Busca de Permutações APN Criptográficas

Daniel Santana de Freitas

Relatório Técnico INE 004/2019

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística

Abstract

O importante papel das funções altamente não-lineares na construção de algoritmos criptográficos simétricos foi inicialmente apontado por Nyberg [11], logo após a divulgação do método de criptoanálise diferencial [18], no início dos anos 90. Desde então, as funções que possuem propriedades ótimas de resistência contra criptoanálise diferencial, ou seja, as funções "Perfeitamente Não-lineares" (PN) e "Quase Perfeitamente Não-lineares" (APN) têm sido objeto de estudo intensivo [8]. O trabalho de pesquisa descrito neste relatório foi realizado em duas partes, entre jan/2016 e fev/2018, e trata de um estudo de permutações APN com o auxílio dos conceitos de *ambiguidade* e *deficiência*, desenvolvidos pelo Prof. Daniel Panario e seu grupo de pesquisa na Universidade de Carleton, em Ottawa, Canadá. A primeira parte deste estudo foi executada durante um pós-doutorado do autor no Canadá (em 2016) e consistiu em uma caracterização diferencial completa (incluindo espectro diferencial, ambiguidade e deficiência) de todos os polinômios de permutação sobre corpos finitos com baixo grau (grau até 6). Os resultados desta primeira parte foram compilados em um artigo publicado, em 2017, na revista "Finite Fields and Their Applications" (classificada como A2 pelo Qualis CAPES de 2017). Na segunda parte, executada de mar/2017 a fev/2018, no escopo de um projeto de pesquisa do departamento INE/UFSC, o objetivo foi realizar uma busca computacional por permutações APN definidas em anéis sobre inteiros. Esta parte envolveu implementações (em C/C++) de buscas exaustivas do tipo "backtracking" podadas com heurísticas específicas a fim de encontrar permutações APN (2-uniformes) sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ (alvo principal do presente trabalho). Os melhores resultados obtidos nesta segunda parte consistiram em algumas permutações *3-uniformes* sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$. Notamos que isto corresponde a uma busca em um universo de busca de tamanho $32! \simeq 2^{117.6}$. Os melhores casos encontrados pelo backtracking (com a poda heurística) foram refinados com a aplicação de técnicas de busca heurística do tipo "Tabu search" e "Simulated Annealing". O melhor resultado obtido nesta segunda parte chegou muito perto de uma permutação APN (2-uniforme) e consistiu em uma permutação *3-uniforme* sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$, mas com apenas 24 valores iguais a 3 no espectro diferencial (todos os outros 968 valores eram menores ou iguais a 2, como é o caso de uma APN).

Palavras-chave: criptografia simétrica, funções booleanas, projeto de caixas-S, funções APN, não-linearidade, criptoanálise diferencial, buscas heurísticas

Contents

Chapter 1

Introdução

1.1 Contextualização

No campo da Criptografia Simétrica, as duas estratégias de projeto de cifradores mais comuns são as Redes de Substituição-Permutação (SPNs) e as Redes de Feistel. Ambas contêm, como componentes não-lineares críticos para um embaralhamento eficaz da mensagem, uma série de componentes de substituição chamados caixas-S. Um exemplo de uma SPN é justamente o padrão mundial atual, o Advanced Encryption Standard (AES) [20].

Uma caixa-S consiste de funções vetoriais booleanas, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, construídas de modo a satisfazer certos critérios criptográficos. Uma condição fundamental a ser imposta sobre estas funções é que elas devem apresentar uma alta resistência às criptoanálises diferencial [18] e linear [19], dois dos principais ataques conhecidos contra cifradores em bloco atuais.

Em particular, o presente trabalho trata da construção de caixas-S resistentes à criptoanálise diferencial. O ataque diferencial tem sucesso quando dois textos em claro, montados de maneira a apresentar uma diferença (xor) especialmente escolhida, produzem, após a penúltima iteração, blocos cuja diferença assume um certo valor (conveniente ao ataque) com uma alta probabilidade. A segurança de uma função com respeito ao ataque diferencial depende, portanto, de uma certa "uniformidade diferencial" das caixas-S usadas no cifrador. De fato, encontrar caixas-S apropriadas, de modo a garantir que o cifrador que as usa resista a ataques diferenciais, tem sido *um dos principais tópicos de pesquisa em criptografia simétrica dos últimos 20 anos* [26].

As funções que possuem a melhor resistência ao ataque diferencial são chamadas de "Quase Perfeitamente Não-lineares" ("Almost perfect nonlinear" ou "APNs"). Mais precisamente:

Definição 1. *Seja $f : G_1 \to G_2$ qualquer mapeamento entre dois grupos abelianos finitos G_1 e G_2 de mesmo tamanho. Para $a \in G_1,\ a \neq 0$, definimos um mapeamento diferencial como:*

$$\Delta_{f,a}(x) = f(x + a) - f(x)$$

*Uma função é chamada de "Perfeitamente Não-linear" (PN) se $\Delta_{f,a}$ é injetiva e "Quase Perfeitamente Não-linear" (**APN**) se $\Delta_{f,a}$ é, no pior caso, 2-para-1.*

Na verdade, a resistência de uma caixa-S à criptoanálise diferencial está de tal forma ligada à injetividade de $\Delta_{f,a}(x)$ que é usual detalhar esta injetividade um pouco melhor, com base no parâmetro definido por Nyberg [11] e reproduzido a seguir.

Definição 2. *[11] Sejam G_1 e G_2 dois grupos abelianos finitos. Um mapeamento $f : G_1 \to G_2$ é chamado de "δ **diferencial**" se, para todo $\alpha \in G_1$, $\alpha \neq 0$, e $\beta \in G_2$, temos:*

$$|\{x \in G_1 \mid f(x+\alpha) - f(x) = \beta\}| \leq \delta$$

Ou seja, se f é δ-diferencial, a função respectiva $\Delta_{f,a}(x)$ pode até não ser injetiva, mas o número de "colisões" registradas, para qualquer x, não pode passar de δ. Em particular, note que o AES usa uma função inversa em $\mathbb{F}_{2^8}$ que é 4-diferencial (ou seja, $\Delta_{f,a}$ é, no pior caso, 4-para-1) [21]. Por outro lado, o sistema criptográfico SAFER [22] usa as funções APN $f(x) = 45^x$ e $f(x) = \log_{45} x$, definidas sobre $\mathbb{Z}_{256}$.

Permutações 4-diferenciais têm grande interesse no projeto de primitivas criptográficas simétricas. Por razões evidentes de implementação, soluções definidas sobre corpos como $\mathbb{F}_{2^{8k}}$ são as preferidas. Ocorre que permutações APN sobre $\mathbb{F}_{2^n}$ para n par só são conhecidas para $n = 6$ (descrito mais abaixo). Então, na falta de APNs (2-uniformes) sobre $\mathbb{F}_{2^{8k}}$, as 4-uniformes são aquelas que garantem a melhor resistência a ataques diferenciais na maioria dos casos práticos [26].

1.1.1 Permutações e criptografia

Definição 3. *Um mapeamento $f : G_1 \to G_2$, entre dois grupos abelianos de mesmo tamanho, é chamado de permutação quando f é uma função bijetora.*

Há muitas vantagens em se ter uma função APN que também é permutação (é fácil ver que permutações PN não existem: a diferença igual a 0 nunca vai aparecer). Permutações APN aparecem em muitas aplicações criptográficas. Além de serem fundamentais no projeto de caixas-S criptográficas, elas aparecem, por exemplo, como componentes fundamentais do paradigma PbE ("permutação-based encryption"), usado na concepção da função hash Keccak, vencedora do recente concurso SHA3 [24].

Neste trabalho de pós-doutorado, o foco foi a busca e a caracterização de funções do tipo *permutação* que apresentam boa resistência à criptoanálise diferencial, ou seja, o foco foi sobre as *permutações APN*.

As permutações de interesse podem ser definidas diretamente sobre corpos finitos $\mathbb{F}_q$ ou sobre anéis, tais como $\mathbb{Z}_n$ (o anel dos inteiros mod n). Conforme mencionado anteriormente, a caixa-S do AES funciona sobre $\mathbb{F}_{2^8}$ e o cifrador SAFER utiliza uma permutação definida sobre $\mathbb{Z}_{256}$.

1.1.2 Construção de permutações APN

De uma maneira geral, as funções APN, ou seja, funções f para as quais $\delta(f) = 2$, são **raras e difíceis de encontrar**. De acordo com Voloch [23], a densidade destas funções tende assintoticamente para zero no conjunto de todas as funções. Além disto, poucas famílias infinitas são conhecidas. Isto indica por que a construção de *permutações* APN ainda é um tema de extrema relevância atualmente.

De fato, a primeira *permutação* APN sobre $\mathbb{F}_{2^6}$ foi apresentada por Blinhaning et al. [14] somente em 2010, refutando de vez uma resistente conjectura de que não havia permutações APN sobre $\mathbb{F}_{2^n}$ para n par. O método empregado por Blinhaning et al. é baseado principalmente na representação de funções APN por códigos. De acordo com Charpin ([8], sec. 9.2.), a busca por permutações APN de $\mathbb{F}_{2^n}$ para n par, com $n \geq 8$, ainda é um tema de pesquisa de grande interesse.

Na busca de permutações APN, costuma-se partir de construções que, reconhecidamente, produzem permutação (tais como alguns polinômios), para depois analisar se as funções produzidas são APN [1].

1.1.3 Construção de APNs sobre $\mathbb{F}_q$

Sobre $\mathbb{F}_q$, costuma-se produzir permutações com **polinômios de permutação**. No clássico livro de Lidl e Niederreiter, podem ser encontrados alguns critérios que permitem identificar se um dado polinômio é de permutação [9]. Algumas classes de polinômios de permutação sobre um corpo finito são as seguintes [1]:

- os monômios $F(x) = x^d$ sobre $\mathbb{F}_q$
- os polinômios linearizados
- os polinômios de Dembowski-Ostrom
- os polinômios de Dickson

Em particular, os monômios formam uma classe muito conveniente de candidatos a permutação, pois eles usualmente possuem um baixo custo de implementação em hardware [27]. A resistência de algumas classes de monômios a ataques diferenciais é analisada por Blondeau et al. em [26] e [27].

Conforme Blondeau et al., algumas classes de permutações APN monomiais sobre $\mathbb{F}_{2^n}$ são conhecidas quando n é ímpar, mas permutações monomiais APN não existem quando n é par. Logo, permutações 4-diferenciais são de grande interesse quando n é par [26]. Note-se que a função utilizada na caixa-S do AES consiste em uma permutação monomial. Note-se ainda, a respeito da função $f(x) = x^{2^n-2}$ sobre $\mathbb{F}_2^n$ utilizada no AES, que Nyberg [11] provou que se trata de uma permutação 4-uniforme (com apenas *uma ocorrência* da colisão 4-para-1), quando n é par.

1.1.4 Construção de APNs sobre $\mathbb{Z}_n$

Sobre $\mathbb{Z}_n$, os métodos encontrados na literatura incluem as permutações APN obtidas com base em **Costas arrays** [25] e também as permutações APN sobre inteiros que são produzidas com base nas **funções derivadas de monômios** propostas por Panario et al. em [6], na busca de permutações com valores ótimos de ambiguidade e deficiência (ver abaixo).

Na busca de permutações APN sobre os inteiros mod n, Drakakis et al. utilizaram uma construção de Costas arrays do tipo Welch para construir permutações APN $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$, sendo p um número primo [25].

De maneira semelhante à construção de Drakakis, Panario et al. também utilizam uma construção do tipo "exponencial", com base em um gerador do grupo multiplicativo de $\mathbb{F}_q$, mas compõem esta exponenciação com um monômio adequadamente escolhido [6].

Neste trabalho, o interesse recaiu sobre a busca de permutações APN $f_2 : \mathbb{Z}_2 \times \mathbb{Z}_{2^k} \to \mathbb{Z}_2 \times \mathbb{Z}_{2^k}$. A definição sobre anéis deste tipo visou verificar se a busca seria, de alguma forma, facilitada pela estrutura diferente em relação à dos anéis simples sobre inteiros, tais como $f_1 : \mathbb{Z}_{2^k} \to \mathbb{Z}_{2^k}$. Também havia interesse em comparar a resistência a ataques diferenciais dos dois tipos de permutações (f_1 e f_2), definidas sobre anéis com estruturas diferentes. Observou-se que a ambiguidade atinge níveis mais baixos no caso simples (f_1), sugerindo que estes anéis mais simples podem ser mais adequados ao uso em criptografia do que os compostos do tipo f_2.

1.1.5 Os conceitos de ambiguidade e deficiência

Neste item é apresentado o último elemento essencial à definição do objeto do presente projeto de pós-doutorado: as noções de ambiguidade e deficiência.

Os trabalhos do Prof. Panario sobre o assunto (por exemplo, [6] e [1]) mostram que estas duas noções constituem-se em medidas mais finas de avaliação da uniformidade diferencial de uma permutação do que as que existiam na literatura para este propósito. Pretende-se, portanto, utilizá-las como um guia eficiente na busca de novas permutações APN e na sua partual classificação posterior.

Foi justamente a tentativa de compreender melhor quão próxima está uma permutação dada (f) de ser uma função APN que levou o grupo do Prof. Panario a uma geralização dos conceitos de injetividade e sobrejetividade de uma função $\Delta_{f,a}$, chegando aos dois conceitos novos. A correta aplicação destes conceitos tem ajudado a compreender melhor as características fundamentais das permutações APN [6].

Em [6], Panario et al. derivam limites inferiores para os valores de ambiguidade e deficiência de uma permutação $f : G \to G$ e mostram que as **funções que correspondem ao mínimo de ambiguidade são sempre APNs**. Mais importante ainda, eles apresentam um método de construção de permutações APN sobre os inteiros ($f : \mathbb{Z}_n \to \mathbb{Z}_n$) que efetivamente leva a permutações que **atingem os valores ótimos (mínimos) para ambiguidade e deficiência**.

A construção por eles proposta é baseada em uma composição de monômios de permutação e geração por elementos primitivos no grupo multiplicativo de $\mathbb{F}_q$. O resultado é um método de construção que, quando aplicado a $\mathbb{Z}_{256}$, produz caixas-S com valores ótimos de ambiguidade e deficiência. Só para comparação, a caixa-S utilizada no cifrador SAFER [22] também utiliza uma permutação APN sobre $\mathbb{Z}_{256}$, mas com valores de ambiguidade e deficiência **mais de 20 vezes superiores ao valor ótimo previsto teoricamente** por Panario et al. [6].

Eles também comparam uma construção (não-APN) por eles proposta com base na função de Möbius como permutação sobre $\mathbb{F}_{2^n}$ à função inversa utilizada na caixa-S do AES e concluem que a função de Möbius sobre o grupo multiplicativo de $\mathbb{F}_q$ está mais próxima de ser APN do que a função inversa [6].

Seus resultados e análises teóricas permitem concluir que as medidas de ambiguidade e deficiência consistem em uma medida segura, mais detalhada do que as tradicionais uniformidades diferenciais, da adequação de uma permutação para ser usada como parte de uma caixa-S. Seus resultados também indicam que as medidas de ambiguidade e deficiência estão fortemente relacionadas com não-linearidade. Em [1], por exemplo, eles computam a linearidade da permutação APN usada no SAFER como sendo 42.484 . Se, em vez da função original, o SAFER utilizasse uma permutação APN com valores ótimos de ambiguidade e deficiência, esta linearidade baixaria para 35.791 . A conclusão é que permutações com valores ótimos de ambiguidade e deficiência são candidatos muito bons ao uso no projeto de caixas-S, levando a construções muito consistentes, tanto em relação à sua resistência a ataques diferenciais quanto às suas sólidas propriedades de não linearidade.

1.2 Trabalho realizado no pós-doutorado

O trabalho realizado neste pós-doutorado consistiu em *duas partes* com características distintas de pesquisa. Na primeira parte, correspondente aos primoiros 8 meses, o foco foi mais matemático, recaindo pesadamente sobre a teoria de corpos finitos. A segunda parte foi mais computacional, consistindo em diversas tentativas de otimização, com métodos heurísticos adequados, das buscas intensivas por uma permutação com as características esperadas sobre os anéis compostos de inteiros.

1.2.1 PARTE I

Nesta primeira parte do trabalho, foi realizada uma caracterização diferencial completa (incluindo espectro diferencial, ambiguidade e deficiência) de todos os polinômios de permutação (normalizados) sobre corpos finitos com baixo grau (grau até 6).

Polinômios de permutação têm sido muito estudados recentemente devido ao fato de apresentarem importantes aplicações relacionadas com criptografia, teoria de códigos e design combinatorial. Muito embora a lista completa dos polinômios de permutação (normalizados) com grau até 6 já tivesse sido determinada há algum tempo (ver [9] e [28]), uma caracterização

completa de suas propriedades diferenciais ainda não havia sido publicada, exatamente devido à dificuldade de análise apresentada por dois polinômios de 5^o grau específicos desta lista. O foco principal desta primeira parte do trabalho de pós-doutorado consistiu justamente no *estudo completo e detalhado deste dois polinômios de* 5^o *grau cruciais*.

Essencialmente, esta primeira parte consistiu na aplicação e adaptação de diversos conceitos de um subdomínio da álgebra abstrata denominado de *corpos finitos* (fundamental ao campo da criptografia), envolvendo muitas deduções teóricas (inclusive com a prova de um teorema aplicado) e também muitas implementações práticas, com o auxílio do sistema computacional matemático em software livre SAGE [33].

Nesta parte, diversos elementos do livro clássico de Lidl e Niederreiter [9] sobre corpos finitos tiveram que ser adaptados ao problema da busca de raízes para polinômios de permutação, no caso dos dois polinômios cruciais. O resultado foi um conjunto de fórmulas exatas descrpardo completamente o perfil diferencial destes polinômios, o que permitiu, junto com diversas outras análises menos extensas, construir os perfis diferenciais de todos os polinômios de permutação (normalizados) com grau menor ou igual a 6.

Os resultados obtidos foram submetidos a um journal da área de corpos finitos ("*Finite Fields e their Applications*", classificado como B1 pela CAPES) e já receberam pareceres favoráveis dos revisores.

1.2.2 PARTE II

A segunda parte envolveu implementações (em C/C++) de buscas exaustivas do tipo "backtracking" podadas com heurísticas específicas, a fim de encontrar permutações APN (2-uniformes) sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ (alvo principal desta parte). [1]

O melhor resultado obtido nesta segunda parte chegou muito perto de uma permutação APN (2-uniforme) e consistiu em uma permutação *3-uniforme* sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$, mas com apenas 24 valores iguais a 3 no espectro diferencial (todos os outros 968 valores eram menores ou iguais a 2, como seria o caso de uma APN). Note-se que, até o momento, nenhuma permutação APN é conhecida em anéis sobre inteiros com 32 elementos, como é caso de $\mathbb{Z}_2 \times \mathbb{Z}_{16}$.

Os resultados da segunda parte ainda estão sendo refinados pelo autor, em conjunto com o grupo de pesquisa do Prof. Panario, e deverão ser encaminhados para publicação nos próximos meses.

[1] Note-se que isto corresponde a um universo de busca de tamanho $32! \simeq 2^{117.6}$.

Part I

Perfil diferencial de polinômios de permutação de baixo grau

Chapter 2

Ambiguidade e deficiência de $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$ sobre $\mathbb{F}_q$

O principal obstáculo para a caracterização completa da lista de polinômios de permutação de grau até 6 consistia exatamente na dificuldade técnica de obtenção do perfil diferencial do polinômio $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$ sobre $\mathbb{F}_q$.

Este capítulo mostra em detalhes a extensa análise deste polinômio, desde a formulação do problema, até a obtenção das fórmulas exatas que caracterizam totalmente o seu espectro diferencial, assim como a sua ambiguidade e deficiência.

2.1 Definições básicas

As definições a seguir foram adaptadas de [1]. Seja um corpo finito $\mathbb{F}_q$ e seja F_w uma função de $\mathbb{F}_q$ para $\mathbb{F}_q$ com parâmetro w. Então, definimos:

Definição 4.

