáveis, obtendo

$$S_{C'}(h) > \Psi(C', M-1) - 2\chi + 4 = \beta_3. \tag{4.19}$$

caso contrario se m_γ é um 5-bloco, usando o Lema 3.5 contraem-se variáveis do nível γ ao nível $\gamma + 1$ o que resulta no caso IV).

IV). Se $m_\gamma \cdot m_{\gamma+1} \neq 0$, tem-se que deve ser satisfeito

$$S_{C'}(h) > \Psi(C', M-2) = \beta_4. \tag{4.20}$$

Com isto, pela Proposição 4.1, tem-se

$$\begin{aligned}
\beta_4 &= \Psi(C', M-2) \\
&= \Psi(C', M-1) - (\Psi(C', M-1) - \Psi(C', M-2)) \\
&\geq \Psi(C', M-1) - \chi \\
&= \beta_2.
\end{aligned} \tag{4.21}$$

De maneira semelhante, e usando o fato de $\chi > 4$, pois $\tau \geq 8$, tem-se as desigualdades: $\beta_4 \geq \beta_2 \geq \beta_1$ e $\beta_2 \geq \beta_3$. Daí, para obter um zero não trivial neste caso é preciso que seja satisfeita a desigualdade (4.20).

Por outra parte, se $m_2 = 0$, tem-se uma $(t_h - 1, t_{2h})$-configuração $C'' = C - \{1, 2\}$, dado que o nível dois não possui variáveis, somente é possível contrair as variáveis do nível 0 ao nível 1 portanto, tem-se

$$S_{C''}(h) = S_C(h) - \gamma^* + t_h. \tag{4.22}$$

Aqui novamente para a função Ψ, toma-se o par $(t_h - 1, t_{2h}) = C''$ para facilitar a notação. Agora, dado que $1, 2 \notin C''$, consideram-se os níveis m_γ, $m_{\gamma+1}$, $m_{\gamma+2}$,

V). Se $m_\gamma = m_{\gamma+1} = m_{\gamma+2} = 0$, de maneira semelhante ao caso I) tem-se que deve ser satisfeito

$$S_{C''}(h) > \Psi(C'') - 3\chi = \beta_5. \tag{4.23}$$

VI). Se $m_\gamma = m_{\gamma+1} = 0$ e $m_{\gamma+2} \geq 1$, tem-se

$$S_{C''}(h) > \Psi(C'', M-1) - 2\chi = \beta_6. \tag{4.24}$$

VII). Se $m_\gamma = m_{\gamma+2} = 0$ e $4 \geq m_{\gamma+1} \geq 1$, de um razoamento semelhante ao caso III) deduz-se

$$S_{C''}(h) > \Psi(C'', M-1) - 3\chi + 4 = \beta_7. \tag{4.25}$$

caso contrario, se $m_{\gamma+1} \geq 5$ segue de VIII).

VIII). Se $m_\gamma = 0$ e $m_{\gamma+1} \cdot m_{\gamma+2} \neq 0$, obtém-se

$$S_{C''}(h) > \Psi(C'', M-2) - \chi = \beta_8. \tag{4.26}$$

IX). Se $16 \geq m_\gamma \geq 5$ e $m_{\gamma+1} = m_{\gamma+2} = 0$, dado que o nível γ pode contrair variáveis ao nível $\gamma + 1$ segue do Lema 3.6 que

$$S_{C''}(h) > \Psi(C'', M-2) - 3\chi + 16 = \beta_9. \tag{4.27}$$

Agora, se $m_\gamma \leq 4$, de maneira semelhante ao caso III)

$$S_{C''}(h) > \Psi(C'', M-1) - 3\chi + 4 = \beta_{10} \tag{4.28}$$

Finalmente se $m_\gamma \geq 17$ tem-se o caso XII).

X). Se $m_\gamma \cdot m_{\gamma+2} \neq 0$, $m_{\gamma+1} = 0$ e $m_\gamma \geq 5$ tem-se o caso XII). Agora, se $m_\gamma \leq 4$.

$$S_{C''}(h) > \Psi(C'', M-2) - 2\chi + 4 = \beta_{11}. \tag{4.29}$$

XI). Se $m_\gamma \cdot m_{\gamma^*+1} \neq 0$ e $m_{\gamma+2} = 0$, obtém-se pelo Lema 3.5 contraindo variáveis dos níveis γ e $\gamma + 1$ uma nova variável no nível $\gamma + 2$ quando $m_\gamma + m_{\gamma+1} \geq 15$ ou, $m_{\gamma+1} \geq 5$ o que segue do caso XII). Caso contrario,

$$S_{C''}(h) > \Psi(C'', M-2) - 3\chi + 14 = \beta_{12}. \tag{4.30}$$

XII). Se $m_\gamma \cdot m_{\gamma+1} \cdot m_{\gamma+1} \neq 0$, segue

$$S_{C''}(h) > \Psi(C'', M-3) = \beta_{13}. \tag{4.31}$$

De forma semelhante ao caso quando $m_2 \geq 1$ tem-se as desigualdades :

$$\beta_{13} \geq \beta_8 \geq \beta_6 \geq \beta_5$$

e $\beta_6 \geq \beta_7$. Por outra parte, tem-se que a desigualdade

$$50 - h < \gamma(10 \log_2(3) - 12) < 10\chi - 2\gamma$$

é satisfeita para todo $\tau \geq 12$ daí, tem-se

$$2t_1 - h + 2 \leq 3\gamma - \gamma^* - h + 2 < 3(3\chi - 16),$$

logo, por (4.13) tem-se que

$$\beta_9 \leq \beta_{13}, \tag{4.32}$$

ainda mais, com uma comprovação direta, tem-se que esta desigualdade é satisfeita para todo $\tau \geq 10$. De forma análoga, mostra-se

$$\beta_{13} \geq \beta_{10},$$

$$\beta_{13} \geq \beta_{11}$$

e $\beta_{13} \geq \beta_{12}$. Com o qual, conclui-se para este caso que para obter um zero não trivial é necessário satisfazer a desigualdade (4.31).

Agora de (4.16) e (4.22), tem-se as desigualdades

$$S_C(h) > \beta_4 + \gamma^* - t_h - \left\lfloor \frac{\gamma^* - t_h - 2}{3} \right\rfloor \tag{4.33}$$

e

$$S_C(h) > \beta_{13} + \gamma^* - t_h, \tag{4.34}$$

por outra parte,

$$\beta_4 - \beta_{13} = t_h - 2 + \left\lfloor \frac{\gamma^* - t_h - 2}{3} \right\rfloor,$$

dado que para $\tau \geq 10$ e $1 \leq h \leq t_2$, tem-se $t_h \geq 2$, segue das desigualdades (4.33) e (4.34)

$$\begin{aligned} S_C(h) &> \beta_4 + \gamma^* - t_h - \left\lfloor \frac{\gamma^* - t_h - 2}{3} \right\rfloor \\ &= \beta_{13} + \gamma^* - 2 \\ &\geq \beta_{13} + \gamma^* - t_h. \end{aligned}$$

Assim, sempre que $m_1 \geq 1$ e $\tau \geq 10$, serão considerados os níveis γ e $\gamma + 1$, tais que $m_\gamma m_{\gamma+1} \neq 0$ e com isto, a condição necessária para obter um zero não trivial é

$$\begin{aligned} S_C(h) &> \beta_4 + \gamma^* - t_h - \left\lfloor \frac{\gamma^* - t_h - 2}{3} \right\rfloor \\ &= \Psi(t_h, t_{2h}, M - 3) + 2. \end{aligned} \tag{4.35}$$

A igualdade em (4.35), obtém-se ao substituir β_4 usando a Proposição 3.3 (b).

4.2.2 Relacionando (t, n)-configurações diferentes.

Observe que (4.35) é uma condição necessária somente para todas as configurações com h blocos de uma t_h-configuração, assim, estabelecem-se as seguintes propriedades com a finalidade de estender esta condição as outras t_h-configurações. Para isto defina-se

$$\upsilon_l(h) = \gamma^* - t_h - \left\lfloor \frac{\gamma^* - t_h}{3} \right\rfloor - l. \tag{4.36}$$

Observe que $\upsilon_l(h) \leq \upsilon_l(h+r)$ para $0 \leq r$, pois da definição de t_h (*ver* (4.3)), tem-se

$$\begin{aligned} \upsilon_l(h) &\leq \gamma^* - t_h + r - \left\lfloor \frac{\gamma^* - t_h + r}{3} \right\rfloor - l \\ &= \gamma^* - t_{h+r} - \left\lfloor \frac{\gamma^* - t_{h+r}}{3} \right\rfloor - l \\ &= \upsilon_l(h+r). \end{aligned} \tag{4.37}$$

Proposição 4.2. *Sejam h, n inteiros positivos fixos e $\varepsilon \geq 0$. Se $M = \gamma^* - t_h - 3$ e*

$$S_C(h) > \Psi(t_h, n, M),$$

então para $0 \leq \varepsilon \leq n$, tem-se que

$$S_C(h) > \Psi(t_h, n - \varepsilon, M) - \varepsilon \upsilon_4(h).$$

Demonstração. Se $\varepsilon = 0$ a prova é imediata. Agora para um n fixo assuma, $n = t_h - s$ e ε de tal forma que satisfaz $0 \leq s + \varepsilon \leq t_h$. Assim, observe que a proposição é verdadeira se

$$\Psi(t_h, t_h - s - \varepsilon, M) - \Psi(t_h, t_h - s, M) < \varepsilon \upsilon_4(h). \tag{4.38}$$

Para mostrar isto e relembrando que $\gamma^* = \lfloor \gamma \log_2(3) \rfloor + 1$, onde $\gamma = \tau + 1$, assuma primeiramente que $47 \leq \gamma$, logo, tem-se que $8 < 2\gamma^* - 3\gamma$ e, portanto a seguinte desigualdade é satisfeita

$$8 - s - 2h \leq \gamma\,(2\log_2(3) - 3) < 2\gamma^* - 3\gamma. \tag{4.39}$$

Usando o fato $2t_1 \leq 3\gamma - \gamma^*$ (*ver*(4.3)), tem-se da parte direita de (4.39) que

$$2\gamma^* - 3\gamma \leq \gamma^* - 2t_1,$$

logo, usando o fato $t_h = t_1 - h + 1$ e da parcela direita de (4.39) conclui-se

$$\gamma^* - s - 6 < 2\left(\gamma^* - t_h\right) - 12.$$

Dividindo a ambos lados da desigualdade anterior e usando a função piso tem-se

$$\left\lfloor \frac{\gamma^* - s}{3} - 2 \right\rfloor < \gamma^* - t_h - \left\lfloor \frac{\gamma^* - t_h}{3} \right\rfloor - 4 = \upsilon_4(h). \tag{4.40}$$

Agora, da Proposição 3.3(c) quando $M = \gamma^* - t_h - 3$ e por (4.40), tem-se

$$\begin{aligned}\Psi(t_h, t_h - s - \varepsilon, M) - \Psi(t_h, t_h - s, M) &< \varepsilon \left\lfloor \frac{\gamma^* - s}{3} - 2 \right\rfloor \\ &< \varepsilon \upsilon_4(\omega).\end{aligned}$$

Finalmente, de (4.39) obtém-se que se $2h + s \geq 8$ mantém-se a proposição para todo $\tau \geq 8$. Assim, por (4.40) pode-se assumir $\varepsilon = 1$ e verifica-se computacionalmente (4.38) para $2h + s \leq 8$ e $9 \leq \gamma \leq 47$, obtendo que (4.38) é valida para todo $\tau \geq 8$, como se queria mostrar. □

De maneira análoga à anterior Proposição, tem-se para $m_1 = 0$ a seguinte propriedade.

Proposição 4.3. *Sejam h, n inteiros positivos fixos e $\varepsilon \geq 0$. Para $m_1 = 0$, se $M = \gamma^* - t_h$ e*

$$S_C^{'}(h) > \Psi(t_h, n, M),$$

então para $0 \leq \varepsilon \leq n$, tem-se

$$S_C^{'}(h) > \Psi(t_h, n - \varepsilon, M) - \varepsilon \upsilon_4(h).$$

Demonstração. Seja $n = t_h - s$ e observe que é suficiente mostrara a desigualdade (4.38). Para isto, tem-se que a desigualdade

$$5 - s < 3\gamma^* - 4\gamma, \tag{4.41}$$

é satisfeita para todo $\tau \geq 8$. Logo, a desigualdade (4.41) acontece se, e somente se,

$$11 - 2(\gamma^* - 2\gamma + t_1 + 3) - s < \gamma^* - 2t_1.$$

Agora, dado que $m_1 = 0$, tem-se pelo Lema 4.1 que $\gamma^* - 2\gamma + t_1 + 3 \leq h$, assim,

$$11 - 2h - s \leq 11 - 2(\gamma^* - 2\gamma + t_1 + 3) - s < \gamma^* - 2t_1,$$

com o qual obtém-se

$$\gamma^* - s - 3 < 2(\gamma^* - t_h) - 12 \leq 3\upsilon_4(h).$$

Daí, pela Proposição (3.3)(c) e usando o fato $M = \gamma^* - t_h$, segue que

$$\Psi(t_h, t_h - s - \varepsilon, M) - \Psi(t_h, t_h - s, M) < \varepsilon \left\lfloor \frac{\gamma^* - s}{3} - 1 \right\rfloor < \varepsilon\upsilon_4(\omega),$$

como queria ser mostrado. □

Lema 4.2. *Se para inteiros positivos h, n, ε e M, tem-se $S_C(h) > \Psi(t_h, n, M)$ e*

$$\Psi(t_h, n, M) - \Psi(t_h - \omega, n - \omega - \varepsilon, M + \omega) \geq \omega, \tag{4.42}$$

para $0 \leq \omega + \varepsilon \leq n$, então

$$S_C(h + \omega) > \Psi(t_h - \omega, n - \omega - \varepsilon, M + \omega).$$

Por outra parte, se $S'_C(h) > \Psi(t_h, n, M)$ e é satisfeita (4.42), então

$$S'_C(h + \omega) > \Psi(t_h - \omega, n - \omega - \varepsilon, M + \omega).$$

Demonstração. Se $\omega = 0$ é imediato, então seja $\omega > 0$. Por (4.42)

$$\begin{aligned}
\Psi(t_h - \omega, n - \omega - \varepsilon, M + \omega) &= \Psi(t_h, n) - (\Psi(t_h, n, M) - \Psi(t_h - \omega, n - \omega - \varepsilon, M + \omega)) \\
&\leq \Psi(t_h, n) - \omega \\
&< S_C(h) - \omega \\
&= S_C(h + \omega).
\end{aligned}$$

Finalmente, a prova para S'_C é análoga ao caso anterior. □

Como já foi visto na seção 4.2.1, tem-se especial interesse nas configurações com exatamente h blocos, ou seja, nas (t_h, t_{2h})-configurações. Observe que para um h fixo, da Proposição 3.1, tem-se que as $(t_h - w, t_{2h} - 2w)$-configurações tem exatamente $h + w$ blocos, sempre que $0 \leq 2w \leq t_h$, e isto permite estabelecer algumas propriedades entre as configurações já mencionadas. Por todo o anterior, fazendo $n = t_{2h}$ e $\omega = \varepsilon$ em (4.42) mostra-se a seguinte Proposição, a qual permite desconsiderar esta hipótese do Lema 4.2 sempre que para algum h dado a (t, n)-configuração tenha exatamente h blocos.

Proposição 4.4. *Para $\tau \geq 8$, se $M = \gamma^* - t_h - 3$ e h, ω são inteiros positivos tais que $0 \leq 2\omega \leq t_{2h}$, então*

$$\Psi(t_h, t_{2h}, M) - \Psi(t_h - \omega, t_{2h} - 2\omega, M + \omega) \geq \omega. \tag{4.43}$$

Por outra parte, a desigualdade (4.43) também é satisfeita quando $M = \gamma^* - t_h$.

Demonstração. Se $\omega = 0$ é imediato. Dado que $\gamma^* - 2t_1 \geq 3\,(1 - h)$ para todo $\tau \geq 8$, pois $h \geq 1$, segue que

$$\gamma^* - 2t_h + h + 2 \geq 3. \tag{4.44}$$

Agora, considere os pares

$$C = (t_h, t_{2h}), \quad C' = (t_h - \omega, t_{2h} - 2\omega) \;\text{ e }\; C'' = (t_h - \omega, t_{2h} - \omega). \tag{4.45}$$

para $\omega \geq 1$. Fazendo $n = t_{2h} - w$, em (b) e (c) da Proposição 3.3, e dado que $M = \gamma^* - t_h - 3$ por hipótese, tem-se

$$\begin{aligned}
\Psi(C, M) - \Psi(C', M + \omega) &= \Psi(C, M) - \Psi(C'', M + \omega) \\
&\quad - (\Psi(C', M + \omega) - \Psi(C'', M + \omega)) \\
&= \sum_{i=0}^{\omega - 1} M + i - \left(\left\lfloor \frac{M + i - 2}{3} \right\rfloor + \left\lfloor \frac{M + n + i - 2}{3} \right\rfloor \right) \\
&\geq \sum_{i=0}^{\omega - 1} \frac{M - n - 2i + 4}{3} \\
&= \frac{\omega}{3} (M - n - \omega + 5) \\
&= \frac{\omega}{3} \left(\gamma^* - 2t_h + h + 2 \right).
\end{aligned}$$

Daí, pela desigualdade (4.44), obtém-se o desejado. Agora, para $M = \gamma^* - t_h$, tem-se para todo $t \geq 8$ que $\gamma^* - 2t_1 \geq -3h$, disto obtém-se

$$\gamma^* - 2t_h + h + 5 \geq 3,$$

assim,

$$\begin{aligned} \Psi(C, M) - \Psi(C', M+\omega) &\geq \frac{\omega}{3}(M - n - \omega + 5) \\ &= \frac{\omega}{3}(\gamma^* - 2t_h + h + 5) \\ &\geq \omega. \end{aligned} \tag{4.46}$$