- *Mapeamento de diferenças:*

$$\forall a \in \mathbb{F}_q,\ a \neq 0: \quad \Delta_{F_w,a}(x) = F_w(x+a) - F_w(x)$$

- *Número de raízes de $\Delta_{F_w,a}(x) = b$:*

$$\forall a, b \in \mathbb{F}_q,\ a \neq 0: \quad \lambda_{a,b}(F_w) = |\Delta^{-1}_{F_w,a}(b)|$$

- *Número de raízes de $\Delta_{F_w,a}(x) = b$ de acordo com sua multiplicidade k:*

$$n^a_k(F_w) = \left|\left\{b \ : \ |\Delta^{-1}_{F_w,a}(b)| = k\right\}\right| \quad (0 \leq k \leq q \ \ e \ \ a \in \mathbb{F}^*_q)$$

Definição 5. *O* ***espectro diferencial*** *de F_w é definido, para $0 \leq k \leq n$, como:*

$$n_k(F_w) = |\{(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q : \ |\Delta_{F_w,a}^{-1}(b)| = k\}|$$

Definição 6. *A* ***deficiência da linha*** *a de F_w é a quantidade de pares tais que $\Delta_{F_w,a}(x) = b$ não tem soluções (para um $a \in \mathbb{F}_q^*$ fixo), ou seja,*

$$D_a(F_w) = n_0^a(F_w) = \left| \left\{ b \in \mathbb{F}_q : \ |\Delta_{F_w,a}^{-1}(b)| = 0 \right\} \right|$$

Definição 7. *A* ***deficiência*** *de F_w, denotada por $D(F_w)$, é definida como $n_0(F_w)$, ou seja:*

$$D(F_w) = \sum_{a \in \mathbb{F}_q^*} D_a(F_w)$$

A deficiência mede o número de pares (a,b) tais que $\Delta_{F_w,a}(x) = b$ *não possui soluções*. Esta é uma medida da *sobrejetividade* de $\Delta_{F_w,a}$: quanto mais baixa a deficiência, mais próximos estão os $\Delta_{F_w,a}$ de serem (coletivamente) sobrejetivos.

Definição 8. *A* ***ambiguidade da linha*** *a de F_w é dada por:*

$$A_a(F_w) = \sum_{b \in \mathbb{F}_q} \binom{\lambda_{a,b}(F_w)}{2} = \sum_{0 \leq k \leq n} n_k^a(F_w) \binom{k}{2}$$

Definição 9. *A* ***ambiguidade*** *(ponderada) de F_w pode ser definida como*

$$A(F_w) = \sum_{a \in \mathbb{F}_q^*} A_a(F_w),$$

ou seja:

$$A(F_w) = \sum_{0 \leq k \leq n} n_k(F_w) \binom{k}{2}$$

Quanto mais baixa a ambiguidade de F_w, mais próxima está a $\Delta_{F_w,a}$ de ser *injetiva*.

2.2 Teorema Principal

O resultado mais importante desta primeira parte do trabalho consistiu na elaboração e prova do "Teorema Principal", apresentado a seguir, o qual resume as fórmulas exatas para o perfil diferencial de F_w.

Teorema 1. *Seja q uma potência prima ímpar com $q \equiv \pm 2 \pmod 5$. Então, para todo $w \in \mathbb{Z}$, a função $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$ é um* polinômio de permutação normalizado *sobre $\mathbb{F}_q$ e, para F_w, valem os seguintes resultados:*

- *Se $-6w/5$ é zero ou não possui raiz quadrada em $\mathbb{F}_q^*$:*

q mod 8	Ambiguidade	Deficiência
1	$(q-1)(q-2)-S$	$\frac{5(q-1)^2}{8}$
3	$(q-1)^2-S$	$\frac{(q-1)(5q-3)}{8}-\frac{S}{2}$
5	$(q-1)(q-2)+S$	$\frac{5(q-1)^2}{8}+\frac{S}{2}$
7	$(q-1)^2+S$	$\frac{(5q-3)(q-1)}{8}$

- *Se $-6w/5$ não é zero e possui raiz quadrada em $\mathbb{F}_q^*$:*

q mod 8	Ambiguidade	Deficiência
1	$(q-3)(q-2)+3(q-1)-S$	$\frac{(q-1)(5q-3)}{8}$
3	$(q-1)(q-2)-S$	$\frac{5q^2-10q+1}{8}-\frac{S}{2}$
5	$(q-3)(q-2)+3(q-1)+S$	$\frac{5q^2-8q+3}{8}+\frac{S}{2}$
7	$(q-1)(q-2)+S$	$\frac{5q^2-10q+1}{8}$

- *Nestas fórmulas,* $S=\sum_{a\in\mathbb{F}_q^*}\chi(\alpha)=\sum_{a\in\mathbb{F}_q^*}\chi\left(\frac{1}{2}+\frac{3w}{5a^2}\right)$ *é dado por*

	$\chi(\frac{1}{2})$	
	$+1$	-1
$\chi(\frac{3w}{5})$		
$+1$	-2	0
0	$q-1$	$-(q-1)$
-1	0	2

2.3 Alguns exemplos numéricos com $w=0$

Para uma melhor compreensão das definições, vamos computar alguns resultados numéricos específicos, para $w=0$, obtidos com SAGE [33], para valores pequenos de q's, antes de tentar obter fórmulas fechadas para ambiguidade e deficiência como funções do tamanho do corpo q.

2.3.1 $F_0(x) = x^5 \in \mathbb{F}_2[x]$

- $F(x)$:

x	0	1
$F(x)$	0	1

$\Delta_{F,a}(x)$:

$a\backslash x$	0	1
1	1	1

$\lambda_{a,b}$:

$a\backslash b$	0	1
1	0	2

$n_k(F)$:

k	0	1	2
n_k	1	0	1

- Deficiência: $D = n_0 = 1$

  Ambiguidade: $A = 1.\binom{0}{2} + 0.\binom{1}{2} + 1.\binom{2}{2} = 1$

2.3.2 $F_0(x) = x^5 \in \mathbb{F}_3[x]$

- $F_0(x)$:

x	0	1	2
$F_0(x)$	0	1	2

$\Delta_{F_0,a}(x)$:

$a\backslash x$	0	1	2
1	1	1	1
2	2	2	2

$\lambda_{a,b}$:

$a\backslash b$	0	1	2
1	0	3	0
2	0	0	3

$n_k^a(F_0)$:

$a\backslash k$	0	1	2	3
1	2	0	0	1
2	2	0	0	1

- Deficiência: $D(F_0) = n_0^1 + n_0^2 = 4$
- Ambiguidade: $A(F_0) = 2 \times \left(2 \times \binom{0}{2} + 0 \times \binom{1}{2} + 0 \times \binom{2}{2} + 1 \times \binom{3}{2}\right) = 6$

2.3.3 $F_0(x) = x^5 \in \mathbb{F}_7[x]$

- $F_0(x)$:

x	0	1	2	3	4	5	6
$F_0(x)$	0	1	4	5	2	3	6

$\Delta_{F_0,a}(x)$:

$a\backslash x$	0	1	2	3	4	5	6
1	1	3	1	4	1	3	1
2	4	4	5	5	4	4	2
3	5	1	6	1	5	5	5
4	2	2	2	2	6	1	6
5	3	5	3	3	2	2	3
6	6	6	4	6	3	6	4

$\lambda_{a,b}$:

$a\backslash b$	0	1	2	3	4	5	6
1	0	4	0	2	1	0	0
2	0	0	1	0	4	2	0
3	0	2	0	0	0	4	1
4	0	1	4	0	0	0	2
5	0	0	2	4	0	1	0
6	0	0	0	1	2	0	4

$n_k^a(F_0)$:

k	0	1	2	3	4	(5..7)
$1 \le a \le 6$	4	1	1	0	1	0

- Deficiência: $D(F_0) = 6 \times n_0^1 = 24$
- Ambiguidade: $A(F_0) = 6 \times \left(4 \times \binom{0}{2} + 1 \times \binom{1}{2} + 1 \times \binom{2}{2} + 0 \times \binom{3}{2} + 1 \times \binom{4}{2}\right) = 42$

2.3.4 $F_0(x) = x^5 \in \mathbb{F}_{3^2}[x]$

- Nota: quando $w = 0$, os casos nos quais $q \equiv 4 \pmod 5$ correspondem a polinômios de permutação.

$F_0(x)$:

x	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
$F(x)$	0	1	2	2x	x+1	2x+1	x	x+2	2x+2

(f(x) = x^2 + 2x+ 2)

$\Delta_{F_0,a}(x)$:

$a\backslash x$	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	1	1	2x+1	x	2	2	x	2x+1
2	2	2	2	1	x+2	2x	x+2	1	2x
x	2x	x	2x+2	2x	1	1	2x	2x+2	x
x+1	x+1	2x	2x+1	2x+2	x+1	2x+2	2x+1	2x	x+1
x+2	2x+1	2x+2	x+2	2	2	2x+1	2x+2	2x+1	x+2
2x	x	x+1	2x	x	2x	x+1	x	2	2
2x+1	x+2	2x+1	x+1	x+1	2x+1	x+2	1	x+2	1
2x+2	2x+2	x+2	x	x+2	2x+2	x	x+1	x+1	2x+2

$\lambda_{a,b}$:

$a\backslash b$	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	0	3	2	2	0	0	0	2	0
2	0	2	3	0	0	2	2	0	0
x	0	2	0	2	0	0	3	0	2
x+1	0	0	0	0	3	0	2	2	2
x+2	0	0	2	0	0	2	0	3	2
2x	0	0	2	3	2	0	2	0	0
2x+1	0	2	0	0	2	3	0	2	0
2x+2	0	0	0	2	2	2	0	0	3

$n_k^a(F_0)$:

$a\backslash k$	0	1	2	3	4	(5..9)
$\forall a \in \mathbb{F}_9^*$	5	0	3	1	0	0

Deficiência: $D(F_0) = 8 \times n_0^1 = 40$

Ambiguidade: $A(F_0) = 8 \times \left(5 \times \binom{0}{2} + 0 \times \binom{1}{2} + 3 \times \binom{2}{2} + 1 \times \binom{3}{2} + 0 \times \binom{4}{2}\right) = 48$

2.3.5 $F_0(x) = x^5 \in \mathbb{F}_{13}[x]$

$F_0(x)$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$F_0(x)$	0	1	6	9	10	5	2	11	8	3	4	7	12

$\Delta_{F_0,a}(x)$:

$a\backslash x$	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	5	3	1	8	10	9	10	8	1	3	5	1
2	6	8	4	9	5	6	6	5	9	4	8	6	2
3	9	9	12	6	1	3	1	6	12	9	9	7	7
4	10	4	9	2	11	11	2	9	4	10	10	12	10
5	5	1	5	12	6	12	5	1	5	11	2	2	11
6	2	10	2	7	7	2	10	2	6	3	5	3	6
7	11	7	10	8	10	7	11	3	11	6	6	11	3
8	8	2	11	11	2	8	12	8	1	7	1	8	12
9	3	3	1	3	3	9	4	11	2	2	11	4	9
10	4	6	6	4	4	1	7	12	10	12	7	1	4
11	7	11	7	5	9	4	8	7	7	8	4	9	5
12	12	12	8	10	12	5	3	4	3	5	12	10	8

$\lambda_{a,b}$:

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10	11	12
1	0	4	0	2	0	2	0	0	2	1	2	0	0
2	0	0	1	0	2	2	4	0	2	2	0	0	0
3	0	2	0	1	0	0	2	2	0	4	0	0	2
4	0	0	2	0	2	0	0	0	0	2	4	2	1
5	0	2	2	0	0	4	1	0	0	0	0	2	2
6	0	0	4	2	0	1	2	2	0	0	2	0	0
7	0	0	0	2	0	0	2	2	1	0	2	4	0
8	0	2	2	0	0	0	0	1	4	0	0	2	2
9	0	1	2	4	2	0	0	0	0	2	0	2	0
10	0	2	0	0	4	0	2	2	0	0	1	0	2
11	0	0	0	0	2	2	0	4	2	2	0	1	0
12	0	0	0	2	1	2	0	0	2	0	2	0	4

$n_k(F_0)$:

$a\backslash k$	0	1	2	3	4	(5..13)
$1 \leq a \leq 12$	7	1	4	0	1	0

Deficiência: $D(F_0) = 12 \times n_0^1 = 84$

Ambiguidade: $A(F_0) = 12 \times \left(7 \times \binom{0}{2} + 1 \times \binom{1}{2} + 4 \times \binom{2}{2} + 0 \times \binom{3}{2} + 1 \times \binom{4}{2}\right) = 120$

2.3.6 $F_0(x) = x^5 \in \mathbb{F}_{17}[x]$

$F_0(x)$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$F_0(x)$	0	1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16

$\Delta_{F_0,a}(x)$:

$a\backslash x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	14	7	16	10	10	4	15	16	15	4	10	10	16	7	14	1
2	15	4	6	9	3	14	2	14	14	2	14	3	9	6	4	15	2
...							...										

$\lambda_{a,b}$:

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	2	0	0	2	0	0	2	0	0	4	0	0	0	2	2	3
2	0	0	3	2	2	0	2	0	0	2	0	0	0	0	4	2	0
...							...										

$n_k(F_0)$:

$a\backslash k$	0	1	2	3	4	$(5-17)$
$1 \leq a \leq 16$	10	0	5	1	1	0

- Deficiência: $D(F_0) = 16 \times n_0^1 = 160$
- Ambiguidade: $A(F_0) = 16 \times \left(10 \times \binom{0}{2} + 0 \times \binom{1}{2} + 5 \times \binom{2}{2} + 1 \times \binom{3}{2} + 1 \times \binom{4}{2}\right) = 224$

2.3.7 $F(x) = x^5 \in \mathbb{F}_{19}[x]$

$F(x)$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$F(x)$	0	1	13	15	17	9	5	11	12	16	3	7	8	14	10	2	4	6	18

$\Delta_{F,a}(x)$:

$a\backslash x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	12	2	2	11	15	6	1	4	6	4	1	6	15	11	2	2	12	1
2	13	14	4	13	7	2	7	5	10	10	5	7	2	7	13	4	14	13	2
...							...												

$\lambda_{a,b}$:

$a\backslash b$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	0	4	4	0	2	0	3	0	0	0	0	2	2	0	0	2	0	0	0
2	0	0	3	0	2	2	0	4	0	0	2	0	0	4	2	0	0	0	0
...							...												

$n_k(F)$:

k	0	1	2	3	4	$5-19$
n_k	216	0	72	18	36	0
$\frac{n_k}{q-1}$	12	0	4	1	2	0

- Deficiência: $D = n_0 = 216$
- Ambiguidade: $A = 216.\binom{0}{2} + 0.\binom{1}{2} + 72.\binom{2}{2} + 18.\binom{3}{2} + 36.\binom{4}{2} = 342$

Chapter 3

Prova do Teorema Principal - Parte 1

3.1 Ambiguidade, Deficiência e $\Delta_{F_w,a}(x) = b$

Os valores de ambiguidade e deficiência para um dado tamanho de corpo $q = p^n$ (uma potência de primo) dependem unicamente dos valores no vetor n_k^a ($0 \leq k \leq q$ e $1 \leq a \leq q$). O vetor n_k^a resume a distribuição de valores em uma linha a dada de $\lambda_{a,b}$, conforme segue:

- para um dado k ($0 \leq k \leq q$), o valor n_k^a conta quantas vezes o valor "k" aparece na linha a da tabela de $\lambda_{a,b}$;
- para um $a \in \mathbb{F}_q^*$ fixo, cada valor na linha a de $\lambda_{a,b}$ mostra, para cada $b \in \mathbb{F}_q$ correspondente, quantas vezes este valor b aparece in linha a de $\Delta_{F,a}(x)$;
- equivalentemente, cada valor $\lambda_{a,b}$ mostra, para um valor $a \in \mathbb{F}_q^*$ fixo, quantas vezes (ou: para quantos x's) um dado $b \in \mathbb{F}_q$ é produzido pela função $F_w(x+a) - F_w(x)$.

Desta forma, n_k^a depende de quantas soluções existem, no corpo $\mathbb{F}_q$, para a equação $\Delta_{F_w,a}(x) = b$, ou seja:

$$(x+a)^5 + w(x+a)^3 + \frac{w^2}{5}(x+a) - x^5 - wx^3 - \frac{w^2}{5}x = b \tag{3.1}$$

E a busca por uma fórmula para computar ambiguidade e deficiência para q e w dados implica na caracterização, em $\mathbb{F}_q$, das raízes da equação quártica:

$$5ax^4 + 10a^2x^3 + (3aw + 10a^3)x^2 + (3a^2w + 5a^4)x + \frac{aw^2}{5} + a^3w + a^5 = b \tag{3.2}$$

Uma vez que esta equação pode ter um máximo de 4 raízes, $\forall a \in \mathbb{F}_q^*$ e $\forall b \in \mathbb{F}_q$, podemos concluir que devemos ter $0 \leq k \leq 4$. Em outras palavras, as entradas em n_k^a contam, para cada possível valor de multiplicidade μ da solução de 3.2, quantas vezes este μ aparece na tabela de $\lambda_{a,b}$.

3.2 Uma equação particular para $\Delta_{F_w,a}(x) = b$

Uma vez que $a \in \mathbb{F}_q^*$, tanto a^{-1} como a^{-2} e a^{-5} sempre existem e podemos executar a seguinte mudança de variáveis:

$$y = \frac{x}{a}$$

$$v = \frac{w}{a^2}$$

$$c = \frac{b}{a^5}$$

levando a:

$$5y^4 + 10y^3 + (3v + 10)y^2 + (3v + 5)y + \frac{v^2}{5} + v + 1 = c \tag{3.3}$$

Note que:

1. enquanto b percorre todos os valores em $\mathbb{F}_q$, c também o faz;
2. uma vez que estamos interessados apenas no número de soluções desta equação, e não nas raízes específicas, não importa se usamos "x" ou "x/a";
3. o parâmetro "v" não pode ser simplificado (por exemplo, para $v = 1$) porque cada "a" diferente define uma equação totalmente diferente.

Concluímos que, para cada v, a caracterização das raízes da Eq. 3.2 pode ser feita, sem perda de geralidade, com o valor de a fixo em 1 para "y" e para "c". Desta forma, a equação a ser analisada pode ser simplificada para $\Delta_{F_v,1}(x) = b$, ou:

$$x^4 + 2x^3 + \left(\frac{3v + 10}{5}\right)x^2 + \left(\frac{5 + 3v}{5}\right)x + \frac{1}{5}\left(1 + \frac{v^2}{5} + v\right) = \frac{b}{5} \tag{3.4}$$

Porém, antes de analisar esta equação, é melhor simplificá-la para a forma quadrática, conforme é descrito abaixo.

3.3 Uma equação quadrática para $\Delta_{F_v,1}(x) = b$

Considere uma equação quártica em sua forma geral:

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

É sabido que, com uma mudança de variável adequada, ela pode ser convertida para uma forma na qual o termo cúbico desaparece e em que a resolução fica usualmente mais fácil [2]:

- mudando a variável para:

$$x = z - \frac{a_3/a_4}{4}$$

- leva a:

$$z^4 + Az^2 + Bz + C = 0$$

- onde:

$$\begin{aligned} A &= \frac{8a_2a_4 - 3a_3^2}{8a_4^2} \\ B &= \frac{a_3^3 - 4a_2a_3a_4 + 8a_1a_4^2}{8a_4^3} \\ C &= \frac{-3a_3^4 + 256a_0a_4^3 - 64a_1a_3a_4^2 + 16a_2a_3^2a_4}{256a_4^4} \end{aligned}$$

Desta forma, com a mudança de variável $z = x + \frac{1}{2}$, obtemos que a Eq. 3.4 pode ser re-escrita como:

$$z^4 + \left(\frac{1}{2} + \frac{3v}{5}\right)z^2 + \left(\frac{v^2}{25} + \frac{v}{20} + \frac{1}{80} - \frac{b}{5}\right) = 0 \tag{3.5}$$

Finalmente, uma vez que esta é uma equação biquadrática, podemos mudar uma vez mais para $t = z^2$, obtendo a equação que será o principal elemento para caracterizar a estrutura de $\lambda_{a,b}$ e, em consequecia, ambiguidade e deficiência em $\mathbb{F}_q$ neste trabalho:

$$t^2 + \left(\frac{1}{2} + \frac{3v}{5}\right)t + \left(\frac{v^2}{25} + \frac{v}{20} + \frac{1}{80} - \frac{b}{5}\right) = 0 \tag{3.6}$$

3.4 Computando o espectro diferencial de $F_v(x)$ em $\mathbb{F}_q$

Vimos que uma caracterização completa das raízes do polinômio $\Delta_{F_v,1}(x) - b = 0$ (ver Eq. 3.4) de acordo com as suas multiplicidades k, resumidas em $n_k^a(F_v)$, leva diretamente à determinação de ambiguidade e deficiência para $F_v(x)$, em um dado $\mathbb{F}_q$. Esta caracterização, também conhecida como *espectro diferencial* de $F_v(x)$ em $\mathbb{F}_q$, pode ser baseada na equação mais simples Eq. 3.5. De fato, uma vez que a relação entre x e z é linear, elas possuem as mesmas multiplicidades.