Como se queria mostrar. □

No decorrido desta seção, quase todas as proposições usaram como hipótese um condicional da forma

$$S_C(h) > \Psi(t_h, n, M),$$

para construir as propriedades. O mesmo foi feito para o caso $S_C^{'}$, tendo a sutileza de mudar o valor de M. As seguintes proposições, vistam de mostra a veracidade destes condicionais para o caso particular das t_h-configurações com exatamente h blocos. Começa-se com o caso para $S_C(h)$ (*ver*(4.7)), como segue:

Proposição 4.5. *Sejam* $\tau \geq 8$, $0 \leq t_{2h}$ *e* $M = \gamma^* - t_h - 3$, *então*

$$S_C(h) > \Psi(t_h, t_{2h}, M) + 2. \tag{4.47}$$

Demonstração. Pelo Lema 4.2 e a Proposição 4.4 para $M = \gamma^* - t_1 - 3$, basta mostrar que

$$S_C(1) > \Psi(t_1, t_2, M) + 2. \tag{4.48}$$

Primeiro, da definição da função Ψ (*ver*(3.26)) e dado que $t_2 = t_1 - 1$, tem-se

$$\begin{aligned} \Psi(t_1, t_2, M) + 2 &= M + t_2 + 2\sum_{i=0}^{t_2-1} M + i - \left\lfloor \frac{M+i-2}{3} \right\rfloor \\ &\leq \frac{1}{3}\left(\sum_{i=0}^{t_2-1} 2(M+i) + 5\right) + M + t_2 + 2 \\ &= t_2\left(\frac{2\gamma^* - t_1}{3}\right) + \gamma^* - t_1 - 1. \end{aligned}$$

Por outra parte, tem-se $3\gamma - \gamma^* - 2 \leq 2t_1 \leq 3\gamma - \gamma^*$ (*ver*(4.3)), portanto,

$$\begin{aligned} t_1^2 + 4t_1 &\geq t_1^2 + 2\left(3\gamma - \gamma^* - 2\right) \\ &= \left(\gamma - \left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor - 1\right)^2 + 2\left(3\gamma - \gamma^* - 2\right) \\ &\geq \left(\frac{3\gamma}{2} - \gamma^* - 1\right)^2 + 2\left(3\gamma - \gamma^* - 2\right) \\ &= \left(\gamma^*\right)^2 - 3\gamma^*\gamma + \frac{9\gamma^2}{4} + 3\gamma - 3. \end{aligned} \tag{4.49}$$

Assim,

$$\begin{aligned} S_C(1) - \Psi(t_1, t_2, M) - 2 &= \left(\gamma^* - \gamma\right)\gamma - 2\gamma^* + 2t_1 + \left\lfloor \frac{\gamma^* - t_1}{3} \right\rfloor - \frac{t_2}{3}\left(2\gamma^* - t_1\right) \\ &\geq \left(\gamma^* - \gamma\right)\gamma - 2\gamma^* + 2t_1 + \frac{\gamma^* - t_1}{3} - \frac{(t_1 - 1)}{3}\left(2\gamma^* - t_1\right) + 1 \\ &= \gamma^*\left(\gamma - \frac{2t_1}{3} - 1\right) + \frac{t_1}{3}\left(t_1 + 4\right) - \gamma^2 + 1 \\ &\geq \gamma^*\left(\gamma^* - 1\right) + \frac{t_1}{3}\left(t_1 + 4\right) - \gamma^2 + 1 \\ &= \gamma^*\left(\frac{4\gamma^*}{3} - \gamma - 1\right) - \frac{\gamma^2}{4} + \gamma. \end{aligned}$$

Dado que $\gamma^* = \lfloor \gamma \log_2(3) \rfloor + 1$, seque que $\gamma \log_2(3) < \gamma^* < \gamma \log_2(3) + 1$, usando este fato na desigualdade acima, obtém-se

$$\begin{aligned} S_C(1) - \Psi(t_1, t_2, M) - 2 &> \frac{4}{3}\gamma^2 \log_2(3)^2 - \gamma \log_2(3) - \gamma^2 \log_2(3) - \frac{\gamma^2}{4} - 1 \\ &= \gamma^2\left(\frac{4}{3}\log_2(3)^2 - \log_2(3) - \frac{1}{4}\right) - \gamma \log_2(3) - 1 \\ &> 0. \end{aligned}$$

A última desigualdade é mantida, dado que a função

$$f(x) = x^2\left(16\log_2(3)^2 - 12\log_2(3) - 3\right) - 12\left(x\log_2(3) - 1\right),$$

é crescente para $x \geq 0$ e positiva para $2 \leq x$. Com isto se conclui que a desigualdade (4.48) é valida para todo $\tau \geq 8$, como queria ser mostrado. $\square$

Agora, lembre que $S_C^{'}(h)$ esta definida para o caso $m_1 = 0$, (*ver* (4.9)) logo para mostrar a desigualdade $S_C^{'}(h) > \Psi\left(t_h, t_{2h}, M\right)$ com $M = \gamma^* - \gamma$, e em virtude do

Lema 4.2, é preciso mostrar que $t_{2h} \geq 0$ para o menor h que satisfaz $m_1 = 0$, o qual é obtido do Lema 4.1. Portanto, para τ um inteiro, defina

$$T_1 = \gamma^* - 2\gamma + t_1 + 3. \tag{4.50}$$

Lema 4.3. *Seja T_1 como em (4.50), então $t_{2T_1} \geq 0$ se, e somente se, $\gamma \geq 54$.*

Demonstração. Seja $T_1 = \gamma^* - 2\gamma + t_1 + 3$, onde $\gamma^* = \lfloor \gamma \log_2(3) \rfloor + 1$, segue de (4.3) que

$$\begin{aligned}
t_{2T_1} &= 4\gamma - 2\gamma^* - t_1 - 5 \\
&\geq 4\gamma - 2\gamma^* - \frac{1}{2}(3\gamma - \gamma^*) - 5 \\
&\geq \frac{\gamma}{2}(5 - 3\log_2(3)) - \frac{13}{2} \\
&\geq 0,
\end{aligned}$$

o qual é satisfeito se, e somente se, $\gamma \geq 54$.

□

Proposição 4.6. *Para $h \geq T_1$, sejam $\gamma \geq 53$, $0 \leq t_{2h}$, e $M = \gamma^* - t_h$, então*

$$S_C^{'}(h) > \Psi(t_h, t_{2h}, M). \tag{4.51}$$

Demonstração. De maneira semelhante a prova da Proposição (4.5), pelo Lema 4.2 e a Proposição 4.4 basta mostrar que

$$S_C^{'}(T_1) > \Psi(t_{T_1}, t_{2T_1}, M), \tag{4.52}$$

com $T_1 = \gamma^* - 2\gamma + t_1 + 3$ (*ver*(4.50)). Assim,

$$\begin{aligned}
\Psi(t_{T_1}, t_{2T_1}, M) &= \sum_{i=h}^{t_h - 1} M + i - \left\lfloor \frac{M + i - h - 2}{3} \right\rfloor + \sum_{i=0}^{h-1} M + i \\
&\leq \sum_{i=h}^{t_{T_1} - 1} M + i + 1 - \left(\frac{M + i - h - 2}{3} \right) + \sum_{i=0}^{h-1} M + i \\
&= \frac{t_{2T_1}}{3}(2M + t_1 + h + 5) + \frac{h}{2}(2M + h - 1) \\
&= \frac{\gamma^*}{6}(16\gamma - 35 - 5\gamma^*) - \frac{t_1}{6}(t_1 - 4\gamma + 17) + 11(\gamma - 1) - 2\gamma^2.
\end{aligned}$$

Por outra parte, dado que $3\gamma - \gamma^* - 2 \leq 2t_1 \leq 3\gamma - \gamma^*$, tem-se

$$\Psi(t_{T_1}, t_{2T_1}, M) \leq \frac{\gamma^*}{24}(62\gamma - 110 - 21\gamma^*) + \frac{\gamma}{24}(174 - 33\gamma) - \frac{25}{3}.$$

Agora, observe que de (4.4) e de (4.50), tem-se que $m(T_1) = 2(\gamma^* - \gamma) + 1$, portanto segue de (4.9) que

$$S_C'(T_1) = (\gamma^* - \gamma)\gamma + 1 - m(T_1) = (\gamma - 2)(\gamma^* - \gamma).$$

Assim, tem-se que

$$\begin{aligned} S_C'(T_1) - \Psi(t_{T_1}, t_{2h}, M) &\geq (\gamma - 2)(\gamma^* - \gamma) + \frac{\gamma^*}{24}(21\gamma^* + 110 - 62\gamma) \\ &\quad + \frac{\gamma}{24}(33\gamma - 174) + \frac{25}{3} \\ &= \frac{\gamma^*}{24}(21\gamma^* + 62 - 38\gamma) + \frac{\gamma}{24}(\gamma - 126) + \frac{25}{3} \\ &\geq \frac{\gamma\log_2(3)}{24}(21\gamma\log_2(3) + 62 - 38\gamma) + \frac{\gamma}{24}(\gamma - 126) + \frac{25}{3} \\ &> 0. \end{aligned}$$