Mas, neste caso, o modo mais fácil de computar o espectro consiste em usar a equação quadrática. Dependendo do discriminante δ_t da Eq. 3.6 sendo um square (SQ), um não-square (NS) ou ZERO, é possível especificar o número de "t-soluções" (raízes de 3.6) que estão no corpo $\mathbb{F}_q$. Então, com base na determinação do caráter de cada "t-solução" como SQ, NS ou ZERO, é possível saber o número exato (0, 1, 2, 3 ou 4) de "z-soluções" em $\mathbb{F}_q$.

Desta forma, a questão relativa a "quantas z-soluções existem para a Eq. 3.4 em $\mathbb{F}_q$?" pode ser respondida com base na Eq. 3.6. Mais especificamente, esta questão pode ser respondida com base no discriminante da Eq. 3.6, dado por:

$$\delta_t = \frac{(v+1)^2 + 4.b}{5} \tag{3.7}$$

e nas suas t-soluções, dadas por:

$$t = \frac{1}{2}\left(-\alpha \pm \sqrt{\delta_t}\right) \tag{3.8}$$

onde α é dado por:

$$\alpha = \frac{1}{2} + \frac{3v}{5} \tag{3.9}$$

As residuosidades quadráticas dos parâmetros δ_t e t são as chaves para a distribuição dos q possíveis valores de $b \in \mathbb{F}_q$ entre as 5 possíveis multiplicidades (0, 1, 2, 3 ou 4) associadas às raízes da Eq. 3.5 (ou Eq. 3.4) que estão em $\mathbb{F}_q$. Portanto, δ_t e t são as chaves para construir $\lambda_{a,b}$ e, consequentemente, para a computação dos valores de ambiguidade e deficiência associados a um dado $F_v(x)$.

A classificação dos valores de δ_t e t como "SQ", "NS" ou "ZERO" leva a uma distribuição dos q possíveis b's entre as multiplicidades das z-soluções. primeiramente, esta distribuição é baseada na residuocidade quadrática de δ_t e, em um segundo monento, as residuosidades quadráticas dos t's determinam o número de z-soluções (raízes) diferentes para a Eq. 3.5.

O parâmetro δ_t, mostrado na Eq. 3.7, é linearmente dependente de b, de modo que ele assume todos os valores em $\mathbb{F}_q$. Uma vez que q é ímpar, é sempre o caso que $x \neq -x$, de modo que, além de 0, exatamente $\frac{q-1}{2}$ valores em $\mathbb{F}_q$ podem ser squares. Isto explica o primoiro nível na seguinte divisão dos q valores assumidos por b em três categorias.

Além disto, a distribuição dos b valores depende do parâmetro α ser ou não zero (note que $\alpha = \frac{1}{2} + \frac{3v}{5}$ foi definido na Eq. 3.9). Como está detalhado no capítulo 5, para $\alpha = 0$, a dedução das formulas deve seguir um rumo particular, saindo do caso geral (onde $\alpha \neq 0$).

Dependendo do valor específico de v, o nível mais alto na distribuição dos q possíveis b-valores entre as 5 possíveis quantidades de z-soluções diferentes consiste dos casos detalhado abaixo. Desta forma,

- seja $N_{\text{X.y.z}}$ o contador do número de ocorrências no item "x.y.z":
  - $N^{\alpha}_{\text{X.y.z}}$ corresponde a $N_{\text{X.y.z}}$ quando $\alpha \neq 0$;
  - $N^{0}_{\text{X.y.z}}$ corresponde a $N_{\text{X.y.z}}$ quando $\alpha = 0$;

- Note que, em ambos os casos de α, os $N_{\text{X.y.z}}$'s devem totalizar q.

Então, uma **caracterização das raízes** completa de $\Delta_{F_v,1}(x) = b$ em $\mathbb{F}_q$ é dada por:

(1) caso $\underline{\delta_t \neq 0 \text{ é SQ}}$: ocorre $N_1 = \frac{q-1}{2}$ vezes

- Neste caso, sempre temos *duas t-soluções* t_1 e t_2 (ver Eq. 3.8)
- Uma vez que $t = z^2$, o número de z-soluções depende de quantas das duas t-soluções são zero.
- Desta forma, os N_1 casos são subdivididos entre as seguintes possibilidades (de acordo com α):

  - Sub-caso $\underline{\alpha \neq 0}$: ocorre $N_1 = N_{11}^{\alpha} + N_{12}^{\alpha} + N_{13}^{\alpha} = \frac{q-1}{2}$ vezes, onde:

(1.1) Se $\boxed{t_1 \neq 0 \text{ e } t_2 \neq 0}$: ($N_{11}^{\alpha} = \frac{q-3}{2}$ vezes)

- Então t_1 e t_2 são dados por: $t_1 = \frac{1}{2}\left(-\alpha - \sqrt{\delta_t}\right)$ $t_2 = \frac{1}{2}\left(-\alpha + \sqrt{\delta_t}\right)$
- e o número de z-soluções depende de quantas das duas t-soluções são resíduos quadráticos (SQ):

(1.1.1) Se t_1 é SQ e t_2 é SQ (N_{111}^{α} vezes): **4** diferente z-soluções são produzidas

(1.1.2) Se (t_1 é SQ e t_2 é NS) ou (t_1 é NS e t_2 é SQ) (N_{112}^{α} vezes): **2** diferente z-soluções são produzidas

(1.1.3) Se t_1 é NS e t_2 é NS (N_{113}^{α} vezes): **0** z-soluções são produzidas

- Note que: $N_{11}^{\alpha} = N_{111}^{\alpha} + N_{112}^{\alpha} + N_{113}^{\alpha}$

(1.2) Se $\boxed{(t_1 \neq 0 \text{ e } t_2 = 0) \text{ ou } (t_1 = 0 \text{ e } t_2 \neq 0)}$: (exatamente $N_{12}^{\alpha} = 1$ vez)

- esta situação sempre ocorre, exatamente para: $b = \frac{1}{16} + \frac{6w}{5}$
- então t_1 e t_2 são dados por: $t_1 = -\alpha$ $t_2 = 0$ (ou vice-versa)
- esta ocorrência única deve se encaixar em um dos seguintes subcasos:

(1.2.1) Se t_1 é SQ: ($N_{121}^{\alpha} = 0$ ou 1)

* este subcaso vai ocorrer ($N_{121}^{\alpha} = 1$) se e somente se $\chi(-\alpha) = 1$
* e **3** z-soluções diferentes serão produzidas

(1.2.2) Se t_1 é NS: ($N_{122}^{\alpha} = 1$ ou 0)

* este subcaso vai ocorrer ($N_{122}^{\alpha} = 1$) se e somente se $\chi(-\alpha) = -1$
* e apenas **1** z-soluções serão produzidas

(1.3) Se $\boxed{t_1 = 0 \;\text{ e }\; t_2 = 0}$: $(N_{13}^{\alpha} = 0)$

– este situação *nunca ocorre* quando $\alpha \neq 0$ e $\delta_t \neq 0$

• Sub-caso $\underline{\alpha = 0}$: ocorre $N_1 = N_{14}^0 + N_{15}^0 + N_{16}^0 = \frac{q-1}{2}$ vezes, onde:

(1.4) Se $\boxed{t_1 \neq 0 \;\text{ e }\; t_2 \neq 0}$: ocorre todas as $\frac{q-1}{2}$ vezes $(N_{14}^0 = \frac{q-1}{2})$

– com t_1 e t_2 dados por: $t_1 = -\frac{\sqrt{\delta_t}}{2}$ $t_2 = \frac{\sqrt{\delta_t}}{2}$

– e o número de z-soluções em cada caso depende de quantas das duas t-soluções são resíduos quadráticos (SQ):

(1.4.1) Se t_1 é SQ e t_2 é SQ $(N_{141}^0$ casos): **4** z-soluções diferentes são produzidas

(1.4.2) Se (t_1 é SQ e t_2 é NS) ou (t_1 é NS e t_2 é SQ) $(N_{142}^0$ casos): **2** diferentes z-soluções são produzidas

(1.4.3) Se t_1 é NS e t_2 é NS $(N_{143}^0$ casos): **0** z-soluções são produzidas

– Note que: $N_{14}^0 = N_{141}^0 + N_{142}^0 + N_{143}^0$

(1.5) Se $\boxed{(t_1 \neq 0 \;\text{ e }\; t_2 = 0) \;\text{ ou }\; (t_1 = 0 \;\text{ e }\; t_2 \neq 0)}$: $(N_{15}^0 = 0)$

– este caso *nunca ocorre*, porque $\alpha = 0$

∗ Note que t_1 e t_2 seriam dados por: $t_1 = -\alpha$ $t_2 = 0$

(1.6) Se $\boxed{t_1 = 0 \;\text{ e }\; t_2 = 0}$: $(N_{16}^0 = 0)$

– este caso *nunca ocorre* quando $\delta_t \neq 0$ (mesmo quando $\alpha = 0$).

(2) caso $\underline{\delta_t \text{ é ZERO}}$: (exatamente $N_2 = 1$ caso)

- este caso único *sempre* ocorre, exatamente para: $b = -\frac{(w+1)^2}{4}$
- este é um caso que leva a *uma t-solução* (ver Eq. 3.8):

• Sub-caso $\underline{\alpha \neq 0}$: $N_2 = N_{21}^{\alpha} + N_{22}^{\alpha} = 1$

- Neste caso, t_1 e t_2 são dados por: $t_1 = t_2 = -\frac{1}{2}\alpha$
- este único sub-caso vai se encaixar em um dos seguintes subcasos:

(2.1) Se $t_1 (= t_2)$ é SQ: $(N_{21}^{\alpha} = 0$ ou $1)$

  - este vai ocorrer $(N_{21} = 1)$ se e somente se $\chi(-\alpha/2) = 1$
  - e **2** diferentes z-soluções serão produzidas

(2.2) Se $t_1(= t_2)$ é NS: $(N_{22}^{\alpha} = 1 \text{ ou } 0)$
  - este vai ocorrer $(N_{22} = 1)$ se e somente se $\chi(-\alpha/2) = -1$
  - e **0** z-soluções serão produzidas

- Sub-caso $\underline{\alpha = 0}$: $N_2 = 1$

- então t_1 e t_2 são dados por: $t_1 = t_2 = 0$
- esta única ocorrência vai levar diretamente a **1** z-solução

(3) caso $\underline{\delta_t \neq 0 \text{ é NS}}$: $(N_3 = \frac{q-1}{2} \text{ vezes})$:

- Nesta situação, não pode haver *nenhuma t-solução* (ver Eq. 3.8)
- Todos os N_3 casos levam a **0** z-soluções

Vários dos valores dos N's já estão completamente determinados, mas mas alguns deles serão computados com a ajuda de *caracteres multiplicativos*, brevemente descritos no capítulo 4. Os N's que ainda precisam ser computados são os seguintes:

- N_{111}^{α}, N_{112}^{α} e N_{113}^{α}: serão determinados no capítulo 5
- N_{121}^{α} e N_{122}^{α}: serão determinados tão logo $\chi(-\alpha)$ pode ser definido (ver capítulo 4)
- N_{141}^{0}, N_{142}^{0} e N_{143}^{0}: serão determinados no capítulo 5
- N_{21}^{α} e N_{22}^{α}: serão determinados tão logo $\chi(-\alpha/2)$ possa ser definido (ver capítulo 4)

Chapter 4

Caracteres multiplicativos

Neste trabalho, usamos o conceito de caracteres multiplicativos para obter fórmulas exatas para a computação dos valores de ambiguidade e deficiência para $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$ sobre $\mathbb{F}_{\tilde{\approx}_q}$, como uma função de q e w. Este capítulo contém uma breve introdução ao assunto "caracteres multiplicativos", assim como alguns resultados básicos necessários nas deduções apresentadas no capítulo 5.

Definição 10. ***([9], pg. 187)*** *Um* caracter χ *é um homomorfismo de um grupo abeliano finito G em um grupo multiplicativo U de números complexos, de valor absoluto 1, que satisfaz:*

$$\forall g_1, g_2 \in G, \quad \chi(g_1 g_2) = \chi(g_1)\chi(g_2)$$

- *O caracter* trivial ϵ *é definido por* $\epsilon(g) = 1, \ \forall g \in G$
- *Se* $\chi \neq \epsilon$, *definimos* $\chi(0) = 0$

Propriedades ([9], pg. 187):

- $\chi(1_G) = 1$, pois: $\chi(1_G) = \chi(1_G)\chi(1_G)$
- $\chi(g)$ é a $|G|^{th}$ raiz da unidade, pois: $(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$
- $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$, pois: $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = 1$
- o conjunto $G^\wedge$ de caracteres de G é finito (os valores dos caracteres só podem ser $|G|^{th}$ raízes da unidade)

Teorema 2. ***([9], theor. 5.4)*** *Se χ é um caracter* nontrivial *do grupo abeliano finito G, então*

$$\sum_{g\in G}\chi(g)=0 \tag{4.1}$$

e, se $g\in G$ com $g\neq 1_G$, então

$$\sum_{\chi\in G^\wedge}\chi(g)=0 \tag{4.2}$$

Corolário 1. ***([9], theor. 5.5)*** *o número de caracteres do grupo abeliano finito G é igual a $|G|$.*

- *Uma vez que* $|G^\wedge|=\sum_{g\in G}\sum_{\chi\in G^\wedge}\chi(g)=\sum_{\chi\in G^\wedge}\sum_{g\in G}\chi(g)=|G|$
  - *Note que $\forall g\neq 1_G$, $\sum_{\chi\in G^\wedge}\chi(g)=0$, e, exatamente para $g=1_G$, $\sum_{\chi\in G^\wedge}\chi(g)=|G^\wedge|$*
  - *Por outro lado, $\forall\chi\neq\epsilon$, $\sum_{g\in G}\chi(g)=0$, e, exatamente para $\chi=\epsilon$, $\sum_{g\in G}\chi(g)=|G|$*

Exemplo 1. ***([9], Ex. 5.1)*** *Considere a situação na qual G é um grupo cíclico finito de ordem n:*

- *seja g um gerador de G*
- *para cada inteiro fixo j $(0\leq j\leq n-1)$, a seguinte função define um caracter de G:*

$$\chi_j(g^k)=\left(e^{\frac{2\pi ij}{n}}\right)^k,\qquad k=0,1,\ldots,n-1 \tag{4.3}$$

- *então, uma vez que $\chi(g)$ deve ser uma n^{th} raiz de unidade, segue que, $\forall\chi\in G^\wedge$, devemos ter $\chi=\chi_j$, para algum $0\leq j\leq n-1$*
- *portanto, neste caso, o conjunto $G^\wedge$ consiste exatamente de $\chi_0,\chi_1,\ldots,\chi_{n-1}$*

4.1 Contando soluções para $x^2 = a$ em $\mathbb{F}_q$

Considere a equação $x^2 = a$ em $\mathbb{F}_q$, a qual é equivalente a determinar se $a \in \mathbb{F}_q$ é um resíduo quadrático ou não. Esta subseção descreve o uso de caracteres para derivar um critério para a solvabilidade desta equação, de acordo com [4].

Teorema 3. ***([9], Theor. 2.8)*** *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

Proposição 1. ***(adaptado de [4], Prop. 4.2.1)*** *Seja p um primo e $q = p^n$. O elemento $a \in \mathbb{F}_q^*$ é um resíduo quadrático ($a = x^2$) se e somente se $a^{\frac{q-1}{2}} = 1$ em $\mathbb{F}_q$.*

Proof. Seja g uma raiz primitiva de $\mathbb{F}_q^*$.

- Então $a = g^b$ e $x = g^y$
- Mas $x^2 = a \quad \Leftrightarrow \quad g^{2y} = g^b$ em $\mathbb{F}_q \quad \Leftrightarrow \quad 2y \equiv b \pmod{q-1}$
- Mas esta congruência pode ser resolvida se e somente se $2|b$
- E $2|b$ se e somente se $a^{\frac{q-1}{2}} = 1$:
  - Se $2|b$: $\quad a^{\frac{q-1}{2}} = g^{b\frac{q-1}{2}} = g^{k(q-1)} = 1$
  - Se $a^{\frac{q-1}{2}} = 1$: $\quad g^{b\frac{q-1}{2}} = 1 \quad \rightarrow \quad (q-1) \mid \frac{b}{2}(q-1) \quad \rightarrow \quad 2|b$
- Portanto, $x^2 = a$ pode ser ersolvida se e somente se $a^{\frac{q-1}{2}} = 1$
- Nota: se $a = 0$ então $x = 0$

□

Proposição 2. ***(adaptado de [4], Prop. 8.1.4)*** *Se $a \in \mathbb{F}_q$, $2|(q-1)$, e $x^2 = a$* não pode ser resolvida*, então existe um caracter χ tal que:*

(a) $\chi^2 = \epsilon$

- *onde ϵ é o caracter multiplicativo trivial, definido por $\epsilon(a) = 1, \ \forall a \in \mathbb{F}_q$*
- *ϵ é equivalente ao caso $j = 0$ na Eq. 4.3*

(b) $\chi(a) \neq 1$

Proof. seja g um gerador de $\mathbb{F}_q^*$:

- Defina o caracter: $\lambda(g^k) = e^{2\pi i \frac{k}{q-1}}$ (ver Eq. 4.3)
  - de modo que: $\lambda(g) = e^{\frac{2\pi i}{q-1}}$
- Atribua $\chi = \lambda^{\frac{q-1}{2}}$ (isto pode ser computado, uma vez que caracteres formam um grupo)
- Então $\chi(g) = \lambda^{\frac{q-1}{2}}(g) = \lambda(g)^{\frac{q-1}{2}} = e^{\pi i} = -1$
- Mas $a = g^l$ para algum l
- Uma vez que $x^2 = a$ *não pode ser resolvida*, devemos ter: $2 \nmid l$ (l é ímpar)
- Então $\chi(a) = \chi(g)^l = (-1)^l = -1 \neq 1$
- Finalmente: $\chi^2 = \lambda^{q-1} = \epsilon$

□

Agora, seja $N(x^2 = a)$ o número de soluções da equação $x^2 = a$ em $\mathbb{F}_q$. Uma vez que $2|q-1$, temos a proposição a seguir.

Proposição 3. ***(adaptado para $\mathbb{F}_q$ de [4], Prop. 8.1.5)***

$$N(x^2 = a) \;=\; \sum_{\chi^2=\epsilon} \chi(a) \;=\; \epsilon(a) + \chi^1(a)$$

Proof.

- Como na Prop. 2, sabemos que existe um caracter χ tal que $\chi(g) = e^{2\pi i/2} = -1$
- Segue que $\chi^0 = \epsilon$ e χ^1 são os (únicos) 2 caracteres distintos de ordem dividindo 2
- Primeiro, note que a fórmula funciona para $a = 0$
  - uma vez que $\epsilon(0) = 1$ e $\chi(0) = 0$ para $\chi \neq \epsilon$
- Agora, suponha que $a \neq 0$ e que $x^2 = a$ é solvável (a é um resíduo quadrático):
  - então existe b tal que $b^2 = a$
  - agora, uma vez que $\chi^2 = \epsilon$:
    - $\chi(a) = \chi(b^2) = \chi(b)^2 = \chi^2(b) = \epsilon(b) = 1$
  - portanto: $\sum_{\chi^2=\epsilon} \chi(a) = 2$

– e a fórmula funciona também neste caso

- Finalmente, suponha que $a \neq 0$ e que $x^2 = a$ é não solvável:
  - seja $T = \sum_{\chi^2=\epsilon} \chi(a)$
  - devemos mostrar que $T = 0$
  - mas este é exatamente o caso da Prop. 2:
    - ∗ então existe um caracter ρ tal que $\rho(a) \neq 1$ e $\rho^2 = \epsilon$
  - agora considere:

$$\rho(a)T = \rho(a) \sum_{\chi^2=\epsilon} \chi(a) = \sum_{\chi^2=\epsilon} \rho(a)\chi(a) = \sum_{\chi^2=\epsilon} \rho\chi(a) = T$$

    - ∗ caracteres de ordem 2 formam um grupo
    - ∗ e obtemos: $(\rho(a) - 1)T = 0$
    - ∗ então, uma vez que $\rho(a) \neq 1$, temos que $T = 0$

□

Exemplo 2. ***(ver [4], pg. 91)*** *Como um caso especial, considere que $q = p$ é um primo ímpar.*

- *Seja g um gerador de $\mathbb{F}_p^*$*
- *O teorema diz que:*

$$N(x^2 = a = g^k) = \sum_{\chi^2=\epsilon} \chi(a) = \chi^0(a)+\chi^1(a) = \epsilon(a)+\chi^1(g^k) = 1+(\chi^1(g))^k = 1+(-1)^k$$

- *Então, uma vez que k é par, se a é um resíduo quadrático, este pode ser re-escrito, em $\mathbb{F}_p$, como:*

$$N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$$

4.2 Avaliando $\chi(2)$ em $\mathbb{F}_q$

Seja q uma potência de primo ($q = p^n$). Afirmamos que $\chi(2)$ em $\mathbb{F}_q$ é dado por

$$\chi(2) = (-1)^{\frac{q^2-1}{8}} \tag{4.4}$$

Para ver isto, seguimos [4] e notamos que, se $\boxed{q \equiv 1 \pmod 8}$ (ver [4], pg. 70):

- Seja γ um gerador de $\mathbb{F}_q^*$
- Defina $\lambda = \gamma^{\frac{q-1}{8}}$. Então, em $\mathbb{F}_q^*$:

$$\lambda^8 \equiv 1 \quad \rightarrow \quad \lambda^4 \equiv -1 \quad \rightarrow \quad \lambda^2 \equiv -\lambda^{-2} \quad \rightarrow \quad \lambda^2 + \lambda^{-2} \equiv 0$$

- Portanto: $(\lambda + \lambda^{-1})^2 \equiv \lambda^2 + 2 + \lambda^{-2} \equiv 2$
  - isto mostra que 2 é um resíduo quadrático em $\mathbb{F}_q^*$
- E a Eq. 4.4 está correta no caso $q \equiv 1 \pmod 8$.

Agora considere o caso em que $\boxed{q \not\equiv 1 \pmod 8}$, ou seja, $q \equiv -1 \pmod 8$ ou $q \equiv \pm 3 \pmod 8$. Nestes casos, a ideia central, de acordo com [4] (pg. 85), é que ainda temos $q^2 \equiv 1 \pmod 8$ e uma dedução similar ainda pode ser efetuada, trabalhando em um corpo finito de dimensão 2 sobre $\mathbb{Z}_q$:

- Desta forma, seja $q^2 \equiv 1 \pmod 8$
- E seja η um gerador em $\mathbb{F}_{q^2}^* = \mathbb{F}_{p^n \times p^n}^* = \mathbb{F}_{p^{2n}}^*$
- Defina: $\mu = \eta^{\frac{q^2-1}{8}}$. Então, em $\mathbb{F}_{q^2}^*$:

$$\mu^8 \equiv 1 \quad \rightarrow \quad \mu^4 \equiv -1 \quad \rightarrow \quad \mu^2 \equiv -\mu^{-2} \quad \rightarrow \quad \mu^2 + \mu^{-2} \equiv 0$$

- Portanto: $(\mu + \mu^{-1})^2 \equiv \mu^2 + 2 + \mu^{-2} \equiv 2$
  - Isto mostra que 2 é (sempre) um resíduo quadrático em $\mathbb{F}_{q^2}^*$.
  - (Mas a situação em $\mathbb{F}_q$ ainda tem que ser determinada.)
- Desta forma, vamos definir: $\tau = \mu + \mu^{-1}$.
  - Note que μ satisfaz à equação $x^8 - 1 = 0$, de modo que μ e τ são inteiros algébricos sobre $\mathbb{F}_q$ e podemos, portanto, trabalhar com congruências em um anel de inteiros algébricos sob (similar a [4], pg. 69).

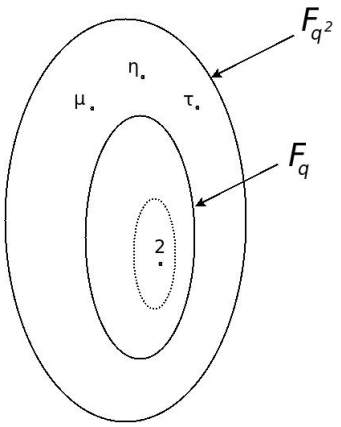

Figure 4.1: Alguns elementos em $\mathbb{F}_{q^2}$

– os 3 elementos η, μ e τ são representados esquematicamente na Fig. 4.1.

- Então temos:

$$\tau^{q-1} = (\tau^2)^{\frac{q-1}{2}} = 2^{\frac{q-1}{2}} \equiv \chi(2) \text{ em } \mathbb{F}_q^* \tag{4.5}$$

– Note que 2 é um resíduo quadrático (QR) em $\mathbb{F}_q^*$ se e somente se $2^{\frac{q-1}{2}} \equiv 1$:

∗ Seja g um gerador de $\mathbb{F}_q^*$ e $2 = g^k$

∗ Se 2 é QR, então k é par, e $2^{\frac{(q-1)}{2}} = g^{\frac{k}{2}(q-1)} \equiv 1$ in $\mathbb{F}_q^*$

∗ Se 2 não é QR, então k é ímpar, e $2^{\frac{(q-1)}{2}} = g^{k\frac{(q-1)}{2}} = \left(g^{\frac{(q-1)}{2}}\right)^k$

- Mas, uma vez que $g^{q-1} \equiv 1$ em $\mathbb{F}_q^*$, devemos ter $g^{\frac{(q-1)}{2}} \equiv -1$

- Finalmente, uma vez que k é ímpar, se 2 não é QR, então $2^{\frac{q-1}{2}} \equiv -1$

- Segue da Eq. 4.5 que:

$$\tau^q \equiv \chi(2)\tau \text{ em } \mathbb{F}_q^* \tag{4.6}$$

- por outro lado:

$$\tau^q = (\mu + \mu^{-1})^q \equiv \mu^q + \mu^{-q} \text{ em } \mathbb{F}_q^*$$

- Lembrando que $\mu^8 \equiv 1$, podemos ver que, em $\mathbb{F}_q^*$:
  - Se $q \equiv \pm 1 \pmod 8$: $\mu^q + \mu^{-q} \equiv \mu + \mu^{-1} = \tau$
  - Se $q \equiv \pm 3 \pmod 8$: $\mu^q + \mu^{-q} \equiv \mu^3 + \mu^{-3} \equiv -(\mu + \mu^{-1}) = -\tau$
    - Uma vez que $\mu^4 \equiv -1 \rightarrow \mu^3 \equiv -\mu^{-1}$

- Eq. 4.6 pode então ser escrita como: $(-1)^{\frac{q^2-1}{8}}\tau \equiv \chi(2)\tau$ em $\mathbb{F}_q^*$
  - o que implica em:

$$\chi(2) = (-1)^{\frac{q^2-1}{8}} \tag{4.7}$$

4.3 Somas de Jacobi

Na análise do capítulo 5, precisaremos ser capazes de computar os valores de algumas somas de caracteres chamadas de "somas de Jacobi".

Definição 11. ***(adaptado de [4], pg. 93)*** *Uma* soma de Jacobi $J(\chi, \lambda)$ *é definida como:*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

- *onde:* χ *e* λ *são caracteres de* $\mathbb{F}_q$

Teorema 4. ***(adaptado de [4], pg. 93)*** *Sejam* χ *e* λ *caracteres não triviais. Então:*

(a) $J(\epsilon, \epsilon) = p$

(b) $J(\epsilon, \chi) = 0$

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$

Proof. A parte (b) é uma imediata consequência da Eq. 4.2. Em relação à parte (c):

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right)$$

- Fixe $\frac{a}{1-a} = c$
- Se $c \neq -1$, então $a = \frac{c}{1+c}$

- segue que, à medida em que a vara sobre $\mathbb{F}_q$, menos o elemento 1, c varia sobre $\mathbb{F}_q$, menos o elemento -1.
  - (existe um único pólo em $a = 1$ e este mesmo pólo é definido por $c = -1$)
- Portanto:

$$J(\chi, \chi^{-1}) = \sum_{c \neq -1} \chi(c) = 0 - \chi(-1) = -\chi(-1)$$

□

4.4 Contando soluções para $x^2 + y^2 = 1$ em $\mathbb{F}_q$

Esta subseção descreve o uso de caracteres para contar o número de soluções para uma equação $x^2 + y^2 = 1$ sobre $\mathbb{F}_q$, de acordo com [4] (ver pg. 92):

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a) \times N(y^2 = b) \tag{4.8}$$

De acordo com a proposição 3, a Eq. 4.8 pode ser re-escrita como:

$$\begin{aligned} N(x^2 + y^2 = 1) &= \sum_{a+b=1} \left(\sum_{\chi^2=\epsilon} \chi(a) \times \sum_{\chi^2=\epsilon} \chi(b) \right) \\ &= \sum_{a+b=1} \Big(\big(\epsilon(a) + \chi(a)\big) \times \big(\epsilon(b) + \chi(b)\big) \Big) \\ &= \sum_{a+b=1} \Big(\big(1 + \chi(a)\big) \times \big(1 + \chi(b)\big) \Big) \\ &= \sum_{a+b=1} \Big(1 + \chi(a) + \chi(b) + \chi(a) \times \chi(b) \Big) \end{aligned}$$

levando a uma soma de somatórios que podem ser avaliados:

$$\begin{aligned} N(x^2 + y^2 = 1) &= \sum_{a+b=1} 1 + \sum_{a+b=1} \chi(a) + \sum_{a+b=1} \chi(b) + \sum_{a+b=1} (\chi(a) \times \chi(b)) \\ &= q + 0 + 0 + \sum_{a+b=1} (\chi(a) \times \chi(b)) \\ &= q + J(\chi, \chi) \\ &= q + J(\chi, \chi^{-1}) \end{aligned}$$

onde a última igualdade vale porque χ é um caracter quadrático (e $\chi^2 = \epsilon$)

Desta forma, o número de soluções de $x^2 + y^2 = 1$ é:

$$N(x^2 + y^2 = 1) \;=\; q \;-\; \chi(-1) \tag{4.11}$$

onde $\chi(-1)$ é dado por:

- Seja g um gerador de $\mathbb{F}_q^*$
- Então:

$$\chi(-1) \;=\; (-1)^k \;= (-1)^{\frac{q-1}{2}} \tag{4.12}$$

  - onde k é definido como: $g^k = -1$ (ver Exemplo 1)
  - temos $k = \frac{q-1}{2}$ porque $g^{\frac{q-1}{2}} = -1$, uma vez que $g^{q-1} = 1$ e $q-1$ é a ordem de $\mathbb{F}_q^*$

4.5 Computando $S_{A,B} = \sum_{x \in \mathbb{F}_q^*} \chi(A + Bx^2)$

Esta subseção descreve o uso de caracteres para computar o valor de

$$S_{A,B} = \sum_{x \in \mathbb{F}_q^*} \chi(A + Bx^2) \tag{4.13}$$

para algumas constantes $A, B \in \mathbb{F}_q^*$. Esta soma é um elemento importante na determinação da ambiguidade e deficiência de $F_w(x)$ (ver seções 6.2 e 6.3).

Para chegar a isto, vamos determinar $\mathcal{N}_\theta$, definido como

$$\mathcal{N}_\theta = \left| \left\{ x \in \mathbb{F}_q^* \;:\; \chi\big(A + Bx^2\big) = \theta \right\} \right| \tag{4.14}$$

para $\theta = +1, 0$ e -1, ou seja, vamos contar separadamente o número de $A + Bx^2 \in \mathbb{F}_q^*$ que caem em cada uma das 3 categorias (SQ, ZERO e NS). Uma vez que estes resultados estejam disponíveis, a Eq. 4.13 pode ser re-escrita simplesmente como

$$S_{A,B} \;=\; \mathcal{N}_{+1} \times (+1) + \mathcal{N}_0 \times (0) + \mathcal{N}_{-1} \times (-1) \;=\; \mathcal{N}_{+1} - \mathcal{N}_{-1} \tag{4.15}$$

As seguintes propriedades da residuosidade quadrática em $\mathbb{F}_q^*$ serão necessárias nas próximas subseções.

Proposição 4. *Seja $a, b \in \mathbb{F}_q^*$. Então temos as propriedades:*

- *Se a e b são SQ in $\mathbb{F}_q^*$, então $a \times b$ também é SQ.*

- *Se a é SQ e b é NS, então $a \times b$ é NS.*
- *Se a é NS e b é NS, então $a \times b$ é SQ.*

Proof. Para um caracter quadrático χ, temos: $\chi(ab) = \chi(a) \times \chi(b)$. □

4.5.1 Contando zeros em $A + Bx^2$

Dados $A, B \in \mathbb{F}_q^*$, precisamos contar o número de $x \in \mathbb{F}_q^*$ tais que $A + Bx^2$ é ZERO. Esta computação deve ser subdividida em 4 casos, dependendo dos valores de A e B:

- Se $A = 0$ e $B = 0$: $\mathcal{N}_0 = q - 1$
  - qualquer que seja o valor de x, o resultado será zero
- Se $A \neq 0$ e $B = 0$: $\mathcal{N}_0 = 0$
- Se $A = 0$ e $B \neq 0$: $\mathcal{N}_0 = 0$
  - nenhum zero pode aparecer porque $x \neq 0$
- Se $A \neq 0$ e $B \neq 0$: $\mathcal{N}_0 = 1 + \chi(-1)\chi(A)\chi(B)$
  - para que um zero ocorra, devemos ter $A + Bx^2 = 0$ ou $-\frac{A}{B} = x^2$
  - ou seja, $-\frac{A}{B}$ deve ser um square em $\mathbb{F}_q^*$
    - Se $\chi(-\frac{A}{B}) = 1$, existem 2 zeros
    - Se $\chi(-\frac{A}{B}) = -1$, não existem zeros
  - Finalmente, note que $\chi(-\frac{A}{B}) = \chi(-1)\chi(A)\chi(B)$

Estes resultados estão resumidos na tabela 4.1.

	$\chi(A)$		
	$+1$	0	-1
$\chi(B)$			
$+1$	$1 + \chi(-1)$	0	$1 - \chi(-1)$
0	0	$q - 1$	0
-1	$1 - \chi(-1)$	0	$1 + \chi(-1)$

Table 4.1: valores de $\mathcal{N}_0$ ("número de $x \in \mathbb{F}_q^*$ tais que $A + Bx^2$ é ZERO").

4.5.2 Contando squares em $A + Bx^2$

Agora, dados $A, B \in \mathbb{F}_q^*$, precisamos contar o número de $x \in \mathbb{F}_q^*$ tais que $A + Bx^2$ é square (SQ). Esta computação também deve ser subdividida em 4 casos, dependendo dos valores de A e B:

- Se $A = 0$ e $B = 0$: $\mathcal{N}_{+1} = 0$
  - qualquer que seja o valor de x, o resultado nunca será SQ

- Se $A \neq 0$ e $B = 0$: $\mathcal{N}_{+1} = (q-1)\frac{(1+\chi(A))}{2}$
  - Se A é SQ $(\chi(A) = 1)$, qualquer que seja o valor de x, $A + Bx^2$ sempre será SQ
  - Se A é NS $(\chi(A) = -1)$, qualquer que seja o valor de x, $A + Bx^2$ nunca será SQ

- Se $A = 0$ e $B \neq 0$: $\mathcal{N}_{+1} = (q-1)\frac{(1+\chi(B))}{2}$
  - Se B é SQ $(\chi(B) = 1)$, qualquer que seja o valor de x, $A + Bx^2$ sempre será SQ
    - porque x^2 é obviamente SQ
  - Se B é NS $(\chi(B) = -1)$, qualquer que seja o valor de x, $A + Bx^2$ nunca será SQ
    - porque o produto de um NS e um SQ é sempre NS (ver proposição 4)

- Se $A \neq 0$ e $B \neq 0$: $\mathcal{N}_{+1} = \frac{q-2-\chi(B)-\chi(A)\left[\chi(-1)\chi(B)+1\right]}{2}$
  - Se $\chi(B) = +1$ (B é SQ):
    - então, para uma constante $A \in \mathbb{F}_q^*$, temos que lidar com $A + r = s$, onde $r = Bx^2$ é, obviamente, square e s é SQ
    - equivalentemente, precisamos computar o número de pares (y, z) que satisfazem $A + z^2 = y^2$ ou
    $$y^2 - z^2 = A \tag{4.16}$$
    - o que pode ser feito com uma ligeira adaptação da seção 4.4
    - Desta forma, seja $N(y^2 - z^2 = A)$ o número de soluções para a Eq. 4.16:

$$
\begin{aligned}
N(y^2 - z^2 = A) &= \sum_{\substack{s-r=A \\ s\neq 0,A \\ r\neq 0,-A}} N(y^2 = s) \times N(z^2 = r) \\
&= \sum_{\substack{s-r=A \\ s\neq 0,A \\ r\neq 0,-A}} ((1+\chi(s)) \times (1+\chi(r))) \\
&= \sum_{\substack{s-r=A \\ s\neq 0,A \\ r\neq 0,-A}} (1+\chi(s)+\chi(r)+\chi(s)\times\chi(r)) \\
&= (q-2) \ + \ (0-\chi(A)) \ + \ (0-\chi(-A)) \ + \ \sum_{\substack{s-r=A \\ s\neq 0,A \\ r\neq 0,-A}} \chi\left(\frac{s}{r}\right) \\
&= (q-2) \ - \ \chi(A)\big[\chi(-1)+1\big] \ + \ \sum_{c\neq 0,1} \chi(c) \\
&= (q-3) \ - \ \chi(A)\big[\chi(-1)+1\big]
\end{aligned}
$$

* então, podemos computar $\mathcal{N}_{+1}^{\chi(B)=+1}$ como:

$$
\mathcal{N}_{+1}^{\chi(B)=+1} = \frac{N(y^2 - z^2 = A)}{2} = \frac{(q-3) \ - \ \chi(A)\big[\chi(-1)+1\big]}{2} \tag{4.18}
$$

- a divisão por 2 é justificada porque s é o mesmo com y e com $-y$

- (no entanto, z e $-z$ vêm de diferentes valores de x e devem ser contados separadamente)

– Se $\chi(B) = -1$ (B é NS):

* então, para uma constante $A \in \mathbb{F}_q^*$, temos que lidar com $A + r = s$, onde $r = Bx^2$ é NS (ver proposição 4) e s é SQ

* equivalentemente, precisamos computar o número de soluções de:

$$
s - r = A \tag{4.19}
$$

onde s é SQ e r é NS

* o que, uma vez mais, pode ser feito com uma ligeira adaptação da seção 4.4

* Desta forma, seja $N(s - r = A)$ o número de soluções da Eq. 4.19:

$$
\begin{aligned}
N(s-r=A) &= \sum_{\substack{s-r=A\\ s\neq 0,A\\ r\neq 0,-A}} N(s=y^2)\times N(r\neq z^2)\\
&= \sum_{\substack{s-r=A\\ s\neq 0,A\\ r\neq 0,-A}} \big((1+\chi(s))\times(1-\chi(r))\big)\\
&= \sum_{\substack{s-r=A\\ s\neq 0,A\\ r\neq 0,-A}} (1+\chi(s)-\chi(r)-\chi(s)\times\chi(r))\\
&= (q-2) \;+\; (0-\chi(A)) \;-\; (0-\chi(-A)) \;-\; (-1)\\
&= (q-1) \;+\; \chi(A)\big[\chi(-1)-1\big]
\end{aligned}
$$

∗ então, podemos computar $\mathcal{N}_{+1}^{\chi(B)=-1}$ como:

$$
\mathcal{N}_{+1}^{\chi(B)=-1} = \frac{(q-1) \;+\; \chi(A)\big[\chi(-1)-1\big]}{2} \tag{4.21}
$$

– Juntando as Eqs. 4.18 e 4.21, obtemos

$$
\mathcal{N}_{+1} = \frac{q-2-\chi(B) \;-\; \chi(A)\big[\chi(-1)\chi(B)+1\big]}{2}
$$

Os resultados desta subseção estão resumidos na tabela 4.2.