A última desigualdade é valida pois, a função

$$f(x) = x\log_2(3)(21x\log_2(3) + 62 - 38x) + x(x - 126) + 200,$$

é uma função positiva para todo $x \in \mathbb{R}$. $\square$

Para uma forma $\mathscr{F}$ aditiva 3-normalizada de grau $k = 3^\tau$ em s variáveis, com $s \geq k(\gamma^* - \gamma) + 1$ e $m_0 = \gamma^* - r$ o Lema 2.7 determina uma limitante a r (*ver* (2.10)) para o qual a forma com este número de variáveis no nível 0 possui zeros não triviais. Em este capítulo, tem-se tomado $m_0(h) = \gamma^* - t_h - 1$, (*ver* (4.4)) assim reescrevendo a limitante (2.10) em termos de h, obtém-se

$$t_1 - \frac{\gamma(\gamma^* - \gamma) - 1}{\gamma^* - 3} + 2 \leq h. \tag{4.53}$$

Com isto, define-se o menor valor que pode assumir h em esta limitante, como sendo

$$T_2 = t_1 - \frac{\gamma(\gamma^* - \gamma) - 1}{\gamma^* - 3} + 2. \tag{4.54}$$

Assim, pelo Lema 2.7, tem-se que se $\mathscr{F}$ é uma forma aditiva como foi descrita acima, com $m_0\,(h) = \gamma^* - t_h - 1$, e $h \geq T_2$, então a forma aditiva possui uma solução não singular. Dado que γ^* e γ são valores que dependem de τ, segue que para um τ fixo, se definem as constantes T_1 e T_2, como em (4.50) e (4.54) respetivamente. A seguinte Proposição, estabelece a relação de ordem entre estas duas constantes.

Proposição 4.7. *Para todo $\tau \geq 65$, sejam T_1 e T_2 constantes como em (4.50) e (4.54) respetivamente. Então, $T_1 < T_2$.*

Demonstração. Comprova-se diretamente que o resultado é mantido para $65 \leq \tau \leq 80$. Assim, assumindo que $\tau > 80$, tem-se que a seguinte desigualdade é satisfeita

$$\gamma^2 \left(\log_2(3) - \log_2(3)^2\right) - 6\gamma + \gamma^2 + 3 > 0.$$

Agora,

$$\begin{aligned} T_2 - T_1 &= t_1 - \frac{\gamma\,(\gamma^* - \gamma) - 1}{\gamma^* - 3} + 2 - (\gamma^* - 2\gamma + t_1 + 3) \\ &\geq \frac{\gamma\gamma^* - (\gamma^*)^2 + 2\gamma^* - 6\gamma + \gamma^2 + 4}{\gamma^* - 3} \\ &> \frac{\gamma^2\,(\log_2(3) - \log_2(3)^2) - 6\gamma + \gamma^2 + 3}{\gamma^* - 3} \\ &> 0. \end{aligned}$$

□

4.2.3 Prova do Teorema 1 para $\tau \geq 8$.

Seja $\mathscr{F}$ uma forma aditiva 3-normalizada de grau $k = 3^\tau$ em s variáveis, com $s \geq k\,(\gamma^* - \gamma) + 1$. Considere

$$m\,(1) \leq m_0 \leq m\,(h)\,,$$

para $1 \leq h \leq \gamma - \lfloor (\gamma^* - \gamma)\,/2 \rfloor$, onde $m\,(h) = \gamma^* - t_h - 1$ (*ver* (4.4)) e

$$t_h = \gamma - \left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor - h$$

(*ver* (4.3)).Alem disso, por (4.50), tem-se que T_1 é menor valor de h tal que, se $1 \geq h < T_1$, então $m_1 \geq 1$, e se $h \leq T_1$, tem-se $m_1 \geq 0$.

Seja $1 \leq h < T_1$ o qual implica que $m_1 \geq 1$. Tem-se da Proposição 4.1 e da desigualdade (4.35) que para $\tau \geq 10$ pode assumir-se $m_\gamma m_{\gamma+1} \neq 0$ e $M = \gamma^* - t_h - 3$. Assim, considere inicialmente a C como sendo uma (t_h, t_{2h})-configuração, segue da Proposição 4.5, que para $1 \leq h < T_1$ tem-se (4.47), ou seja,

$$S_C(h) > \Psi(t_h, t_{2h}, M) + 2,$$

o qual, pelo Corolário 3.4, implica que $\mathscr{F}$ possui zeros 3-ádicos não triviais. Daí, seja C uma $(t_h, t_{2h} + \varepsilon)$-configuração, com $\varepsilon \geq 0$. Do que tem-se

$$S_C(h) > \Psi(t_h, t_{2h} + \varepsilon, M) + 2$$

pois, $\Psi(t, n, M)$ é estritamente decrescente em função de n, logo, tem-se do Corolário 3.4 que a forma possui um zero não trivial.

Agora, suponha a configuração $C = (t_h, t_{2h} - \varepsilon)$, com $0 \leq t_{2h} - \varepsilon$, esta configuração possui $h + \varepsilon$ blocos e se, pelo menos $h + 1$ destes blocos são 5-blocos, o resultado segue do Lema 3.6 pois, assumindo $m_0 = \gamma^* - t_1 - 1$, tem-se t_h níveis distribuídos em $h + 1$ blocos, os quais, admitem contração pelo Lema 3.5 ao seguinte nível vazio e, dado que o último bloco pode terminar no nível τ, tem-se pelo menos h novos níveis entre os níveis 1 ate τ obtendo

$$t_h + h = t_1 - 1$$

níveis. Portanto, sejam ε blocos 4-limitados logo,

$$\sum_{j=1}^{\varepsilon} b_{i_j} \geq \varepsilon v_4(h),$$

com b_{i_j} em (3.27) daí, tem-se

$$\begin{aligned} S_C(h) &> \Psi(t_h, t_{2h} - \varepsilon, M) + 2 - \varepsilon v_4(h) \\ &\geq \Psi(t_h, t_{2h} - \varepsilon, M) + 2 - \sum_{i=1}^{\varepsilon} b_{i_j}, \end{aligned}$$

e pelo Corolário 3.5, obtém-se um zero não trivial.

Por outra parte, seja T_2 como em (4.54), segue do Lema 2.7 que a forma $\mathscr{F}$ com $m_0 = \gamma^* - t_h - 1$, possui um zero não trivial sempre que $h \geq T_2$. Logo, pela Proposição 4.7, tem-se $T_2 \leq T_1$ para $\tau < 65$. Daí, para $10 \leq \tau < 65$ e $1 \leq h \leq t_1$, obtém-se um zero não trivial quando o nível 0 tem $\gamma^* - t_h - 1$ variáveis, com $1 \leq h \leq \gamma - \lfloor (\gamma^* - \gamma)/2 \rfloor$.

Agora, considere $\tau \geq 65$ e $m(1) \leq m_0 \leq m(h)$. Para $1 \leq h < T_1$ o resultado segue do caso $m_1 \geq 1$, e se $h \geq T_2$ existem zeros 3-ádicos não triviais pelo Lema 2.7. Portanto, considere $T_1 \leq h \leq T_2$ e $m_1 = 0$. Relembrando que em este ponto não serão considerada a existência de variáveis nos níveis maiores que τ, e que para uma t-configuração C, toma-se $\Sigma_C^{'} = S_C^{'}$ (*ver* (4.8)).

Do Lema 4.3 se deduz que para $\tau \geq 53$ existe pelo menos um $h \geq T_1$ tal que $t_{2h} \geq 0$. Assim, seja h' o maior inteiro para o qual $t_{2h'} \geq 0$. Logo, pela Proposição 4.6 tem-se a desigualdade

$$S_C^{'}(h) > \Psi(t_h, t_{2h}, M).$$

para todo $T_1 \leq h \leq h'$ com $M = \gamma^* - t_h$. Agora, seja C uma $(t_h, t_{2h} + \varepsilon)$-configuração, para $T_1 \leq h \leq h'$ e $\varepsilon \geq 0$. Tem-se de (a) da Proposição 3.3, que a função $\Psi(t, n, M)$ é decrescente em n, assim segue do Corolário 3.4 que a forma aditiva $\mathscr{F}$ possui um zero 3-ádico não trivial.

Por sua vez, se C é uma $(t_h, t_{2h} - \varepsilon)$-configuração, com $\varepsilon \geq 1$, por um argumento análogo ao caso para $\tau < 65$ para os blocos 4-limitados, tem-se

$$S_C'(h) > \Psi(t_h, t_{2h} - \varepsilon, M) - \varepsilon v_4(h),$$

para $T_1 \leq h \leq h'$ e portanto, pelo Corolário 3.5 um zero não trivial. Logo, se $h' \geq T_2$, o resultado segue do Lema 2.7, caso contrario, pelo Lema 4.2, tem-se para $M = \gamma^* - t_{h'}$ e $0 \leq n < t_{h'}$,

$$S_C'(h' + \omega) > \Psi(t_{h'} - \omega, n - \omega, M + \omega),$$

com $0 \leq w \leq T_2 - t_{h'}$ e $0 \leq n - \omega$. O qual implica um zero não trivial pelo Corolário 3.4. E novamente, pelo Lema 2.7 é claro que o resultado mantém-se para os $T_2 \leq h \leq t_1$, quando $m_0 = \gamma^* - t_h - 1$. Com tudo, para $\tau \geq 65$, fica mostrado a existência de um zero não trivial quando o nível 0 possui $\gamma^* - t_h - 1$ variáveis com $1 \leq h \leq t_1$.