	$\chi(A)$		
	$+1$	0	-1
$\chi(B)$			
$+1$	$\frac{q-\chi(-1)}{2}-2$	$q-1$	$\frac{q+\chi(-1)}{2}-1$
0	$q-1$	0	0
-1	$\frac{q+\chi(-1)}{2}-1$	0	$\frac{q-\chi(-1)}{2}$

Table 4.2: valores de $\mathcal{N}_{+1}$ ("número de $x \in \mathbb{F}_q^*$ tais que $A+Bx^2$ é SQ").

4.5.3 Contando non-squares em $A + Bx^2$

Para completar a caracterização quadrática de $A+Bx^2$, dados $A, B \in \mathbb{F}_q^*$, precisamos contar o número de $x \in \mathbb{F}_q^*$ tais que $A + Bx^2$ é non-square (NS). Isto poderia seguir um caminho

similar ao que foi feito na subseção 4.5.2, mas um modo muito mais fácil é notar que deve ser o caso que:

$$\mathcal{N}_{+1} + \mathcal{N}_0 + \mathcal{N}_{-1} \;=\; q - 1$$

e os resultados para este caso são mostrados na tabela 4.3.

	$\chi(A)$		
	$+1$	0	-1
$\chi(B)$			
$+1$	$\frac{q-\chi(-1)}{2}$	0	$\frac{q+\chi(-1)}{2} - 1$
0	0	0	$q-1$
-1	$\frac{q+\chi(-1)}{2} - 1$	$q-1$	$\frac{q-\chi(-1)}{2} - 2$

Table 4.3: valores de $\mathcal{N}_{-1}$ ("número de $x \in \mathbb{F}_q^*$ tais que $A + Bx^2$ é NS").

4.5.4 Somando tudo em $S_{A,B}$

Finalmente, usando as Tables 4.2 e 4.3, podemos facilmente computar o valor de $S_{A,B}$, o qual, de acordo com as Eqs. 4.13 e 4.15, é dado por

$$S_{A,B} = \sum_{x \in \mathbb{F}_q^*} \chi(A + Bx^2) \;=\; \mathcal{N}_{+1} - \mathcal{N}_{-1}$$

Os resultados são mostrados na tabela 4.4.

	$\chi(A)$		
	$+1$	0	-1
$\chi(B)$			
$+1$	-2	$q-1$	0
0	$q-1$	0	$-(q-1)$
-1	0	$-(q-1)$	2

Table 4.4: Valores de $S_{A,B}$.

Chapter 5

Prova do Teorema Principal - Parte 2

A distribuição do número de raízes de $\Delta_{F_v,a} = b$ de acordo com suas multiplicidades k, registrada em $n_k^a(F_v)$, é também conhecida como o *espectro diferencial* de $F_v(x)$. Como foi discutido na seção 3.4, ele pode ser deduzido a partir de uma caracterização das soluções para uma equação quártica. Esta distribuição é resumida abaixo para referência:

- Seja $t = z^2$ uma raiz de: $\quad t^2 + \left(\frac{1}{2} + \frac{3v}{5}\right) t + \left(\frac{v^2}{25} + \frac{v}{20} + \frac{1}{80} - \frac{b}{5}\right) = 0$

  então: $\quad t = \frac{1}{2}\left(-\alpha \pm \sqrt{\delta_t}\right)$

  onde: $\quad \delta_t = \frac{(v+1)^2+4.b}{5}$, $\quad \alpha = \frac{1}{2} + \frac{3v}{5}$ $\quad$ e $\quad v = \frac{w}{a^2}$

- então, de acordo com os q possíveis valores de b, temos a seguinte distribuição:

(1) Se $\underline{\delta_t \neq 0 \text{ é SQ}}$: $\quad (N_1 = \frac{q-1}{2}$ casos)

- Se $\underline{\alpha \neq 0}$: $\quad N_1 = N_{11}^{\alpha} + N_{12}^{\alpha}$, $\quad$ onde:

(1.1) Se $\boxed{t_1 \neq 0 \;\text{ e }\; t_2 \neq 0}$: $\quad N_{11}^{\alpha} = N_{111}^{\alpha} + N_{112}^{\alpha} + N_{113}^{\alpha} = \frac{q-3}{2}$

$t_1 = \frac{1}{2}\left(-\alpha - \sqrt{\delta_t}\right) \qquad t_2 = \frac{1}{2}\left(-\alpha + \sqrt{\delta_t}\right)$

(1.1.1) Se t_1 é SQ e t_2 é SQ, temos: N_{111}^{α} casos de **4** z-soluções

(1.1.2) Se (t_1 é SQ e t_2 é NS) ou (t_1 é NS e t_2 é SQ): N_{112}^{α} casos de **2** z-soluções

(1.1.3) Se t_1 é NS e t_2 é NS: N_{113}^{α} casos de **0** z-soluções

(1.2) Se $\boxed{(t_1 = 0 \text{ e } t_2 \neq 0) \text{ ou } (t_1 \neq 0 \text{ e } t_2 = 0)}$: $N_{12}^{\alpha} = 1$

$t_1 = -\alpha \qquad t_2 = 0$

(1.2.1) Se $\chi(-\alpha) = 1$, este caso leva a **3** diferentes z-soluções

(1.2.2) Se $\chi(-\alpha) = -1$, este caso leva a apenas **1** z-solução

(1.3) Se $\boxed{t_1 = 0 \text{ e } t_2 = 0}$: nunca ocorre

- Se $\underline{\alpha = 0}$: $N_1 = N_{14}^0$, onde:

(1.4) Se $\boxed{t_1 \neq 0 \text{ e } t_2 \neq 0}$: $N_{14}^0 = N_{141}^0 + N_{142}^0 + N_{143}^0 = \frac{q-1}{2}$

$t_1 = -\frac{\sqrt{\delta_t}}{2} \qquad t_2 = \frac{\sqrt{\delta_t}}{2}$

(1.4.1) Se t_1 é SQ e t_2 é SQ, temos: N_{141}^0 casos de **4** z-soluções

(1.4.2) Se (t_1 é SQ e t_2 é NS) ou (t_1 é NS e t_2 é SQ): N_{142}^0 casos de **2** z-soluções

(1.4.3) Se t_1 é NS e t_2 é NS: N_{143}^0 casos de **0** z-soluções

(1.5) Se $\boxed{(t_1 = 0 \text{ e } t_2 \neq 0) \text{ ou } (t_1 \neq 0 \text{ e } t_2 = 0)}$: nunca ocorre

(1.6) Se $\boxed{t_1 = 0 \text{ e } t_2 = 0}$: nunca ocorre

(2) Se $\underline{\delta_t \text{ é ZERO}}$: (exatamente $N_2 = 1$ caso)

- Se $\underline{\alpha \neq 0}$: $N_2 = N_{21}^{\alpha} + N_{22}^{\alpha} = 1 \qquad t_1 = t_2 = -\frac{1}{2}\alpha$

(2.1) Se $\chi(-\alpha/2) = 1$, este único caso leva a **2** diferente z-soluções

(2.2) Se $\chi(-\alpha/2) = -1$, este único caso leva a **0** z-soluções

- Se $\underline{\alpha = 0}$: este único caso vai levar diretamente a **1** z-solução

(3) Se $\underline{\delta_t \neq 0 \text{ é NS}}$: $N_3 = \frac{q-1}{2}$ casos levando a **0** z-soluções

Vários dos valores dos N's já estão completamente determinados, mas a distribuição dos $\frac{q-3}{2}$ casos no item (1.1) entre os três sub-casos precisa ser considerada em mais detalhe, assim

como o distribuição dos $\frac{q-1}{2}$ casos no item (1.4). É necessário obter as seis fórmulas faltantes (para N^{α}_{111}, N^{α}_{112} e N^{α}_{113} e N^{0}_{141}, N^{0}_{142} e N^{0}_{143}), a fim de caracterizar completamente n^a_k e, portanto, computar ambiguidade e deficiência.

Uma vez que $\delta_t \neq 0$ em todos estes 6 casos, eles sempre levam a duas t-soluções. Os casos faltantes estão relacionados especificamente a contar o número de z-soluções quando os dois t's são não-zero.

5.1 Casos com "$\delta_t \neq 0$ é SQ e $t_1, t_2 \neq 0$" quando $\alpha \neq 0$

Primeiro, vamos contar o número de z-soluções nos subcasos do item (1.1) (N^{α}_{111}, N^{α}_{112} e N^{α}_{113}). Na seção 5.2, os casos com $\alpha = 0$ serão analisados. Esta subdivisão é necessária porque, quando $\alpha = 0$, a *dedução* tem que ser ajustada, e não simplesmente as fórmulas finais.

Uma vez que $t = z^2$, o número de z-soluções depende de quantas das duas t-soluções são SQ.

5.1.1 Caso "t_1 é SQ e t_2 é SQ" (fórmula para N^{α}_{111})

Note que, uma vez que ambos os t's são SQ, para cada t existe um z tal que $t = z^2$ e contar o número N^{α}_{111} de casos no item (1.1.1) é o mesmo que computar quantos pares $(\pm z_1, \pm z_2)$, com $z_1 \neq z_2$, levam ao mesmo $\delta_t \neq 0$. Desta forma, é o mesmo que contar o número de pares que são soluções para:

$$(2z_1^2 + \alpha)^2 = (2z_2^2 + \alpha)^2 \quad \text{em } \mathbb{F}_q$$

- isto é verdadeiro em duas situações: $(2z_1^2 + \alpha) = \pm(2z_2^2 + \alpha)$
- o sinal mais leva à condição: $z_1^2 - z_2^2 = (z_1 + z_2)(z_1 - z_2) = 0 \quad \text{em } \mathbb{F}_q$
  - a qual, uma vez que $z_1 + z_2 \neq 0$, implica na contradição: $z_1 = z_2 \quad \text{em } \mathbb{F}_q$
- o sinal menos leva à condição correta a ser analisada:

$$z_1^2 + z_2^2 = -\alpha \quad \text{em } \mathbb{F}_q \tag{5.1}$$

  - com $z_1^2 \notin \{0, -\frac{\alpha}{2}, -\alpha\}$ e $z_2^2 \notin \{0, -\frac{\alpha}{2}, -\alpha\}$
  - Note que os t's não podem ser $-\alpha/2$ ou $-\alpha$ porque:
    - $t_1 = -\alpha$ exige $t_2 = 0$ (ver item (1.2));

$*$ $t_1 = -\frac{\alpha}{2}$ exige $\delta_t = 0$ (ver item (2)).

$*$ onde (ver Eq. 3.9): $\alpha = \frac{1}{2} + \frac{3v}{5}$

Antes de contar as soluções para a Eq. 5.1, é útil ilustrar esta situação, onde $t_1 \neq 0$ e $t_2 \neq 0$ são ambos SQ's, vindo do mesmo $\delta_t \neq 0$, com os dois exemplos abaixo.

Exemplo 3. *Em* $\mathbb{F}_{13}$, *com* $v = 0$, *temos* $\alpha = \frac{1}{2}$. *A tabela abaixo lista todos os possíveis valores de* δ_t*:*

z	$t = z^2$	$\delta_t = \frac{(4t+1)^2}{4}$
0	0	-3
± 1	1	3
± 2	4	4
± 3	**-4**	**1**
± 4	3	0
± 5	-1	-1
± 6	**-3**	**1**

- *Neste caso, existem 8 possíveis pares de números* z *em* $\mathbb{F}_{13}$ *cujos quadrados não são* 0, $-\frac{1}{4}$ *(que é* 3 *em* $\mathbb{F}_{13}$*) ou* $-\frac{1}{2}$ *(que é* 6 *em* $\mathbb{F}_{13}$*) e levam ao mesmo* $\delta_t \neq 0$*:*

  $$(3,-6),(3,6),(-3,-6),(-3,6),(-6,3),(6,3),(-6,-3),(6,-3)$$

- *Os 4 possíveis valores de* z *(que são* 3, 6, 7 *e* 10*) correspondem aos 4 valores de* $x = z - \frac{1}{2} = z + 6$ *que são contados como soluções para a equação* $\Delta_{F_0,a}(x) = b = 1$ *em* $\mathbb{F}_{13}$.

- *Desta forma, estes 8 pares são contados como um único caso de tipo* (1.1.1) *e, em* $\mathbb{F}_{13}$, *se* $\alpha \neq 0$, *temos* $N^{\alpha}_{111} = 1$.

Exemplo 4. *A tabela abaixo lista todos os possíveis valores de* δ_t, *em* $\mathbb{F}_{3^2}$, *quando* $v = 0$ $(\alpha = \frac{1}{2})$*:*

- *Neste caso, não existem pares de tuplas diferentes* $(z, -z)$ *em* $\mathbb{F}_9$, *cujos quadrados não são* 0 *ou* $-\frac{1}{4}$ *(o qual é* 2 *em* $\mathbb{F}_9$*) ou* $-\frac{1}{2}$ *(o qual é* 1 *em* $\mathbb{F}_9$*), que levam ao mesmo* δ_t.

$(z,-z)$	$t=z^2$	$\delta_t=\frac{(4t+1)^2}{4}$
$(0,0)$	0	1
$(t,2t)$	$t+1$	$2t+2$
$(t+1,2t+2)$	2	0
$(2t+1,t+2)$	$2t+2$	$t+1$
$(2,1)$	1	1

- *Concluímos que nenhum valor de b em $\mathbb{F}_9$ pode levar a 4 diferentes soluções em x ($N_1=0$).*

Agora, para contar os pares $(\pm z_1,\pm z_2)$ que satisfazem a Eq. 5.1, precisamos usar o conceito de *caracteres multiplicativos*. Se $\alpha\neq 0$, podemos computar este número de soluções de um modo similar ao que é descrito na seção 4.4 (sobre contar as soluções para $x^2+y^2=1$):

$$8N_{111}^{\alpha}=N(z_1^2+z_2^2=-\alpha) \tag{5.2}$$

onde:

$$N(z_1^2+z_2^2=-\alpha)=\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} N(z_1^2=t_1)\times N(z_2^2=t_2)=\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\left(\sum_{\chi^2=\epsilon}\chi(t_1)\times\sum_{\chi^2=\epsilon}\chi(t_2)\right) \tag{5.3}$$

$$=\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\Big(\big(\epsilon(t_1)+\chi(t_1)\big)\times\big(\epsilon(t_2)+\chi(t_2)\big)\Big)$$

$$=\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\Big(\big(1+\chi(t_1)\big)\times\big(1+\chi(t_2)\big)\Big)$$

$$=\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\Big(1+\chi(t_1)+\chi(t_2)+\chi(t_1)\chi(t_2)\Big)$$

$$N(z_1^2+z_2^2=-\alpha)=\ (q-3)\ +\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\chi(t_1)\ +\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\chi(t_2)\ +\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\Big(\chi(t_1)\chi(t_2)\Big)$$

$$=\ (q-3)\ +\ 2\Big(0-\chi(0)-\chi(-\alpha/2)-\chi(-\alpha)\Big)\ +\sum_{\substack{t_1+t_2=-\alpha\\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}}\Big(\chi(t_1)\chi(t_2)\Big)$$

E o número de soluções para a Eq. 5.1 é dado por:

$$N(z_1^2 + z_2^2 = -\alpha) = \ (q-3) \ - \ 2\chi(-\alpha/2) \ - \ 2\chi(-\alpha) \ + \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\chi(t_1)\chi(t_2)\Big)$$

$$N(z_1^2+z_2^2 = -\alpha) = \ (q-3) \ - \ 2\chi(-1)\chi(2)\chi(\alpha) \ - \ 2\chi(-1)\chi(\alpha) \ + \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\chi(t_1)\chi(t_2)\Big)$$

$$N(z_1^2+z_2^2 = -\alpha) = \ (q-3) \ - \ 2(-1)^{\frac{q-1}{2}}\chi(\alpha)\Big(\chi(2) \ + \ 1\Big) \ + \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\chi(t_1)\chi(t_2)\Big) \quad (5.6)$$

onde $\chi(-1) = (-1)^k$, com k dado por: $g^k = -1$

Para tornar esta expressão uma fórmula explícita, nós ainda precisamos avaliar $\chi(2)$ e a do tipo "Jacobi" como funções de q e w (ou α).

Seja q uma potência de primo ($q = p^n$). Então, de acordo com a seção 4.2, $\chi(2)$ em $\mathbb{F}_q$ é dado (ver Eq. 4.4) como

$$\chi(2) = (-1)^{\frac{q^2-1}{8}} \quad (5.7)$$

A soma na Eq. 5.6 pode ser avaliada como no teorema 4 (ver seção 4.3):

$$\begin{aligned}
\sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \chi(t_1)\chi(t_2) \ &= \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \chi(t_1)\chi^{-1}(t_2) && (5.8a)\\
&= \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \chi\left(\frac{t_1}{t_2}\right) && (5.8b)\\
&= \sum_{t_1\neq 0,-\frac{\alpha}{2},-\alpha} \chi\left(\frac{t_1}{-\alpha-t_1}\right) && (5.8c)
\end{aligned}$$

Para avaliar a última soma:

- Fixe $c = \frac{t_1}{-\alpha-t_1}$
- Se $c \neq -1$, então: $t_1 = -\frac{\alpha c}{(1+c)}$
- segue que, à medida em que t_1 varia sobre $\mathbb{F}_q$, exceto para o elemento $-\alpha$, c varia sobre $\mathbb{F}_q$, exceto para -1
  (ou: existe um único pólo em $t_1 = -\alpha$ e este mesmo pólo é definido por $c = -1$)

- Portanto:

$$\sum_{t_1\neq 0,-\frac{\alpha}{2},-\alpha} \chi\left(\frac{t_1}{-\alpha-t_1}\right) = \sum_{c\neq -1,0,1} \chi(c) = 0 \ - \ \chi(-1) \ - \ \chi(0) \ - \ \chi(1)$$

E a soma é dada por

$$\sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \chi(t_1)\chi(t_2) \ = \ -\chi(-1)-1 \ = \ -(-1)^{\frac{q-1}{2}}-1 \tag{5.9}$$

Substituindo as Eqs. 4.4 e 5.9 na Eq. 5.6, podemos computar a quantidade N_{111}^{α} (definida na Eq. 5.2) como

$$N_{111}^{\alpha} = \frac{1}{8}\times N(z_1^2+z_2^2=-\alpha) = \frac{1}{8}\times\left[(q-3) \ - \ 2(-1)^{\frac{q-1}{2}}\chi(\alpha)\left((-1)^{\frac{q^2-1}{8}} \ + \ 1\right) \ - \ (-1)^{\frac{q-1}{2}}-1\right]$$

$$N_{111}^{\alpha} = \frac{1}{8}\times\left\{(q \ - \ 4) \ - \ (-1)^{\frac{q-1}{2}}\left[2\chi(\alpha)\left((-1)^{\frac{q^2-1}{8}}+1\right) \ + \ 1\right]\right\} \tag{5.10}$$

Esta fórmula também pode ser escrita como

$$N_{111}^{\alpha} = \begin{cases} \frac{q-9}{8}+\frac{1-\chi(\alpha)}{2}\ , & \text{if } q\equiv 1 \pmod 8 \\ \frac{q-3}{8}\ , & \text{if } q\equiv 3 \pmod 8 \\ \frac{q-5}{8}\ , & \text{if } q\equiv 5 \pmod 8 \\ \frac{q+1}{8}-\frac{1-\chi(\alpha)}{2}\ , & \text{if } q\equiv 7 \pmod 8 \end{cases} \tag{5.11}$$

5.1.2 Caso "um t SQ, um t NS" (fórmula para N_{112}^{α})

A quantidade N_{112}^{α} pode ser computada de um modo similar à Eq. 5.2, mas agora temos que lidar com o número N de soluções para uma equação envolvendo a soma de um SQ e um NS:

$$8N_{112}^{\alpha} = N(\ \overline{t_1}+t_2=-\alpha \quad \text{or} \quad t_1+\overline{t_2}=-\alpha\ ) \tag{5.12}$$

onde, $\overline{t}$ indica que t é NS. Adaptando a Eq. 5.3 a esta nova situação, obtemos:

$$N_{112}^{\alpha} = \frac{1}{8} \times \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(N(t_1 \neq z_1^2) \times N(t_2 = z_2^2) \; + \; N(t_1 = z_1^2) \times N(t_2 \neq z_2^2) \Big) \tag{5.13a}$$

$$= \; \frac{1}{8} \times 2 \times \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(N(t_1 = z_1^2) \times N(t_2 \neq z_2^2) \Big)$$

$$= \; \frac{1}{4} \times \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\big(1+\chi(t_1)\big) \times \big(1-\chi(t_2)\big) \Big)$$

$$= \; \frac{1}{4} \times \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(1+\chi(t_1)-\chi(t_2)-\chi(t_1)\chi(t_2) \Big)$$

$$= \; \frac{1}{4} \times \left((q-3) \; - \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\chi(t_1)\chi(t_2) \Big) \right)$$

Então, usando a Eq. 5.9 de novo, obtemos:

$$N_2 = \frac{1}{4} \times \Big(q - 2 + (-1)^{\frac{q-1}{2}} \Big) \tag{5.14}$$

Ou, equivalentemente:

$$N_2 = \begin{cases} \frac{q-1}{4} \; , & \text{if } q \equiv 1 \pmod 4 \\ \frac{q-3}{4} \; , & \text{if } q \equiv 3 \pmod 4 \end{cases} \tag{5.15}$$

5.1.3 Caso "t_1 é NS e t_2 é NS" (fórmula para N_{113}^{α})

A quantidade N_{113}^{α} pode ser computada de um modo similar a N_{111}^{α} e N_{112}^{α}, mas lidando com a soma de dois não-squares:

$$8N_{113}^{\alpha} = N(\; \overline{t_1} + \overline{t_2} = -\alpha \;) \tag{5.16}$$

onde:

$$N(\; \overline{t_1} + \overline{t_2} = -\alpha \;) = \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(N(z_1^2 \neq t_1) \times N(z_2^2 \neq t_2) \Big)$$

$$N(\ \overline{t_1}+\overline{t_2}=-\alpha\ ) = \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(\big(1-\chi(t_1)\big)\times\big(1-\chi(t_2)\big)\Big) \tag{5.17a}$$

$$= \sum_{\substack{t_1+t_2=-\alpha \\ t_1,t_2\neq 0,-\frac{\alpha}{2},-\alpha}} \Big(1-\chi(t_1)-\chi(t_2)+\chi(t_1)\chi(t_2)\Big)$$

Então, de modo similar à computação de N_{111}^{α}, obtemos:

$$N_{113}^{\alpha} = \frac{1}{8}\times\left[(q\ -\ 3)\ +\ 2(-1)^{\frac{q-1}{2}}\chi(\alpha)\left((-1)^{\frac{q^2-1}{8}}\ +\ 1\right)\ -\ (-1)^{\frac{q-1}{2}}-1\right]$$

$$N_{113}^{\alpha} = \frac{1}{8}\times\left\{(q\ -\ 4)\ +\ (-1)^{\frac{q-1}{2}}\left[2\chi(\alpha)\left((-1)^{\frac{q^2-1}{8}}+1\right)\ -\ 1\right]\right\} \tag{5.18}$$

Esta fórmula também pode ser escrita como:

$$N_{113}^{\alpha} = \begin{cases} \frac{q-1}{8}-\frac{1-\chi(\alpha)}{2}\ , & \text{if } q\equiv 1 \pmod 8 \\ \frac{q-3}{8}\ , & \text{if } q\equiv 3 \pmod 8 \\ \frac{q-5}{8}\ , & \text{if } q\equiv 5 \pmod 8 \\ \frac{q-7}{8}+\frac{1-\chi(\alpha)}{2}\ , & \text{if } q\equiv 7 \pmod 8 \end{cases} \tag{5.19}$$

5.2 Casos com "$\delta_t \neq 0$ é SQ e $t_1, t_2 \neq 0$" quando $\alpha = 0$

Se $\underline{\alpha = 0}$, alguns ajustes precisam ser feitos *antes que* as fórmulas finais sejam obtidas. Trata-se essencialmente das mesmas deduções feitas para $\alpha \neq 0$, mas as adaptações irão levar a um conjunto de expressões totalmente diferente de simplesmente fixar $\alpha = 0$ nas Eqs. 5.11, 5.14 e 5.19.

5.2.1 Caso "t_1 é SQ e t_2 é SQ" (fórmula para N_{141}^{0})

Neste caso, tanto $-\alpha/2$ como $-\alpha$ também são zero e a Eq. 5.1 assume a seguinte forma:

$$z_1^2 + z_2^2 = 0 \quad \text{em } \mathbb{F}_q\ , \qquad z_1^2 \neq 0 \quad \text{e} \quad z_2^2 \neq 0$$

A quantidade N^0_{141} depende do número de soluções para esta equação e pode ser computada por uma ligeira adaptação do que foi feto acima (para $\alpha \neq 0$):

$$8N^0_{141} = N(z_1^2 + z_2^2 = 0) \tag{5.20}$$

onde:

$$N(z_1^2 + z_2^2 = 0) = \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(\big(1+\chi(t_1)\big) \times \big(1+\chi(t_2)\big) \Big) \tag{5.21a}$$

$$= \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1+\chi(t_1)+\chi(t_2)+\chi(t_1)\chi(t_2) \Big) \tag{5.21b}$$

Então, uma vez que $\sum_{i\neq 0}\chi(i) = 0$, e uma vez que χ é um caracter quadrático, esta expressão pode ser reduzida a:

$$N(z_1^2 + z_2^2 = 0) = \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1+\chi(-1) \Big) \tag{5.22}$$

e o número de soluções para a Eq. 5.1, com $\alpha = 0$, é dado por:

$$N(z_1^2 + z_2^2 = 0) = \ (q-1) \ + \ (q-1).\chi(-1)$$

Agora, usando a Eq. 4.12, obtemos:

$$N(z_1^2 + z_2^2 = 0) = \ (q-1)\left(1+(-1)^{\frac{q-1}{2}}\right) \tag{5.23}$$

Então, usando a Eq. 5.20, obtemos:

$$N^0_{141} = \ \frac{(q-1)}{8}\left(1+(-1)^{\frac{q-1}{2}}\right) \tag{5.24}$$

Esta fórmula também pode ser escrita como:

$$N^0_{141} = \begin{cases} \frac{q-1}{4} \ , & \text{if } q \equiv 1 \pmod 4 \\ 0 \ , & \text{if } q \equiv 3 \pmod 4 \end{cases} \tag{5.25}$$

5.2.2 Caso "um t SQ, um t NS" (fórmula para N^0_{142})

Se $\underline{\alpha = 0}$, a Eq. 5.14 não é válida e alguns ajustes precisam ser feitos. Neste caso, tanto $-\alpha/2$ como $-\alpha$ são também zero e a Eq. 5.12 assume a seguinte forma:

$$8N^0_{142} = N(\ \overline{t_1} + t_2 = 0 \quad \text{or} \quad t_1 + \overline{t_2} = 0\ ) \tag{5.26}$$

onde, como antes, $\bar{t}$ indica que t é NS. Adaptando a Eq. 5.13 a esta nova situação, obtemos:

$$N^0_{142} = \frac{1}{8} \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(N(t_1 \neq z_1^2) \times N(t_2 = z_2^2) \ + \ N(t_1 = z_1^2) \times N(t_2 \neq z_2^2) \Big) \tag{5.27a}$$

$$= \ \frac{1}{8} \times 2 \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(N(t_1 = z_1^2) \times N(t_2 \neq z_2^2) \Big)$$

$$N^0_{142} = \ \frac{1}{4} \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(\big(1 + \chi(t_1)\big) \times \big(1 - \chi(t_2)\big) \Big) \tag{5.28a}$$

$$= \ \frac{1}{4} \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1 + \chi(t_1) - \chi(t_2) - \chi(t_1)\chi(t_2) \Big)$$

$$= \ \frac{1}{4} \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1 - \chi(-1) \Big)$$

$$= \ \frac{1}{4} \times (q-1) \Big(1 \ - \ \chi(-1) \Big)$$

Então, usando a Eq. 4.12, obtemos a seguinte fórmula:

$$N^0_{142} = \frac{1}{4} \times (q-1) \Big(1 - (-1)^{\frac{q-1}{2}} \Big) \tag{5.29}$$

a qual também pode ser escrita como:

$$N^0_{142} = \begin{cases} 0\ , & \text{if } q \equiv 1 \pmod 4 \\ \frac{q-1}{2}\ , & \text{if } q \equiv 3 \pmod 4 \end{cases} \tag{5.30}$$

5.2.3 Caso "t_1 é NS e t_2 é NS" (fórmula para N^0_{143})

Se $\underline{\alpha = 0}$, a Eq. 5.19 não pode ser diretamente aplicada, os valores $-\alpha/2$ e $-\alpha$ são ambos zero e a quantidade N^0_3 pode ser computada por uma ligeira adaptação do que foi feito acima (para $\alpha \neq 0$):

$$8N^0_{143} = N(\ \overline{t_1} + \overline{t_2} = 0\ ) \tag{5.31}$$

onde:

$$N(\ \overline{t_1} + \overline{t_2} = 0\ ) = \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(N(z_1^2 \neq t_1) \times N(z_2^2 \neq t_2) \Big)$$

$$\begin{aligned} N(\ \overline{t_1} + \overline{t_2} = 0\ ) &= \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(\big(1-\chi(t_1)\big) \times \big(1-\chi(t_2)\big) \Big) \qquad (5.32a) \\ &= \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1 - \chi(t_1) - \chi(t_2) + \chi(t_1)\chi(t_2) \Big) \end{aligned}$$

De modo similar à computação de N^0_{141}, obtemos:
onde:

$$\begin{aligned} N^0_{143} &= \frac{1}{8} \times \sum_{\substack{t_1+t_2=0 \\ t_1,t_2\neq 0}} \Big(1 + \chi(-1) \Big) \\ &= (q-1)\Big(1 \ + \ \chi(-1) \Big) \end{aligned}$$

Então, usando a Eq. 4.12, obtemos:

$$N^0_{143} = \ \frac{(q-1)}{8} \Big(1 + (-1)^{\frac{q-1}{2}} \Big) \tag{5.34}$$

Esta fórmula também pode ser escrita como:

$$N^0_{143} = \begin{cases} \frac{q-1}{4}\ , & \text{if } q \equiv 1 \pmod 4 \\ 0\ , & \text{if } q \equiv 3 \pmod 4 \end{cases} \tag{5.35}$$

5.3 Resumo para "$\delta_t \neq 0$ é SQ e $t_1, t_2 \neq 0$"

Este capítulo pode ser resumido nas tabelas 5.1 e 5.2. [1]

q mod 8	N^{α}_{111}	N^{α}_{112}	N^{α}_{113}
1	$\frac{q-9}{8} + \left(\frac{1-\chi(\alpha)}{2}\right)$	$\frac{q-1}{4}$	$\frac{q-1}{8} - \left(\frac{1-\chi(\alpha)}{2}\right)$
3	$\frac{q-3}{8}$	$\frac{q-3}{4}$	$\frac{q-3}{8}$
5	$\frac{q-5}{8}$	$\frac{q-1}{4}$	$\frac{q-5}{8}$
7	$\frac{q+1}{8} - \left(\frac{1-\chi(\alpha)}{2}\right)$	$\frac{q-3}{4}$	$\frac{q-7}{8} + \left(\frac{1-\chi(\alpha)}{2}\right)$

Table 5.1: Fórmulas para $\alpha \neq 0$.

q mod 8	N^{0}_{141}	N^{0}_{142}	N^{0}_{143}
1	$\frac{q-1}{4}$	0	$\frac{q-1}{4}$
3	0	$\frac{q-1}{2}$	0
5	$\frac{q-1}{4}$	0	$\frac{q-1}{4}$
7	0	$\frac{q-1}{2}$	0

Table 5.2: Fórmulas para $\alpha = 0$.

[1] Estas fórmulas foram verifcadas por meio da computação direta das raízes da Eq. 3.6, com o auxílio do pacote SAGE [33] (software livre), para $v \in \mathbb{Z}$, $1 \leq v \leq 50$, para tamanhos de corpo q incluindo todas as potências ímpares de primos menores do que 487 e com $q \equiv \pm 2 \pmod 5$.

Chapter 6

Prova do Teorema Principal - Parte 3

A seguir, obtemos fórmulas para a computação do espectro diferencial e, portanto, ambiguidade e deficiência para o polinômio $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$, em um corpo $\mathbb{F}_q$, com q podendo ser qualquer potência ímpar de primo ($q = p^n,\ p$ ímpar) e $q \equiv \pm 2 \pmod 5$.

Agora que sabemos como avaliar cada ramo mencionado na subseção 3.4, também podemos avaliar o vetor n_k^a para cada linha "a" da tabela $\lambda_{a,b}$, e para n_k^a como descrito na seção 2.1. Este vetor, também conhecido como "espectro diferencial da linha-a de $F_w(x)$", contém informação suficiente para que a "ambiguidade da linha-a" e a "deficiência da linha-a" sejam imediatamente computadas pelas definições correspndentes (ver seção 2.1). A partir dos valores da "linha-a", os valores completos (totalizados sobre todos os $a \in \mathbb{F}_q^*$) pode ser facilmente derivado.

6.1 Espectro, ambiguidade e deficiência da linha-a para $F_w(x)$

Note que estamos buscando expressões para o número de soluções para $F_w(x+1) - F_w(x) = b$ ($b \in \mathbb{F}_q$), que $\alpha = \frac{1}{2} + \frac{3w}{5a^2}$ e também que n_k^a é o número de b's na linha "a" de $\lambda_{a,b}$ que levam a exatamente k soluções diferentes para esta equação.

Então, a tabela 6.1 resume as fórmulas para computar o espectro diferencial da linha-a, n_k^a, quando $\underline{\alpha = 0}$ e a tabela 6.2 resume as fórmulas para computar n_k^a quando $\underline{\alpha \neq 0}$. [1]

Uma vez que temos as quantidades em cada linha a de $\lambda_{a,b}$ completamente caracterizadas (por n_k^a), uma simples aplicação das definições apresentadas na seção 2.1 leva às formulas para a ambiguidade da linha-a e para a deficiência da linha-a mostradas nas tabelas 6.3 e 6.4, para uma potência de primo q, com q ímpar e $q \equiv \pm 2 \pmod 5$.

[1] Como uma verificação simples, pode-se notar que, na tabela 6.1, para cada $q \bmod 4$, a soma total é igual a q, e, na tabela 6.2, para cada $q \bmod 8$, a soma total é igual a q.

$q \bmod 4$	n_0^a	n_1^a	n_2^a	n_3^a	n_4^a
1	$\frac{3(q-1)}{4}$	1	0	0	$\frac{q-1}{4}$
3	$\frac{q-1}{2}$	1	$\frac{q-1}{2}$	0	0

Table 6.1: Fórmulas para computar o espectro da linha-a quando $\alpha = 0$.

$q \bmod 8$	n_0^a	n_1^a	n_2^a	n_3^a	n_4^a
1	$\frac{5(q-1)}{8}$	$\frac{1-\chi(\alpha)}{2}$	$\frac{q-1}{4}+\left(\frac{1+\chi(\alpha)}{2}\right)$	$\frac{1+\chi(\alpha)}{2}$	$\frac{q-9}{8}+\left(\frac{1-\chi(\alpha)}{2}\right)$
3	$\frac{5q+1}{8}-\left(\frac{1+\chi(\alpha)}{2}\right)$	$\frac{1+\chi(\alpha)}{2}$	$\frac{q-3}{4}+\left(\frac{1+\chi(\alpha)}{2}\right)$	$\frac{1-\chi(\alpha)}{2}$	$\frac{q-3}{8}$
5	$\frac{5q-9}{8}+\left(\frac{1+\chi(\alpha)}{2}\right)$	$\frac{1-\chi(\alpha)}{2}$	$\frac{q-1}{4}+\left(\frac{1-\chi(\alpha)}{2}\right)$	$\frac{1+\chi(\alpha)}{2}$	$\frac{q-5}{8}$
7	$\frac{5q-3}{8}$	$\frac{1+\chi(\alpha)}{2}$	$\frac{q-3}{4}+\left(\frac{1-\chi(\alpha)}{2}\right)$	$\frac{1-\chi(\alpha)}{2}$	$\frac{q+1}{8}-\left(\frac{1-\chi(\alpha)}{2}\right)$

Table 6.2: Fórmulas para computar o espectro da linha-a quando $\alpha \neq 0$.

$q \bmod 4$	ambiguidade da linha-a		deficiência da linha-a
1	$\left[\frac{q-1}{4}\right] \times (6) + [0] \times (3) + [0] \times (1)$	$= \frac{3(q-1)}{2}$	$\frac{3(q-1)}{4}$
3	$[0] \times (6) + [0] \times (3) + \left[\frac{q-1}{2}\right] \times (1)$	$= \frac{q-1}{2}$	$\frac{q-1}{2}$

Table 6.3: Fórmulas para ambiguidade da linha-a e deficiência da linha-a quando $\alpha = 0$.

$q \bmod 8$	ambiguidade da linha-a		deficiência da linha-a
1	$\left[\frac{q-9}{8}+\frac{1-\chi(\alpha)}{2}\right](6)+\left[\frac{1+\chi(\alpha)}{2}\right](3)+\left[\frac{q-1}{4}+\frac{1+\chi(\alpha)}{2}\right](1)$	$= q-2-\chi(\alpha)$	$\frac{5(q-1)}{8}$
3	$\left[\frac{q-3}{8}\right](6)+\left[\frac{1-\chi(\alpha)}{2}\right](3)+\left[\frac{q-3}{4}+\frac{1+\chi(\alpha)}{2}\right](1)$	$= q-1-\chi(\alpha)$	$\frac{5q+1}{8}-\left(\frac{1+\chi(\alpha)}{2}\right)$
5	$\left[\frac{q-5}{8}\right](6)+\left[\frac{1+\chi(\alpha)}{2}\right](3)+\left[\frac{q-1}{4}+\frac{1-\chi(\alpha)}{2}\right](1)$	$= q-2+\chi(\alpha)$	$\frac{5q-9}{8}+\left(\frac{1+\chi(\alpha)}{2}\right)$
7	$\left[\frac{q+1}{8}-\frac{1-\chi(\alpha)}{2}\right](6)+\left[\frac{1-\chi(\alpha)}{2}\right](3)+\left[\frac{q-3}{4}+\frac{1-\chi(\alpha)}{2}\right](1)$	$= q-1+\chi(\alpha)$	$\frac{5q-3}{8}$

Table 6.4: Fórmulas para ambiguidade da linha-a e deficiência da linha-a quando $\alpha \neq 0$.

6.2 Espectro, ambiguidade e deficiência (totais) de $F_w(x)$

Uma vez que temos as expressões para computar espectro, ambiguidade e deficiência para cada linha a da matriz $\lambda_{a,b}$, os valores totais de espectro, ambiguidade e deficiência para $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$ são dados pela soma dos valores "de linha-a" sobre todas as linhas, como segue:

- Espectro de F_w:
$$n_k(F_w) = \sum_{a \in \mathbb{F}_q^*} n_k^a(F_w) \tag{6.1}$$

- Deficiência de F_w:
$$D(F_w) = \sum_{a \in \mathbb{F}_q^*} D_a(F_w) \tag{6.2}$$

- Ambiguidade de F_w:
$$A(F_w) = \sum_{a \in \mathbb{F}_q^*} A_a(F_w) \tag{6.3}$$

As expressões para espectro, ambiguidade e deficiência da linha-a dependem diretamente de α e indiretamente de a, já que, para um valor fixo de w, temos $\alpha = 1/2 + (3w)/(5a^2)$. Isto significa que, para cada linha a, as fórmulas fornecem valores diferentes e, especificamente, se o valor a da linha leva a $\alpha = 0$, os valores devem ser tomados de acordo com a tabela correspondente. Note que as fórmulas para $\alpha = 0$ serão usadas apenas se este caso ocorrer. Para que o caso $\alpha = 0$ ocorra, o seguinte valor não pode ser zero (senão, $\alpha = 1/2 + (3w)/(5a^2)$ nunca poderia ser zero) e deve ser um square no corpo:

$$a^2 = -\frac{6w}{5}$$

E este valor será um square dependendo de cada corpo $\mathbb{F}_q$. Desta forma, haverá dois tipos de fórmulas para os valores totais (ou seja, sobre todos os $a \in \mathbb{F}_q^*$) de espectro, ambiguidade e deficiência, dependendo de se $\alpha = 0$ aparece.