Com todo o anterior, foi mostrado que para $\tau \geq 10$, a forma $\mathscr{F}$ possui um zero 3-ádico não trivial quando $m_0 = \gamma^* - t_h - 1$ e $1 \leq h \leq \gamma - \lfloor (\gamma^* - \gamma)/2 \rfloor$, o qual é equivalente a mostrar que a forma $\mathscr{F}$ possui zeros 3-ádicos não triviais quando $m_0 = \gamma^* - \gamma + r$ e

$$\left\lfloor \frac{\gamma^* - \gamma}{2} \right\rfloor - 1 < r \leq \gamma - 1.$$

Logo, pelo Corolário 3.1, a forma $\mathscr{F}$ possui zeros não triviais quando

$$1 \leq r \leq \left\lfloor \frac{\gamma^* - \gamma^*}{2} \right\rfloor - 1.$$

Portanto, para $\tau \geq 10$ é satisfeita a desigualdade

$$\Gamma^* (3^\tau, 3) \leq 3^\tau (\gamma^* - \gamma) + 1.$$

Agora, quando $8 \leq \tau \leq 9$, tem-se que $m(1) = 9$ (*ver* (4.4)). Por outra parte, pelo Lema 2.7, tem-se que a forma $\mathscr{F}$ possui um zero 3-ádico quando $m_0 \geq 12$, assim, assuma $m(1) \leq m_0 \leq (h)$ para $1 \leq h \leq 3$, ou seja

$$9 \leq m_0 \leq 12.$$

Isto implica, que $m_1 \geq 1$, pois

$$m_1 \geq 2(\gamma^* - \gamma) + 1 - m_0 = 13 - m_0 \geq 1.$$

Agora, para $h = 1$, tem-se $m_0 = 9$. Dado que contraindo variáveis do nível 0, podem ser obtidas duas novas variáveis no nível 1, tem-se que $m_1 \leq \gamma^* - 3$, daí se $10 \leq m_1 \leq \gamma^* - 3$, segue que

$$\sum_{i=2}^{\tau+1} \geq (\gamma + 1)(\gamma^* - \gamma^* + 1) + 1 - m_0 - m_1 \geq \gamma (\gamma^* - \gamma^* + 1) - 5 - \gamma^* = \beta.$$

Então, se este número de variáveis é distribuído em $\gamma^* - 12$ variáveis, segue do Lema 3.6 que $\mathscr{F}$ tem um zero 3-ádico não trivial, pois contraindo variáveis do nível 0 ao nível 1, tem-se $m_1 \geq 12$. Assim, assuma que pelo menos β variáveis são distribuídas em não mais que $\gamma^* - 13$ níveis, isto implica que cada nível, tem pelo menos $\gamma^* - 1$ variáveis, e o resultado segue do Lema 3.6 aplicado ao menor nível maior o igual que 2, com variáveis. Do anterior, tem-se que $1 \leq m_1 \leq 9$, daí $m_2 \geq 1$ e, portanto esta no caso $m_2 \geq 1$ do análise da seção 4.2.1. Logo, assuma $m_\gamma \cdot m_{\gamma+1} \neq 0$, assim para C uma t_1-configuração, tem-se que a desigualdade (4.35)

$$S_C(1) > \Psi(t_1, t_2, \gamma^* - t_1 - 3) + 2. \tag{4.55}$$

Logo, o resultado segue de maneira semelhante ao caso $\tau \geq 10$ quando é considerada C uma $(t_1, t_2 - \varepsilon)$-configuração, com $0 \leq \varepsilon \leq t_2$.

Agora, se $2 \leq h \leq 3$, tem-se que $m_2 \geq 0$. Se $m_2 \geq 1$, se esta no caso anterior, y dado que a desigualdade (4.55) é satisfeita para $h = 1$, pela Proposição 4.5, a desigualdade

$$S_C(h) > \Psi(t_h, t_{2h}, \gamma^* - t_h - 3) + 2,$$

é satisfeita par $2 \leq h \leq 3$ e o resultado segue semelhante ao caso $\tau \geq 10$. Assim, seja $m_2 = 0$ e C'' uma $(t_h - 1, t_{2h})$-configuração. Da Proposição 4.1, pode-se assumir $m_\gamma \geq 1$ e da desigualdade (4.22), obtém-se a desigualdade

$$S_C(h) > \Psi(t_h - 1, t_{2h}, \gamma^* - t_h - 1) + \gamma^* - t_h,$$

a qual, rescreve-se por (b) da Proposição 3.3 como

$$S_C(h) > \Psi(t_h, t_{2h}, \gamma^* - t_h - 2) + \left\lfloor \frac{\gamma^* - t_h - 1}{3} \right\rfloor - \left\lfloor \frac{\gamma^* - h - 1}{3} \right\rfloor.$$

Esta desigualdade verifica-se diretamente para $\tau = 8, 9$ e $h = 2, 3$. Daí, tomando C como uma $(t_h, t_{2h} - \varepsilon)$-configuração, com ε um inteiro, e fazendo um raciocínio semelhante ao caso $\tau \geq 10$, obtém-se que $\mathscr{F}$ representa um zero 3-adíco não trivial. Logo, pelo Corolário 3.1, tem-se que $\mathscr{F}$ representa um zero 3-ádico não trivial, quando $7 \leq m_0 \leq 8$. Assim, para todo $8 \leq \tau \leq 9$, tem-se

$$\Gamma^*(3^\tau, 3) \leq 3^\tau(\gamma^* - \gamma) + 1.$$

Finalmente, com os resultados da seção 4.1 e com o mostrado anteriormente, tem-se que se $\tau \geq 1$ e $k = 3^{\tau}$ a desigualdade (4.1) é satisfeita, isto é,

$$\Gamma^{*}\left(k,3\right) \leq k\left(\gamma^{*}-\gamma\right)+1.$$

Como queria ser mostrado. $\square$

Capítulo

5

$\Gamma^*(81)$ e outros valores

Apresenta-se aqui alguns resultados que na procura de encontrar valores exatos para $\Gamma^*(3^\tau)$. Quando $\tau = 1$, Lewis em [19] mostra que $\Gamma^*(3) = 7$. Por sua vez, Norton [21] mostra que $\Gamma^*(9) = 37$ e Knapp [16] mostra $\Gamma^*(27) = 109$. É precisamente sobre a método de que estabeleceu Knapp em [16] e com ajuda do Teorema 1 que são obtidos os resultados deste Capítulo. Começando com um resultado direto do Lema 2.4.

Corolário 5.1. *Seja $k \geq 3$ ímpar, se $p = 2k + 1$ é primo, então*

$$\Gamma^*(k, p) = k\lfloor \log_2(p) \rfloor + 1.$$

Demonstração. Por hipótese, tem-se que $2k + 1 = p$ é um primo que não divide k, portanto $\gamma = 1$. Dado que k é ímpar, tem-se que ± 1 são as únicas k-ésimas potencias modulo p. Assim que a congruência

$$\mathscr{G}(\mathbf{x}) = x_1^k + 2x_2^k + \cdots + 2^{t-1}x_t^k \equiv 0 \pmod{p} \tag{5.1}$$

com $t = \lfloor \log_2(p) \rfloor$, não possui soluções primitivas. Segue que a forma aditiva

$$\mathscr{G}(\mathbf{x_1}) + p\mathscr{G}(\mathbf{x_2}) + \cdots + p^{k-1}\mathscr{G}(\mathbf{x_k})$$

com $k\lfloor \log_2(p) \rfloor$ variáveis não representa zeros p-ádicos, onde $\mathbf{x_1}, \ldots, \mathbf{x_k}$ representam conjuntos disjuntos de variáveis da forma $\mathbf{x_i} = (x_{i,1}, \ldots, x_{i,t})$. Isto implica que uma forma aditiva de grau k no corpo $\mathbb{Q}_p$ precisa pelo menos $k\lfloor \log_2(p)\rfloor + 1$ variáveis, para ter um zero não trivial, portanto

$$\Gamma^*(k,p) \geq k\lfloor \log_2(p)\rfloor + 1.$$

Por outra parte, seja $\mathscr{F}$ uma forma aditiva p-normalizada de grau k em s variáveis, com $s \geq k\lfloor \log_2(p)\rfloor + 1$. Dado que $p \nmid k$, tem-se por (2.2) que

$$\gamma^* = \lfloor \log_2(p)\rfloor + 1.$$

Dado que $m_0 \geq \gamma^*$, pela p-normalização (*ver* Lema 1.8) e que k é ímpar, portanto -1 é uma potencia k-ésima modulo p, segue do Lema 2.4 que $\mathscr{F}$ possui um zero p-ádico não trivial, e portanto

$$\Gamma^*(k,p) \leq k\lfloor \log_2(p)\rfloor + 1.$$

Portanto,

$$\Gamma^*(k,p) = k\lfloor \log_2(p)\rfloor + 1.$$

□

5.1 Valor exato de $\Gamma^*(81)$

Considere $\mathscr{F}$ uma forma aditiva de grau k e a congruência

$$\mathscr{F}_0 = a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv 0 \pmod{p^\gamma}. \tag{5.2}$$

Dado que $k = 81$, tem-se que $2k + 1 = 163$ é primo, logo pelo Corolário 5.1 a congruência (5.2) não possui soluções com $t = 7$ variáveis, e

$$\Gamma^*(81, 163) = 568.$$

Assim, assuma-se que uma forma aditiva de grau 81, tem pelo menos 8 variáveis no nível 0, além disso, considere $p \neq 3$. Dado que k é ímpar, então -1 é uma k-ésima potencia modulo p^γ, com o qual do Lema 2.5, tem-se que a congruência (5.2) possui soluções não singulares quando $256 = 2^8 > p^\gamma$. Por outra parte fazendo $n = 8$ na congruência (5.2) e usando o Lema 1.5 a congruência possui solução para $p > 27576$.

Agora, para os primos p tais que $d = (81, p-1) = 1, 3$, tem-se pelo Teorema de Warning 1.10, que a congruência (5.2) possui solução não trivial. Por outro lado, para primos p tal que $d = 9, 27$, e $p \geq 256$, tem-se do Lema 1.6

$$Q\,(81, p, 8) < 1,$$

(*ver* A.1) particularmente,

d	p	$Q\,(81, p, 8)$
9	307	0.00453421
27	271	0.772044

Isto implica, que para todo primo $p \neq 3$ tal que $(k, p-1) \in \{1, 3, 9, 27\}$ tem-se

$$\Gamma^*\,(81, p) \leq 568.$$

Fazendo uso novamente do Lema 1.6 para os primos p satisfazendo $p \equiv 1 \pmod{81}$

p	$Q\,(81, p, 8)$
811	3.45271
1297	1.16385
1621	0.462156

Assim, para $p = 811$ e $p = 1297$ na tabela abaixo exibe-se um contraexemplo de uma forma que só possui zeros triviais módulo p, estes resultados encontram-se computacionalmente (*ver*A.2).

p	$\mathscr{F}_0$
811	$x_1^{81} + 2x_2^{81} + 4x_3^{81} + 9x_4^{81}$
1297	$x_1^{81} + 2x_2^{81} + 4x_3^{81}$

Por outro lado, é achado computacionalmente (*ver Apêndice* A.2) que para o primo 811 uma forma com 5 variáveis no nível 0 possui solução não trivial, portanto $\Gamma^*\,(81, 811) = 325$. Da mesma forma, para $p = 1297$ quatro variáveis no nível 0 são suficientes para obter uma solução não trivial, portanto, $\Gamma^*\,(81, 1297) = 244$.

Finalmente, pelo Teorema 1 tem-se que

$$\Gamma^*\,(81, 3) \leq 244,$$

com o qual, tem-se que

$$\Gamma^* (81) = 568.$$

5.2 Limitantes para 243 e 729

Assuma $k = 3^\tau$ com $\tau = 5, 6$. Tem-se que $2k + 1$ é um número primo, logo pelo Corolário 5.1 tem-se os valores na seguinte tabela.

τ	$\Gamma^* (k, 2k + 1)$
5	1945
6	7291

Com isto, assuma que a forma aditiva de grau k possui pelo menos 9 variáveis no nível 0 quando $\tau = 5$, e 11 variáveis quando $\tau = 6$. Por outra parte, pelo Teorema 1, tem-se que $\Gamma^* (243, 3) \leq 973$ e $\Gamma^* (729, 3) \leq 3646$, assim, assuma $p \neq 3$. Do Lema 2.5 e do Lema 1.5, tem-se solução para os primos:

τ	n	$2^n > p^\gamma$	$p > (k-1)^{(2n-2)/(n-2)}$
5	9	512	281010
6	11	2048	2292409

Fazendo uso do Lema 1.6 para $k = 243$ e $p = 811$, tem-se $Q(243, 811, 9) \approx 2.38078$, e $Q(243, 1297, 9) < 1$, mas para $a_1 \cdots a_n \not\equiv 0 \pmod{811}$

$$a_1 x_1^{243} + \cdots + a_n x_n^{243} \equiv a_1 x_1^{81} + \cdots + a_n x_n^{81} \pmod{811}$$

e já tinha-se visto que esta congruência tem solução com 5 variáveis, isto implica, $\Gamma^* (243, 811) = 973$. Outros valores da função $Q(k, p, n)$ quando $p \equiv 1 \pmod{d}$ com $d \neq k$ exibem-se na seguinte tabela.

τ	n	d	$p \equiv 1 \pmod{d}$	$Q(3^\tau, p, n)$
5	9	9	523	0.000426427
		27	541	0.210533
6	11	27	2053	$4.75226 \cdot 10^{-6}$
		81	2269	0.0119812
		243	3889	0.728689

Com isto, ficam os primos $p \equiv 1 \pmod{k}$.

τ	n	$p \equiv 1 \pmod{k}$	$Q(k,p,n)$
5	9	3889	1.97422
		4861	1.02627
		5347	0.974315
6	11	2917	159.722
		32077	0.0412035
		36451	0.0270805

Infelizmente, encontrar soluções computacionalmente para esta parte não tem sido possível, mas foram encontrados os seguintes contraexemplos: Estes contraexemplos

τ	p	$\mathscr{F}_0$
5	3889	$x_1^k + 2x_2^k + 4x_3^k + 8x_4^k$
	4861	$x_1^k + 2x_2^k + 4x_3^k + 10x_4^k$
6	2917	$x_1^k + 2x_2^k + 4x_3^k + 8x_4^k + 16x_5^k$

permitem dar uma limitante inferior para $\Gamma^*(k,p)$, como segue:

$$973 \leq \Gamma^*(243, p) \quad \text{para} \quad p = 3889, 4861$$

e

$$3646 \leq \Gamma^*(729, 2917).$$

Finalmente, do Teorema 3.25 de Norton [21], tem-se as limitantes $1945 \leq \Gamma^*(243)$ e $7291 \leq \Gamma^*(729)$, mas conjetura-se aqui que as igualdades são satisfeitas.

Referências

[1] Ronald Gale Bierstedt, *Some problems on the distribution of kth power residues modulo a priime*, ProQuest LLC, Ann Arbor, MI, 1963, Thesis (Ph.D.)–University of Colorado at Boulder. MR 2616571

[2] Z. I. Borevich and Igor R. Shafarevich, *Number theory*, Pure and Applied Mathematics, Academic Press, New York, NY, 1966.

[3] J. D. Bovey, $\Gamma^*(8)$, Acta Arith. **25** (1973/74), 145–150. MR 347713

[4] Christopher Broll, Michael P. Knapp, Jessica A. Kuiper, Paulo H. A. Rodrigues, and Daiane Veras, *More exact values of the function* $\Gamma^*(k)$, J. Number Theory **233** (2022), 481–497. MR 4356862

[5] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1935), no. 1, 73–75. MR 3069644

[6] S. Chowla, *On a conjecture of Artin. I, II*, Norske Vid. Selsk. Forh. (Trondheim) **36** (1963), 135–141. MR 160759

[7] S. Chowla and G. Shimura, *On the representation of zero by a linear combination of the k-th powers*, Norske Vid. Selsk. Forh. (Trondheim) **36** (1963), 169–176. MR 160760

[8] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. London Ser. A **274** (1963), 443–460. MR 153655

[9] M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163–210. MR 213296

[10] Hemar Godinho and Michael P. Knapp, *Infinitely many counterexamples to a conjecture of Norton*, Michigan Math. J. **69** (2020), no. 3, 533–543. MR 4132602

[11] Hemar Godinho, Michael P. Knapp, Paulo H. A. Rodrigues, and Daiane Veras, *On the values of $\Gamma^*(k,p)$ and $\Gamma^*(k)$*, Acta Arith. **191** (2019), no. 1, 67–80. MR 3998981

[12] Robert M. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, 2 ed., Addison-Wesley, 1994.

[13] James Francis Gray, *Diagonal forms of prime degree*, ProQuest LLC, Ann Arbor, MI, 1959, Thesis (Ph.D.)–University of Notre Dame. MR 2939062

[14] Helmut Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 113–130. MR 1581027

[15] Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982, Translated from the Chinese by Peter Shiu. MR 665428

[16] Michael P. Knapp, *Exact values of the function* $\Gamma^*(k)$, J. Number Theory **131** (2011), no. 10, 1901–1911. MR 2811557

[17] ______, *2-adic zeros of diagonal forms*, J. Number Theory **193** (2018), 37–47. MR 3846799

[18] D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields*, Ann. of Math. (2) **56** (1952), 473–478. MR 49947

[19] ______, *Cubic congruences*, Michigan Math. J. **4** (1957), 85–95. MR 84013

[20] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, New York, NY, USA, 1986.