6.2.1 Caso 1: $-6w/5$ é zero ou não é um square em $\mathbb{F}_q^*$

Neste caso, $\alpha = 0$ não aparece, as somas nas Eqs. 6.1, 6.2 e 6.3 são apenas sobre as expressões das tabelas 6.2 e 6.4, e obtemos as fórmulas para $n_k(F_w)$, $A(F_w)$ e $D(F_w)$ mostradas nas tabelas 6.5 [2] e 6.6, com o valor de S dado pela tabela 6.9.

Note que, porque os valores "de linha-a" dependem, evidentemente, de a, os resultados "totais" dependerão de uma soma de caracteres especial, dada por

[2] Como uma verificação simples, pode-se notar que, na tabela 6.5, para cada $q \bmod 8$, a soma total é igual a $q \times (q-1)$.

$q \bmod 8$	n_0	n_1	n_2	n_3	n_4
1	$\frac{(q-1)(5q-5)}{8}$	$\frac{q-1}{2}-\frac{S}{2}$	$\frac{(q-1)(q+1)}{4}+\frac{S}{2}$	$\frac{q-1}{2}+\frac{S}{2}$	$\frac{(q-1)(q-5)}{8}-\frac{S}{2}$
3	$\frac{(q-1)(5q-3)}{8}-\frac{S}{2}$	$\frac{q-1}{2}+\frac{S}{2}$	$\frac{(q-1)(q-1)}{4}+\frac{S}{2}$	$\frac{q-1}{2}-\frac{S}{2}$	$\frac{(q-1)(q-3)}{8}$
5	$\frac{(q-1)(5q-5)}{8}+\frac{S}{2}$	$\frac{q-1}{2}-\frac{S}{2}$	$\frac{(q-1)(q+1)}{4}-\frac{S}{2}$	$\frac{q-1}{2}+\frac{S}{2}$	$\frac{(q-1)(q-5)}{8}$
7	$\frac{(q-1)(5q-3)}{8}$	$\frac{q-1}{2}+\frac{S}{2}$	$\frac{(q-1)(q-1)}{4}-\frac{S}{2}$	$\frac{q-1}{2}-\frac{S}{2}$	$\frac{(q-1)(q-3)}{8}+\frac{S}{2}$

Table 6.5: Fórmulas para computar o espectro total $n_k(F_w)$ quando $\alpha \neq 0$.

$q \bmod 8$	Ambiguidade	Deficiência
1	$(q-1)(q-2)-S$	$\frac{(q-1)(5q-5)}{8}$
3	$(q-1)(q-1)-S$	$\frac{(q-1)(5q-3)}{8}-\frac{S}{2}$
5	$(q-1)(q-2)+S$	$\frac{(q-1)(5q-5)}{8}+\frac{S}{2}$
7	$(q-1)(q-1)+S$	$\frac{(q-1)(5q-3)}{8}$

Table 6.6: Formulas para $A(F_w)$ e $D(F_w)$ quando o caso "$\alpha = 0$" does not happen.

$$S = \sum_{a \in \mathbb{F}_q^*} \chi(\alpha) = \sum_{a \in \mathbb{F}_q^*} \chi\left(\frac{1}{2} + \frac{3w}{5a^2}\right) \tag{6.4}$$

Esta soma pode ser dada em forma fechada, como uma função simples de $\chi(\frac{1}{2})$ e $\chi(\frac{3w}{5})$ (ver seção 6.3 abaixo).

6.2.2 Case 2: $-6w/5$ é não zero e é um square em $\mathbb{F}_q^*$

Neste caso, $\alpha = 0$ efetivamente aparece e os valores dados pelas tabelas 6.1 e 6.3 devem ser adicionados exatamente duas vezes (para os dois valores de a que levam a a^2) à soma das expressões mostrada nas tabelas 6.2 e 6.4 (executadas sobre os $q-3$ valores restantes de a) e obtemos as formulas apresentadas abaixo.

Note que S é definido na Eq. 6.4 e que, uma vez que $\chi(0) = 0$, devemos ter:

$$\sum_{\substack{a \in \mathbb{F}_q^* \\ a^2 \neq -\frac{6w}{5}}} \chi(\alpha) = \sum_{a \in \mathbb{F}_q^*} \chi(\alpha) = S$$

- caso $q \equiv 1 \pmod 8$:

– Espectro diferencial:

$$n_0(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \frac{5(q-1)}{8} + 2\times\frac{3(q-1)}{4}$$
$$= (q-3)\times\frac{5(q-1)}{8} + \frac{3(q-1)}{2} \;=\; (q-1)\times\frac{(5q-3)}{8}$$

$$n_1(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1-\chi(\alpha)}{2}\right) + 2\times 1$$
$$= \frac{(q-3)}{2} - \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{\chi(\alpha)}{2}\right) + 2 \;=\; \frac{(q+1)}{2} - \frac{S}{2}$$

$$n_2(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q-1}{4} + \frac{1+\chi(\alpha)}{2}\right) + 2\times 0$$
$$= (q-3)\times\frac{(q+1)}{4} + \frac{1}{2}\times \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \chi(\alpha) \;=\; (q-3)\times\frac{(q+1)}{4} + \frac{S}{2}$$

$$n_3(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1+\chi(\alpha)}{2}\right) + 2\times 0 \;=\; \frac{(q-3)}{2} + \frac{S}{2}$$

$$n_4(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q-9}{8} + \frac{1-\chi(\alpha)}{2}\right) + 2\times\frac{(q-1)}{4}$$
$$= (q-3)\times\frac{(q-5)}{8} - \frac{S}{2} + \frac{q-1}{2}$$

– Ambiguidade:

$$A(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \big(q-2-\chi(\alpha)\big) + 2\times\frac{3(q-1)}{2} \;=\; (q-3)(q-2) - S + 3(q-1)$$

– Deficiência:

$$D(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5(q-1)}{8}\right) + 2\times\frac{3(q-1)}{4} = \frac{(q-3)5(q-1)}{8} + \frac{3(q-1)}{2} = \frac{(q-1)(5q-3)}{8}$$

- caso $q \equiv 3 \pmod 8$:

  – Espectro diferencial:

$$n_0(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5q+1}{8} - \frac{1+\chi(\alpha)}{2}\right) + 2\times\frac{(q-1)}{2} = (q-3)\times\frac{(5q-3)}{8} - \frac{S}{2} + (q-1)$$

$$n_1(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1+\chi(\alpha)}{2}\right) + 2\times 1 = \frac{(q+1)}{2} + \frac{S}{2}$$

$$n_2(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q-3}{4} + \frac{1+\chi(\alpha)}{2}\right) + 2\times\frac{(q-1)}{2}$$

$$= (q-3)\times\frac{(q-1)}{4} + \frac{S}{2} + (q-1) = (q-1)\times\frac{(q+1)}{4} + \frac{S}{2}$$

$$n_3(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1-\chi(\alpha)}{2}\right) + 2\times 0 = \frac{(q-3)}{2} - \frac{S}{2}$$

$$n_4(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \frac{(q-3)}{8} + 2\times 0 = (q-3)\times\frac{(q-3)}{8}$$

  – Ambiguidade:

$$A(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \big(q-1-\chi(\alpha)\big) + 2\times\frac{(q-1)}{2}$$
$$= (q-3)(q-1) - \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \chi(\alpha) + (q-1) \;=\; (q-2)(q-1) - S$$

– Deficiência:

$$D(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5q+1}{8} - \frac{1+\chi(\alpha)}{2}\right) + 2\times\frac{q-1}{2}$$
$$= \frac{(q-3)(5q+1)}{8} - \frac{(q-3)}{2} - \frac{S}{2} + (q-1) \;=\; \frac{(5q^2-10q+1)}{8} - \frac{S}{2}$$

- caso $q \equiv 5 \pmod 8$:

– Espectro diferencial:

$$n_0(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5q-9}{8} + \frac{1+\chi(\alpha)}{2}\right) + 2\times\frac{3(q-1)}{4} \;=\; (q-1)\times\frac{(5q-3)}{8} + \frac{S}{2}$$

$$n_1(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1-\chi(\alpha)}{2}\right) + 2\times 1 \;=\; \frac{(q+1)}{2} - \frac{S}{2}$$

$$n_2(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q-1}{4} + \frac{1-\chi(\alpha)}{2}\right) + 2\times 0 \;=\; (q-3)\times\frac{(q+1)}{4} - \frac{S}{2}$$

$$n_3(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1+\chi(\alpha)}{2}\right) + 2\times 0 \;=\; \frac{(q-3)}{2} + \frac{S}{2}$$

$$n_4(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \frac{(q-5)}{8} + 2\times\frac{(q-1)}{4} \;=\; (q-3)\times\frac{(q-5)}{8} + \frac{q-1}{2}$$

– Ambiguidade:

$$A(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \big(q-2+\chi(\alpha)\big) + 2\times\frac{3(q-1)}{2}$$
$$= (q-3)(q-2) + 3(q-1) + \sum_{a\in\mathbb{F}_q^*}\chi(\alpha)$$

– Deficiência:

$$D(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5q-9}{8} + \frac{1+\chi(\alpha)}{2}\right) + 2\times\frac{3(q-1)}{4}$$
$$= \frac{(q-3)(5q-9)}{8} + \frac{(q-3)}{2} + \frac{S}{2} + \frac{3(q-1)}{2} \;=\; \frac{(5q^2-8q+3)}{8} + \frac{S}{2}$$

• caso $q \equiv 7 \pmod 8$:

– Espectro diferencial:

$$n_0(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \frac{(5q-3)}{8} + 2\times\frac{(q-1)}{2} \;=\; (q-3)\times\frac{(5q-3)}{8} + (q-1)$$

$$n_1(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1+\chi(\alpha)}{2}\right) + 2\times 1 \;=\; \frac{(q-3)}{2} + \frac{S}{2} + 2 \;=\; \frac{(q+1)}{2} + \frac{S}{2}$$

$$n_2(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q-3}{4} + \frac{1-\chi(\alpha)}{2}\right) + 2\times\frac{(q-1)}{2}$$
$$= (q-3)\times\frac{(q-1)}{4} - \frac{S}{2} + (q-1) \;=\; (q-1)\times\frac{(q+1)}{4} - \frac{S}{2}$$

$$n_3(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{1-\chi(\alpha)}{2}\right) + 2\times 0 \;=\; \frac{(q-3)}{2} - \frac{S}{2}$$

$$n_4(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{q+1}{8} - \frac{1-\chi(\alpha)}{2}\right) + 2\times 0$$
$$= (q-3)\times\frac{(q-3)}{8} + \frac{S}{2}$$

– Ambiguidade:

$$A(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \big(q-1+\chi(\alpha)\big) + 2\times\frac{(q-1)}{2}$$
$$= (q-2)(q-1) + \sum_{a\in\mathbb{F}_q^*}\chi(\alpha)$$

– Deficiência:

$$D(F_w) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a^2\neq -\frac{6w}{5}}} \left(\frac{5q-3}{8}\right) + 2\times\frac{(q-1)}{2}$$
$$= \frac{(q-3)(5q-3)}{8} + (q-1) = \frac{5q^2-10q+1}{8}$$

As tabelas 6.7 e 6.8 resumem os resultados para os casos em que $\alpha = 0$ ocorre (ou seja, quando "$-6w/5$ é não-zero e é um square em $\mathbb{F}_q^*$ ").

q mod 8	n_0	n_1	n_2	n_3	n_4
1	$\frac{(q-1)(5q-3)}{8}$	$\frac{q+1}{2}-\frac{S}{2}$	$\frac{(q-3)(q+1)}{4}+\frac{S}{2}$	$\frac{q-3}{2}+\frac{S}{2}$	$\frac{(q-3)(q-5)}{8}+\frac{q-1}{2}-\frac{S}{2}$
3	$\frac{(q-3)(5q-3)}{8}+(q-1)-\frac{S}{2}$	$\frac{q+1}{2}+\frac{S}{2}$	$\frac{(q-1)(q+1)}{4}+\frac{S}{2}$	$\frac{q-3}{2}-\frac{S}{2}$	$\frac{(q-3)(q-3)}{8}$
5	$\frac{(q-1)(5q-3)}{8}+\frac{S}{2}$	$\frac{q+1}{2}-\frac{S}{2}$	$\frac{(q-3)(q+1)}{4}-\frac{S}{2}$	$\frac{q-3}{2}+\frac{S}{2}$	$\frac{(q-3)(q-5)}{8}+\frac{q-1}{2}$
7	$\frac{(q-3)(5q-3)}{8}+(q-1)$	$\frac{q+1}{2}+\frac{S}{2}$	$\frac{(q-1)(q+1)}{4}-\frac{S}{2}$	$\frac{q-3}{2}-\frac{S}{2}$	$\frac{(q-3)(q-3)}{8}+\frac{S}{2}$

Table 6.7: Fórmulas para computar o espectro total quando o caso "$\alpha = 0$" ocorre.

Como uma verificação simples, pode-se notar que, na tabela 6.7, para cada q mod 8, a soma total é igual a $q\times(q-1)$. Os valores produzidos pelas expressões listadas nas tabelas 6.6 e 6.8 foram comparados com valores experimentais obtidos com SAGE [33] a partir das definições (diretamente as matrizes Δ e λ). Os resultados bateram para $w\in\mathbb{Z},\ 1\leq w\leq 50$,

q mod 8	Ambiguidade	Deficiência
1	$(q-3)(q-2)+3(q-1)-S$	$\frac{(q-1)(5q-3)}{8}$
3	$(q-1)(q-2)-S$	$\frac{(q-3)(5q-3)}{8}+(q-1)-\frac{S}{2}$
5	$(q-3)(q-2)+3(q-1)+S$	$\frac{(q-1)(5q-3)}{8}+\frac{S}{2}$
7	$(q-1)(q-2)+S$	$\frac{(q-3)(5q-3)}{8}+(q-1)$

Table 6.8: Fórmulas para $A(F_w)$ e $D(F_w)$ quando o caso "$\alpha = 0$" ocorre.

e para tamanhos de corpo q incluindo todas as potências ímpares de primos menores do que 487, tais que $q \equiv \pm 2 \pmod 5$.

6.3 Computando $\sum_{a\in\mathbb{F}_q^*} \chi(\alpha)$

Conforme discussão na seção 4.5, para um dado $\mathbb{F}_q$, o valor deste tipo de soma:

$$\sum_{x\in\mathbb{F}_q^*} \chi\left(A+Bx^2\right)$$

depende apenas de q e pode ser diretamente determinado, tão logo os valores de $\chi(A)$ e $\chi(B)$ estejam disponíveis.

Desta forma, de acordo com a tabela 4.4, o valor de:

$$S = \sum_{a\in\mathbb{F}_q^*} \chi(\alpha) = \sum_{a\in\mathbb{F}_q^*} \chi\left(\frac{1}{2}+\frac{3w}{5a^2}\right)$$

pode ser computado por simples inspeção na tabela 6.9, depois de computar, em $\mathbb{F}_q$, os valores de:

$$\chi(\tfrac{1}{2}) = \chi(2) = (-1)^{\frac{q^2-1}{8}} \qquad \text{e} \qquad \chi(\tfrac{3w}{5})$$

	$\chi(\frac{1}{2})$	
	$+1$	-1
$\chi(\frac{3w}{5})$		
$+1$	-2	0
0	$q-1$	$-(q-1)$
-1	0	2

Table 6.9: Valores de S em $\mathbb{F}_q$.

6.4 Resumo das fórmulas

Esta seção resume os resultados obtidos neste capítulo.

A ambiguidade e a deficiência de:

$$F_w(x) = x^5 + wx^3 + 5^{-1}w^2x$$

em um corpo $\mathbb{F}_q$, com q sendo qualquer potência ímpar de primo, $q \equiv \pm 2 \pmod 5$, e $w \in \mathbb{Z}$ qualquer, pode ser obtida pela seguinte sequência de operações:

1. Compute $\chi(\frac{1}{2}) = (-1)^{\frac{q^2-1}{8}}$
2. Compute $\chi(\frac{3w}{5})$ em $\mathbb{F}_q$
3. Busque o valor de S na tabela 6.9
4. Compute $\gamma = -\frac{6w}{5}$ em $\mathbb{F}_q$
5. Compute $q \bmod 8$
6. Se $\gamma = 0$ ou γ é NS em $\mathbb{F}_q^*$:

   obtenha ambiguidade e deficiência da tabela 6.6
7. Se $\gamma \neq 0$ e γ é SQ em $\mathbb{F}_q^*$:

   obtenha ambiguidade e deficiência da tabela 6.8

Chapter 7

Artigo submetido a revista

O Teorema Principal, cuja prova está detalhada nos capítulos 3 a 6, consiste no elemento fundamental para a completa caracterização diferencial de todos os polinômios de permutação de baixo grau (grau menor ou igual a 6) sobre corpos finitos. Com efeito, esta caracterização só não havia sido feita ainda porque a referida prova ainda não havia aparecido.

Com o Teorema Principal provado, os casos mais difíceis na lista completa de polinômios de permutação de baixo grau sobre corpos finitos (ver [9, Section 7.1] e [28]) puderam ser caracterizados do ponto de vista diferencial. Os demais casos são simples aplicações de resultados conhecidos ou então envolvem somente computações numéricas.

O resultado deste estudo foi compilado em um artigo que foi publicado na revista "Finite Fields and their Applications", classificado como A2 pela CAPES:

- D. Panario, D. Santana, Q. Wang, "Ambiguidade, Deficiência e espectro diferencial de normalizado permutação polinômios over Finite Fields", "Finite Fields and Their Applications", 2017.

Part II

Ambiguidade e deficiência de permutações sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$

Nesta segunda parte, o trabalho passou a lidar com anéis sobre inteiros do tipo $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$, por razões que serão discutidas posteriormente. Nos capítulos a seguir, são discutidos os fundamentos teóricos e computacionais que podem auxiliar uma busca de permutações APN sobre estes domínios sem passar por todas as possibilidades, ou seja, sem fazer uma busca exaustiva.

O principal fundamento são os *automorfismos de grupo* e as relações de equivalência afins que deles são derivadas (Afins estendidas ou EA). Também possuem um papel muito importante relações de equivalência que consistem em uma espécie de "generalização" destas relações afins, as relações de equivalência de Carlet-Charpin-Zinoviev (CCZ). As classes CCZ são estritamente maiores do que as classes EA e as englobam perfeitamente, ou seja, todo par de permutações que é EA equivalente também é CCZ equivalente (mas o contrário não pode ser afirmado).

Estas relações parecem promissores auxiliares na busca por permutações APNs em um grupo abeliano finito, pois dividem o domínio de busca em grandes classes de equivalência cujos componentes apresentam o mesmo perfil diferencial, ou seja, o *espectro diferencial é invariante sob estas relações*. Desta forma, na busca de uma permutação sobre um grupo abeliano com ambiguidade e deficiência ótimas (mínimas), seria necessário, em tese, apenas focar nos representantes das classes, os quais são em número muito menor do que o tamanho total do domínio de busca. Na prática, porém, não foi possível chegar a nenhuma relação entre os representantes que permitisse lidar apenas com eles e que permitisse, apenas trabalhando com classes (e não com todas as permutações individualmente), chegar a alguma permutação da classe que contém as permutações de ambiguidade e deficiência ótimas.

Então, após várias tentativas infrutíferas de identificar uma "aritmética" entre os representantes das classes, este trabalho passou a focar em buscas heurísticas, descritas no capítulo 10, em uma tentativa de obter uma permutação APN em um domínio suficientemente grande (no caso, $\mathbb{Z}_2 \times \mathbb{Z}_{2^5}$) e com isto inferir propriedades que pudessem ser generalizadas e posteriormente provadas.

No final, foi com as buscas heurísticas que os melhores resultados foram obtidos, chegando-se a uma permutação 3-uniforme sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^5}$ muito próxima de uma APN (2-uniforme).

Esta parte do trabalho vai continuar sendo desenvolvida como um projeto de pesquisa em 2017. Acredita-se que ainda existe a possibilidade de, por meio de um aperfeiçoamento adequado das buscas heurísticas, obter uma permutação APN sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^5}$. Além disto, acredita-se que é necessário explorar melhor a "aritmética CCZ", a qual pode funcionar com um "atalho" para chegar a uma permutação com ambiguidade e deficiência ótimas e, portanto, APN.