[21] K. K. Norton, *On homogeneous diagonal congruences of odd degee*, ProQuest LLC, Ann Arbor, MI, 1966, Thesis (Ph.D.)–University of Illinois at Urbana-Champaign. MR 2616020

[22] Guy Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A612. MR 197450

[23] Aimo Tietäväinen, *On a problem of Chowla and Shimura*, J. Number Theory **3** (1971), 247–252. MR 285484

[24] D. Veras, *Formas aditivas sobre corpos p-ádicos*, Universidade de Brasilia, 2017, Thesis (Ph.D.). MR 2616020

[25] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Dover Publications, Inc., Mineola, NY, 2004. MR 2104806

Apêndice

Apêndice

A

Comandos

Neste apêndice se encontram os comandos que são necessários para as comprovações computacionais, geradas nos desenvolvimento da dissertação. Para os cálculos que seguem, é usado o software *Mathematica 11,* em dois computadores: *Asus TUF FX504GM* com Intel (R) Core (TM) i7-8750H, 32GB de memoria RAM a 2667 Mhz. Também foi usado um *Lenovo Ideapad 320-15IKB* com Intel (R) Core (TM) i5-7200U, memoria RAM 8GB a 2133Mhz. Toda a documentação e descrição das funções de *Mathematica 11,* podem ser encontradas em no site

`https://www.wolfram.com/language/`

A.1 Função $Q(k, p, n)$ e primos excepcionais para 81, 273 e 729.

Define-se os comandos que compõem a função $Q(k, p, n)$.

- A função exponencial $\exp(2\pi i x/p) = e_p(x)$

```
Ex[p_,x_]:= Exp[2*Pi*I*x/p];
```

- Somas Gaussianas

```
S[k_,p_,b_]:= Sum[Ex[p, b*x^k], {x, 0, p - 1}];
```

- Função $Q(k, p, n)$ (1.14)

```
Q[k_,p_,n_]:= Sum[Abs[S[k, p, b]]^n,{b, 1, p-1}]/(p^n - p);
```

As seguintes, são as entradas e a descrição das variáveis usadas, com a finalidade de encontrar os primos p tais que $Q(k,p,n) > 1$ para cada uma das potencias $k = 3^\tau$, com $\tau = 4, 5, 6$ e os n dados correspondentes em cada caso. Essas linhas de código serão posteriormente aninhadas para mostrar os resultados desejados em cada caso.

- A variável `K` lista as potencias de 3 a serem analisadas

  ```
  K = Table[3^j, {j,4,6}];
  ```

- A variável `k` é uma potencia 3 particular, lida da lista `K` por `k=K[[f]];`. Onde `f` representa a f-ésima posição na lista `K`.

- Dado que $2 \cdot 3^\tau + 1$ é primo, fixa-se n com a variável

  ```
  n=Floor[Log[2, 2 k + 1]]+1;
  ```

- O comando `H=Divisors[k];` salva uma lista dos divisores de `k`. Por outra parte, a variável `DiH = Dimensions[H][[1]]` salva o número de divisores de `k`.

- O conjunto de divisores é dividido em duas partes, em virtude do Lema 1.11 como segue:

  ```
  Dm={};
  Do[ If[H[[i]] < n, Dm = Union[Dm, {H[[i]]}]], {i, 1,  DiH}];
  DM = Complement[H, Dm];
  ```

  A variável `Dm` lista os divisores primos de `k` menores que o número de variáveis `n`. Por sua vez, `Dm` lista os divisores primos de `k`, que são maiores o iguais que o número de variáveis `n`.

- A seguinte lista de comandos lista em `P` os primeiros 10 primos p, tais que $d = (k, p-1)$, onde d é um divisor primo maior que o número de variáveis n. Foi observado que a rotina até achar o primeiro primo p tal que $Q(k,p,n) < 1$ não precisava destes 10 primos. Este valor pode ser alterado segundo as demandas de próximos trabalhos. Além disso, a variável `i` começa em 4, dado que para `i=2` já tem-se solução pelo Corolário 5.1, por outra parte, pelo Lema 2.5 os primos que fazem parte `P`, devem ser maiores que 2^n.

```
P = {};
c = 0;
i = 4;
While[c <= 10,
  If[Mod[i, 3]== 0, ,
   If[And[PrimeQ[i*DM[[e]] + 1], i*DM[[e]] + 1 > 2^n],
    And[P = Union[P, {i*DM[[e]] + 1}], c++]
    ]
   ];
  i++];
```

- Gera-se uma tabela contendo os valores para $Q(k,p,n)$, para os diferentes primos, e o programa para quando $Q(k,p,n) < 1$.

```
CAn = {};
Do[
  r = Q[k, P[[h]], n];
  If[r > 1,
   CAn = Union[CAn, {{P[[h]], N[r]}}],
   CAn = Union[CAn, {{P[[h]], N[r]}}]; Break[]],
  {h, 1, Dimensions[P][[1]]}];
```

Finalmente, mostra-se aqui uma serie de comandos integrando algumas outras justificativas para gerar um informe, como segue.

```
Do[
 k = K[[f]];
 n = Floor[Log[2, 2 k + 1]] + 1;
 Pk = PrimeQ[2 k + 1];
 H = Divisors[k];
 DiH = Dimensions[H][[1]];
 Dm = {};
 Do[ If[H[[i]] < n, Dm = Union[Dm, {H[[i]]}]], {i, 1, DiH}];
 DM = Complement[H, Dm];
 Print[
  "--------------------------------------------
```

```
 ___________ CASO k=", k, " __________________
 ___________________________________________"];
Print[" Pelo Lema 1.5 tem-se solução para   p>",
 Ceiling[(k-1)^((2 n-2)/(n-2))], ", E pelo Lema 1.11 p^g<",
 2^n, ". Agora, p que pertencem a ", Dm,
 " e pelo Lema 1.13, a congruência possui Solução, pois Dp<", n];
Do[ Print[" *****Caso para (k,p-1)=", DM[[e]], "*****"];
 P = {};
 c = 0;
 i = 4;
 While[c <= 10,
  If[Mod[i, 3] == 0, ,
   If[And[PrimeQ[i*DM[[e]] + 1], i*DM[[e]] + 1 > 2^n],
    And[P = Union[P, {i*DM[[e]] + 1}], c++]]];
  i++];
 Print["
  ____________________________________________________________
  ________ Possiveis conjuntos a analizar por Q(k,p,t)________
  ____________________________________________________________
  "];
 CAn = {};
 Do[
 r = Q[k, P[[h]], n];
  If[r > 1, CAn = Union[CAn, {{P[[h]], N[r]}}],
   CAn = Union[CAn, {{P[[h]], N[r]}}]; Break[]],
 {h, 1,Dimensions[P][[1]]}];
 Print[TableForm[CAn,TableHeadings -> {None, {"p","Q(k,p,n)"}}]],
 {e, 1, Dimensions[DM][[1]]}];
Print["
 ===================== Fin do Cálculo ========================
 "],
 {f, 1, Dimensions[K][[1]]}]
```

A.2 Comandos para congruências

Em esta secção é primeiro estabelecido um argumento teórico que diminui o número de congruências da forma (1.5) que devem ser avaliadas para obter uma solução não trivial. Esta estratégia foi estabelecida por Knapp em [16] como segue: Seja $\mathbb{K}$ o subgrupo multiplicativo das k-ésimas potencias módulo p. Observe que se $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times$ é o grupo multiplicativo de $(\mathbb{Z}/p^\gamma\mathbb{Z})$, então

$$\mathbb{L} = (\mathbb{Z}/p^\gamma\mathbb{Z})^\times /\mathbb{K}$$

é um grupo multiplicativo cíclico. Além disso, dado que

$$|\mathbb{K}| = \frac{\psi(p^\gamma)}{(k, \psi(p^\gamma))} = r,$$

onde $\psi(n)$ é a função totiente de Euler, tem-se que o cardinal de $\mathbb{L}$ esta dado por

$$|\mathbb{L}| = (k, \psi(p^\gamma)) = L.$$

Portanto, existe $\overline{g} \in \mathbb{L}$ de ordem L, tal que $\langle \overline{g} \rangle = \mathbb{L}$. Assim, seja $g \in \overline{g}$ um representante da classe, logo, o conjunto $\mathcal{L} = \{1, g, \ldots, g^L\}$ contem um representante de cada classe de $\mathbb{L}$. Desta forma, pode-se assumir que os coeficientes de (1.5) pertencem ao conjunto $\mathcal{L}$, ou qualquer conjunto de cardinalidade L onde cada elemento seja o único representante da sua classe. Ainda mais, dado que estes elementos fazem parte do grupo multiplicativo, pode-se assumir que $a_1 = 1$, e por sua vez, dado que k é ímpar, então -1 é uma potencia k-ésima da unidade, assim, se dois coeficientes são iguais, já tem-se uma solução, portanto pode-se assumir que $a_i = g^{c_i}$ com $2 \leq c_i \leq L - 1$ para $i = 2, \ldots, n$, onde $c_i \neq c_j$ para $i, j = 2, \ldots, n$.

Com o anterior, obtém-se dois fatos: Primeiro, se $n = 2$, então a congruência (1.5) só possui soluções triviais, pois, suponha que existem ζ_1, ζ_2 inteiros tais que $\zeta_1 \cdot \zeta_2 \not\equiv 0 \pmod{p^\gamma}$ e

$$a_1\zeta_1^k + a_2\zeta_2^k \equiv 0 \pmod{p^\gamma},$$

isto implica que

$$a_1 \equiv a_2 \left(-\zeta_1^{-k} \cdot \zeta_2^k\right) \pmod{p^\gamma},$$

logo, a_1 pertence a mesma classe a_2 em $\mathbb{L}$, dado que $\left(-\zeta_1^{-k} \cdot \zeta_2^k\right) \in \mathbb{K}$ o que contradisse a escolha dos coeficientes. O reciproco desta afirmação também é valido, isto é, para $n = 2$ a congruência (1.5) possui solução não trivial se, e somente se, a_1, a_2 pertencem a mesma classe em $\mathcal{L}$.

O segundo fato é: Observe que para um n e p fixos, o número de congruências módulo p^γ em n-variáveis é $\psi\left(p^\gamma\right)^n$. Mas ao fixar $a_1 = 1$ e dado que os coeficientes em $\mathcal{L}$ são de classes diferentes em $\mathbb{L}$, então o que resta é combinar estes $L - 1$ coeficientes nas $n - 1$ possibilidades, o qual implica uma economia computacional bastante grande, porem, não chega a ser suficiente em muitos casos.

Definem-se os comandos para esta parte como segue:

- As entradas são as variáveis `k`$= k$ e `p`$= p^\gamma$.
- Nas seguintes listas pode ser omitido o comando `Sort[]`, o qual ordena a lista. A variável `A` lista as k-ésimas potencias módulo p incluindo o zero, isto é, $\mathbb{K} \cup \{0\}$. Por sua vez, `A1` lista os elementos de $\mathbb{K}$

  ```
  A = Sort[DeleteDuplicates[Table[Mod[t^k, p], {t, 1, p}]]];
  A1 = Sort[DeleteDuplicates[Table[Mod[t^k, p], {t, 1, p - 1}]]];
  r = Dimensions[A][[1]];
  ```

- A variável `G` lista as classes de $\mathbb{L}$ e a variável `G1` é um conjunto de representantes de cada uma das classes, isto é, `G1` lista os elementos de $\mathcal{L}$. Assim, fazendo L$= L$, tem-se os seguintes comandos:

  ```
  G = DeleteDuplicates[Table[Sort[Mod[A1*t, p]], {t, 1, p - 1}]];
  L = Dimensions[G][[1]];
  G1 = Table[G[[y, 1]], {y, 1, L}];
  ```

- O número de congruências com n variáveis, a ser avaliadas esta dado por

  ```
  NCoe=Binomial[L - 1, n - 1]]
  ```

- A variável `Var` lista todas as n-uplas formadas por `A`.

  ```
  Var = Tuples[A, n];
  ```

- A lista Coe esta formada por todas as n-uplas de elementos de G1 que começam em 1.

```
Coe = Subsets[G1, {n}, NCoe];
```

A ideia da programação é a seguinte: Para n e j dados, avalia-se o j-ésimo elemento de Coe com cada as n-uplas de Var, assim, todos os possíveis resultados da equação

$$x_{1,j}^k + a_{2,j}x_{2,j}^k + \cdots + a_{n,j}x_{n,j}^k \pmod{p^\gamma} \tag{A.1}$$

estão dados pelo comando Var[[i]].Coe[[j]] fazendo variar $2 \leq i \leq NCoe$ pois, Var[[1]] é a n-úpla onde todas entradas são 0. Se para algum i a equação (A.1) é 0 módulo p^γ, então deve parar, e seguir com $j+1$. Caso contrario, se para nenhum i a equação (A.1) é 0 módulo p^γ, então Coe[[j]] representa um contraexemplo e n variáveis não são suficientes, com o qual deve seguir o analise para $n+1$. Agora, se n variáveis são suficientes o programa deve parar e não fazer $n+1$. O registo da solubilidade com n e j de (A.1) esta salvo na variável B. Com isto, para um suspeito número máximo w de variáveis que pode ter solução, os comandos são:

```
Do[
 NCoe = Binomial[L - 1, n - 1];
 Var = Tuples[A, n];
 Coe = Subsets[G1, {n}, NCoe];
 Do[
  B = 0;
  Do[
     If[Mod[Var[[i]].Coe[[j]], p] == 0, B = 1; Break[]],
   {i, 2, r^n}];
     If[B == 0, s = j; Break[]],
  {j, 1, NCoe}];
   If[B == 0,
    Print["Contraexemplo:", Coe[[s]]],
    Print["A forma com ", n, " variáveis no nível 0, possui solução"];
  Break[]],
  {n, 3, w}]
```

Observe que n começa em 3, pois como já foi dito as congruências com duas variáveis não possuem solução não trivial, a menos que os coeficientes estejam na mesma classe, o que não acontece nestes comandos.

Observe que se a congruência (5.2) possui solução não trivial com s variáveis, o número total de congruências a avaliar é

$$\sum_{n=3}^{s} \binom{L-1}{n-1}$$

congruências. Logo, o número de cálculos é exponencial, devido aos possíveis valores que podem tomar as variáveis. Isto implica que o máximo número de congruências comprovadas é

$$\sum_{n=3}^{s} \binom{L-1}{n-1} (r^n - 1). \tag{A.2}$$

Claramente, nem todas essas congruências são efetuadas, pois os comandos estão regulados para parar no momento que encontram um zero módulo p^γ. Por exemplo, para $k = 81$ e $p = 1297$ o número dado por (A.2) é 2252493377600 com o comando `RepeatedTiming[]` no computador Lenovo, obtém-se o tempo médio de calculo de cada calculo o qual é $2.1 \cdot 10^{-6} seg$, o que pelo número de operações seriam aproximadamente 53 dias, mas o tempo total de cálculo com o código é apenas um pouco mais de 6 horas.

A.3 Mínimo q do Teorema 0.2.

Seja `Gm`$=\gamma^*(k,p)$, então

```
Gm[t_, p_] := Floor[(t + 1) Log2[p] + 1];
```

Com o seguinte comando é gerada uma lista, salvada na variável `Table` contendo os valores de τ e o menor q que satisfaz o Teorema 0.2, como se mostra na Tabela 2.1.

```
 i = 2;
Tabla = {};
Do[
  q = Prime[i];
  While[
```

```
   t > ((t + 1) (Gm[t, q] - (t + 1)) - 1)/(Gm[t, q] - 3),
   q = Prime[i]; i++];
  Tabla = Union[Tabla, {{t, q}}],
  {t, 3, 30}];
TableForm[Tabla, TableHeadings -> {None, {"t", "q"}}]
```

A.4 Outros Valores para a função $Q(k,p,n)$.

Expressam-se aqui valores da função $Q(k,p,n)$. para alguns valores de p, nos intervalos dados pelo Lema 1.5 e o Lema 2.5.

A.4.1 $k = 81$.

Para os primos p tais que $9 = (k, p-1)$, tem-se que $(81, 307, 8) = 0.00453421$. Agora, para os primos p, tais que $27 = (k, p-1)$, são obtidos os seguintes valores.

p	$Q(81,p,8)$
271	0.772044
379	0.380389
433	0.163563
541	0.368057
757	0.0246605
919	0.0620837
1567	0.00550669
1999	0.001957

Finalmente, para os primos p tais que $81 = (k, p-1)$, são obtidos os seguintes valores.

p	$Q(81,p,8)$
811	3.45271
1297	1.16385
1621	0.462156
1783	0.316225
2269	0.152374
2593	0.259184
3079	0.317776
3727	0.023267

p	$Q(81,p,8)$
4051	0.0433099
5023	0.0224325
6481	0.00731708
6967	0.00846196
7129	0.00490783
8101	0.0111741
9397	0.00144453
9883	0.00457398

p	$Q(81,p,8)$
10369	0.00159183
10531	0.0010977
11503	0.0161591
11827	0.00102961
12799	0.000837164
13933	0.000681392
14419	0.000997074

A.4.2 $k = 243$

Para os primos p tais que $9 = (k, p-1)$, tem-se que $(243, 523, 9) = 0.000426427$. Agora, para os primos p, tais que $27 = (k, p-1)$, são obtidos os seguintes valores. Note que os valores da função $Q(243, p, 9)$ para este caso, são menores que os valores

p	$Q(243, p, 9)$
541	0.210533
757	0.00834026
919	0.0269584
1567	0.00149165

da função para o caso $k = 81$ e $n = 8$. De maneira semelhante, segue que os valores da função $Q(243, p, 9)$, para os primos p tais que $81 = (243, p-1)$, seguem como no caso $k = 81$ e $n = 8$. De fato, os valores de $Q(243, p, 9) < Q(81, p, 8)$ para estes primos.

Finalmente, para os primos p tais que $243 = (k, p-1)$, são obtidos os seguintes valores.

p	$Q(81, p, 8)$
3889	1.97422
4861	1.02627
5347	0.974315
8263	0.211445
9721	0.0841662
12637	0.035845
17011	0.00939339
19441	0.00542505
19927	0.0119749
20899	0.00470321