Chapter 8

Equivalências EA e CCZ

Neste capítulo, são apresentadas algumas relações de equivalência que possuem um grande potencial de diminuir o esforço computacional na busca por permutações APN:

- A relação de equivalência Afim-Estendida ("Extended-Affine" ou EA): baseada no fato de que os automorfismos de grupo preservam as características diferenciais de uma permutação;
- A relação de equivalência de Carlet-Charpin-Zinoviev (CCZ): baseada no fato de que faz sentido considerar transformações lineares agindo simultaneamente nas variáveis independente e dependente de uma permutação.

As propriedades diferenciais de uma permutação são invariantes sob estas relações. Desta forma, a tarefa de buscar uma permutação com ambiguidade mínima (por exemplo) fica, em tese, reduzida à tarefa de encontrar qualquer permutação da (grande) classe específica das permutações com ambiguidade mínima.

8.1 Isomorfismos lineares e afins em funções booleanas

"Whatever you have to do with a structure-endowed entity Σ, try to determine its group of automorphisms. You can expect to gain a deep insight into the constitution of Σ in this way." Hermann Weyl, Symmetry

Certas propriedades diferenciais de funções booleanas definidas sobre $\mathbb{F}_2^n$ são invariantes sob a aplicação de isomorfismos afins às suas componentes. Do ponto de vista destas propriedades, portanto, estes isomorfismos afins levam a um agrupamento destas funções em classes de funções "linearmente semelhantes". Estas classes normalmente são muito grandes e interessam particularmente na busca de funções booleanas sobre $\mathbb{F}_2^n$ com características específicas de uniformidade diferencial, como é o caso das permutações APN. Estes isomorfismos podem ser produzidos por operações lineares matriciais ou por composição com o grupo de automorfismos associado ao anel subjacente.

A seguir são definidos estes isomorfismos no caso das funções booleanas, conforme discussão em [15], a fim de ressaltar a grande importância do grupo de automorfismos na busca por permutações APN em anéis do tipo $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$.

Seja f uma função booleana sobre $\mathbb{F}_2^n$ e seja L um isomorfismo afim de dimensão n, ou seja:

$$L(x) = Mx + a$$

onde M é uma matriz $n \times n$ não-singular e a é um vetor em $\mathbb{F}_2^n$.

Definição 12. *[15] Duas funções booleanas f, g sobre $\mathbb{F}_2^n$ são chamadas de equivalentes afins se existe um isomorfismo afim $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $L(x) = Mx + a$, tal que $f \circ L = g$. Se o vetor $a = \mathbf{0}$, então f e g são chamados de linearmente equivalentes.*

De acordo com [15], uma vez que L^{-1} também é um isomorfismo afim, é fácil ver que isto define uma relação de equivalência.

O interessante desta definição é que algumas propriedades importantes para a criptografia, tais como a não-linearidade e o grau algébrico, são invariantes sob esta transformação afim. Mas, mais importante, é que quando passamos para funções booleanas vetoriais, como as usadas nas caixas-S, notamos que esta transformação preserva os seus perfis diferenciais. Este ponto, importantíssimo para o objetivo deste trabalho, é discutido nas seções a seguir.

8.2 Equivalência "Extended-Affine" (EA)

Agora vamos estender a relação de equivalência descrita na seção anterior para funções vetoriais booleanas. Os conceitos e discussões apresentados a seguir também foram extraídos de [15].

Uma vez que uma (m, m)-função booleana vetorial F mapeia de $\mathbb{F}_2^m$ para $\mathbb{F}_2^m$, podemos compor F à direita e à esquerda com uma permutação afim.

Definição 13. *[15] Sejam F, G duas (m, m)-funções e sejam $A, A_1, A_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ tais que A é uma função afim e A_1 e A_2 são permutações afins quaisquer. As duas funções F e G são chamadas de "EA" equivalentes ("Afim Estendido") se*

$$G = A_1 \circ F \circ A_2 + A$$

Se $A = 0$, chamamos F e G de equivalentes afins.

A prova de que esta operação de fato define uma relação de equivalência entre F e G pode ser encontrada em [15].

De um ponto de vista prático, no caso dos anéis que são o escopo do presente trabalho, A, A_1 e A_2 são dados pelos automorfismos de grupo associados aos grupos aditivos respectivos. Estes automorfismos são conhecidos e, para os anéis de interesse, estão resumidos na tabela 8.1.

Anel	Automorfismos
$\mathbb{Z}_2 \times \mathbb{Z}_4$	[0 1 2 3 4 5 6 7], [0 3 2 1 4 7 6 5], [0 1 2 3 6 7 4 5], [0 3 2 1 6 5 4 7], [0 5 2 7 4 1 6 3], [0 7 2 5 4 3 6 1], [0 5 2 7 6 3 4 1], [0 7 2 5 6 1 4 3]
$\mathbb{Z}_2 \times \mathbb{Z}_8$	[0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15], [0 3 6 1 4 7 2 5 8 11 14 9 12 15 10 13], [0 5 2 7 4 1 6 3 8 13 10 15 12 9 14 11], [0 7 6 5 4 3 2 1 8 15 14 13 12 11 10 9], [0 1 2 3 4 5 6 7 12 13 14 15 8 9 10 11], [0 3 6 1 4 7 2 5 12 15 10 13 8 11 14 9], [0 5 2 7 4 1 6 3 12 9 14 11 8 13 10 15], [0 7 6 5 4 3 2 1 12 11 10 9 8 15 14 13], [0 9 2 11 4 13 6 15 8 1 10 3 12 5 14 7], [0 11 6 9 4 15 2 13 8 3 14 1 12 7 10 5], [0 13 2 15 4 9 6 11 8 5 10 7 12 1 14 3], [0 15 6 13 4 11 2 9 8 7 14 5 12 3 10 1], [0 9 2 11 4 13 6 15 12 5 14 7 8 1 10 3], [0 11 6 9 4 15 2 13 12 7 10 5 8 3 14 1], [0 13 2 15 4 9 6 11 12 1 14 3 8 5 10 7], [0 15 6 13 4 11 2 9 12 3 10 1 8 7 14 5]
$\mathbb{Z}_2 \times \mathbb{Z}_{16}$	[0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31], [0 5 10 15 4 9 14 3 8 13 2 7 12 1 6 11 16 21 26 31 20 25 30 19 24 29 18 23 28 17 22 27], [0 9 2 11 4 13 6 15 8 1 10 3 12 5 14 7 16 25 18 27 20 29 22 31 24 17 26 19 28 21 30 23], [0 13 10 7 4 1 14 11 8 5 2 15 12 9 6 3 16 29 26 23 20 17 30 27 24 21 18 31 28 25 22 19], [0 17 2 19 4 21 6 23 8 25 10 27 12 29 14 31 16 1 18 3 20 5 22 7 24 9 26 11 28 13 30 15], [0 21 10 31 4 25 14 19 8 29 2 23 12 17 6 27 16 5 26 15 20 9 30 3 24 13 18 7 28 1 22 11], [0 25 2 27 4 29 6 31 8 17 10 19 12 21 14 23 16 9 18 11 20 13 22 15 24 1 26 3 28 5 30 7], [0 29 10 23 4 17 14 27 8 21 2 31 12 25 6 19 16 13 26 7 20 1 30 11 24 5 18 15 28 9 22 3], [0 3 6 9 12 15 2 5 8 11 14 1 4 7 10 13 16 19 22 25 28 31 18 21 24 27 30 17 20 23 26 29], [0 7 14 5 12 3 10 1 8 15 6 13 4 11 2 9 16 23 30 21 28 19 26 17 24 31 22 29 20 27 18 25], [0 11 6 1 12 7 2 13 8 3 14 9 4 15 10 5 16 27 22 17 28 23 18 29 24 19 30 25 20 31 26 21], [0 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 16 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17], [0 19 6 25 12 31 2 21 8 27 14 17 4 23 10 29 16 3 22 9 28 15 18 5 24 11 30 1 20 7 26 13], [0 23 14 21 12 19 10 17 8 31 6 29 4 27 2 25 16 7 30 5 28 3 26 1 24 15 22 13 20 11 18 9], [0 27 6 17 12 23 2 29 8 19 14 25 4 31 10 21 16 11 22 1 28 7 18 13 24 3 30 9 20 15 26 5], [0 31 14 29 12 27 10 25 8 23 6 21 4 19 2 17 16 15 30 13 28 11 26 9 24 7 22 5 20 3 18 1], [0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 24 25 26 27 28 29 30 31 16 17 18 19 20 21 22 23], [0 5 10 15 4 9 14 3 8 13 2 7 12 1 6 11 24 29 18 23 28 17 22 27 16 21 26 31 20 25 30 19], [0 9 2 11 4 13 6 15 8 1 10 3 12 5 14 7 24 17 26 19 28 21 30 23 16 25 18 27 20 29 22 31], [0 13 10 7 4 1 14 11 8 5 2 15 12 9 6 3 24 21 18 31 28 25 22 19 16 29 26 23 20 17 30 27], [0 17 2 19 4 21 6 23 8 25 10 27 12 29 14 31 24 9 26 11 28 13 30 15 16 1 18 3 20 5 22 7], [0 21 10 31 4 25 14 19 8 29 2 23 12 17 6 27 24 13 18 7 28 1 22 11 16 5 26 15 20 9 30 3], [0 25 2 27 4 29 6 31 8 17 10 19 12 21 14 23 24 1 26 3 28 5 30 7 16 9 18 11 20 13 22 15], [0 29 10 23 4 17 14 27 8 21 2 31 12 25 6 19 24 5 18 15 28 9 22 3 16 13 26 7 20 1 30 11], [0 3 6 9 12 15 2 5 8 11 14 1 4 7 10 13 24 27 30 17 20 23 26 29 16 19 22 25 28 31 18 21], [0 7 14 5 12 3 10 1 8 15 6 13 4 11 2 9 24 31 22 29 20 27 18 25 16 23 30 21 28 19 26 17], [0 11 6 1 12 7 2 13 8 3 14 9 4 15 10 5 24 19 30 25 20 31 26 21 16 27 22 17 28 23 18 29], [0 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19 18 17 16 31 30 29 28 27 26 25], [0 19 6 25 12 31 2 21 8 27 14 17 4 23 10 29 24 11 30 1 20 7 26 13 16 3 22 9 28 15 18 5], [0 23 14 21 12 19 10 17 8 31 6 29 4 27 2 25 24 15 22 13 20 11 18 9 16 7 30 5 28 3 26 1], [0 27 6 17 12 23 2 29 8 19 14 25 4 31 10 21 24 3 30 9 20 15 26 5 16 11 22 1 28 7 18 13], [0 31 14 29 12 27 10 25 8 23 6 21 4 19 2 17 24 7 22 5 20 3 18 1 16 15 30 13 28 11 26 9]

Table 8.1: Automorfismos para alguns anéis do tipo $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$.

Em resumo, após a aplicação de qualquer automorfismo a uma permutação definida sobre um anel, o perfil diferencial (incluindo o espectro diferencial, a ambiguidade e a deficiência) não se altera. Em outras palavras, pode-se procurar por uma permutação APN nos anéis $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$ "a menos dos respectivos automorfismos".

Um outro modo de descrever o efeito destes automorfismos é que, ao se identificar uma permutação com certas características diferenciais, automaticamente obtemos diversas outras permutações (a quantidade depende do tamanho do grupo de automorfismos) com as mesmas características. Esta observação justifica a utilização dos automorfismos na otimização da busca descrita nos capítulos a seguir.

8.3 Equivalência "Carlet-Charpin-Zinoviev" (CCZ)

Ainda segundo [15], existe uma noção mais geral de equivalência entre funções booleanas, definida por Carlet, Charpin e Zinoviev em [17], chamada de equivalência CCZ.

Definimos o *grafo* de uma função (m, m) como:

$$G_F := \{(x, F(x)) : x \in \mathbb{F}_2^m\}$$

Definição 14. *[15] Sejam F, F' duas funções (m, m) e seja $\mathcal{L}$ uma permutação linear sobre $\mathbb{F}_2^{2m}$. As funções F e F' são chamadas de CCZ-equivalentes se*

$$\mathcal{L}(G_F) = G_{F'}$$

A noção de CCZ-equivalência é estritamente mais geral do que a noção de EA-equivalência. Todo par de funções EA-equivalentes também é CCZ-equivalente, mas o contrário não é verdadeiro, em geral. Por exemplo, conforme mostrado em [15], uma função F é CCZ-equivalente à sua inversa. No entanto, em geral, F e F^{-1} não são EA-equivalentes.

A importância deste conceito para o presente estudo é evidenciada pela proposição 5 e pelo corolário 2 apresentados a seguir.

Antes, note que podemos reescrever a definição de função APN (definição 1) do modo mostrado no lema a seguir.

Lema 1. *([15, Lemma 5.17]) Seja F uma função (m, m). Então F é APN se e somente se o sistema de equações dado por*

$$\begin{cases} x + y & = a \\ F(x) + F(y) & = b \end{cases}$$

admite no máximo duas soluções para todo $a, b \in \mathbb{F}_2^m$, $a \neq 0$.

Proof. Isto segue imediatamente, já que podemos substituir y por $x + a$. □

Proposição 5. *([15, Proposition 5.25]) O espectro diferencial é CCZ-invariante.*

Proof. Sejam F e F' duas funções (m, m) que são CCZ-invariantes, com $\mathcal{L}(G_F) = G_{F'}$. Sejam $a, b \in \mathbb{F}_2^m$, $a \neq \mathbf{0}$, pelo lemma 1 temos

$$\begin{aligned}\delta_{F'}(a,b) &= |\{F'(x) + F'(x+a) = b\}| = |\{(x, F'(x)) + (y, F'(y)) = (a,b)\}| \\ &= |\{\mathcal{L}(x, F(x)) + \mathcal{L}(y, F(y)) = (a,b)\}| \\ &= |\{(x, F(x)) + (y, F(y)) = \mathcal{L}^{-1}(a,b)\}| = \delta_F(\mathcal{L}^{-1}(a,b))\end{aligned}$$

Uma vez que $\mathcal{L}$ é uma permutação, $\mathcal{L}^{-1}$ também é permutação e os espectros diferenciais de Δ_F e $\Delta_{F'}$ são iguais a menos de uma permutação. Portanto, o espectro diferencial é CCZ-invariante. □

Corolário 2. *([15, Corollary 5.26]) A propriedade APN é CCZ-invariante.*

Chapter 9

Permutações APN sobre $\mathbb{Z}_n$

Para se adaptar aos hardwares mais comuns, os principais algoritmos criptográficos foram projetados para trabalhar sobre o corpo finito $\mathbb{F}_{2^n}$. Um valor de n muito importante é $n = 8$, pois está associado à noção de um byte e seus 2^8 valores possíveis. No entanto, constatou-se que é muito difícil encontrar permutações APN sobre $\mathbb{F}_{2^n}$ quando n é par. Até agora só foi encontrada uma permutação deste tipo, sobre $\mathbb{F}_{2^6}$ [30].

Desta forma, de acordo com Yu e Wang [29], é comum encontrarmos permutações 4-uniformes fazendo parte de caixas-S de cifradores modernos (um exemplo é o AES, padrão atual em criptografia simétrica). Então, considerando esta situação, uma generalização da busca por permutações APN consiste em trabalhar sobre anéis de inteiros [29].

A estrutura de anéis sobre inteiros já foi empregada na família de sistemas criptográficos SAFER, proposta por Massey [31], a qual usava permutações de $\mathbb{Z}_{256}$ para ele mesmo. Neste contexto, conforme Drakakis et al. [32], a definição de funções PN/APN é muito similar à definição de um tipo de permutação conhecida como Costas arrays. Um modo de construir Costas arrays, chamado de construção de Welch, fornece permutações APN sobre $\mathbb{Z}_{p-1}$, onde p é um primo. Esta construção de Welch consiste, portanto, em uma *generalização da função empregada por Massey em seu cifrador*.

A função APN de Massey e a sua generalização com o auxílio da construção de Welch para Costas arrays constituem-se em exemplos fundamentais de permutações sobre os inteiros (neste caso, $\mathbb{Z}_n$). Elas indicam a grande dificuldade de se obter permutações APN nestes domínios. Neste trabalho, no capítulo 10, é examinada a possibilidade da estrutura algébrica dos anéis do tipo $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$ tornar mais fácil a busca de APNs em domínios de tamanho 2^n.

9.1 A função de Massey (SAFER)

Massey [31] descreve a função por ele utilizada da seguinte forma:

- Se o byte de input é o inteiro j, então o byte de output é dado por:

$$45^j \bmod 257, \quad j = 0, 1, \ldots, 255$$

- Se o resultado modular é 256, o que ocorre para $j = 128$, este output é tomado como zero (0).
- Uma vez que 257 é primo, a aritmética é a de $\mathbb{F}_{257}$.
- O elemento 45 é um elemento primitivo deste corpo, i.e., as suas 256 primeiras potências geram todos os 256 elementos de corpos não nulos.

9.2 Generalização da função de Massey: a construção de Welch para Costas arrays

A construção de Welch é uma construção algébrica para Costas arrays baseada em corpos finitos que *leva a permutações APN*. Esta construção é descrita a seguir, de acordo com Drakakis et al. [32].

Definição 15 (Definition 5 in [32])**.** *Seja $\mathbb{Z}_p$ o corpo finito de ordem p (primo), $p > 2$. Seja g uma raiz primitiva de $\mathbb{Z}_p$. A bijeção Welch-Costas exponencial $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ é definida pela fórmula $f(i) = g^i$.*

Note que o domínio de f é naturalmente $\mathbb{Z}_{p-1}$, uma vez que $g^{p-1} = 1$.

Para simplificar, vamos considerar $\mathbb{Z}_{p-1}$ como o conjunto $\{0, 1, \ldots, p-2\}$ e também $\mathbb{Z}_p^*$ como o conjunto $\{1, 2, \ldots, p-1\}$. A fim de obter uma bijeção de $p-1$ elementos para $p-1$ elementos, Drakakis et al. [32] subtraem 1 dos valores de f. Em seguida, permutando os elementos dos conjuntos como se fossem as classes que eles representam, eles constróem uma permutação de $\mathbb{Z}_{p-1}$.

Em resumo, Drakakis et al. [32] obtêm uma nova função $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$, onde

$$f(i) = (g^i \bmod p) - 1$$

Esta função é por eles chamada de permutação Welch-Costas.

Então, eles provam o seguinte teorema:

Teorema 5 (Theorem 6 in [32])**.** *As permutações Welch-Costas são permutações APN sobre $\mathbb{Z}_{p-1}$.*

Proof. Ver a prova do Theorem 6 em [32]. □

Chapter 10

Permutações APN sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$

Este capítulo trata das buscas efetivamente realizadas no presente trabalho. Foram realizadas análises e buscas preliminares sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$ e $\mathbb{Z}_2 \times \mathbb{Z}_{2^3}$, de modo a identificar padrões que pudessem auxiliar nas análises e buscas sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$ (alvo principal desta parte do trabalho).

10.1 Análise exaustiva e lista de classes de equivalência

Os espaços de busca das permutações sobre os anéis $\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$ e $\mathbb{Z}_2 \times \mathbb{Z}_{2^3}$ são de tamanho razoável ($7! \simeq 2^{12}$ e $15! \simeq 2^{40}$ respectivamente) [1] e podem ser explorados de forma exaustiva.

A análise exaustiva serve, neste caso, para identificar todos os valores de ambiguidade e deficiência que aparecem. Os valores de ambiguidade possíveis foram aqui encarados como "classes" semelhantes às classes CCZ, muito mais difíceis de calcular. A seguir, são apresentados os resultados obtidos. Para cada "classe" de ambiguidade, é apresentada a primeira permutação encontrada (em ordem canônica) como sendo a representante da "classe". Para esta permutação, é apresentado o espectro diferencial. Note que, quando um valor de ambiguidade é atingido por mais de uma classe, todas são apresentadas.

Esta classificação "semelhante a CCZ" recaiu sobre os diferentes valores de ambiguidade porque o objetivo principal desta parte do trabalho era encontrar pelo menos uma permutação da classe de ambiguidade mínima (e, portanto, APN) do conjunto das permutações sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$. Esperava-se encontrar padrões nos conjuntos menores que pudessem ser utilizados no caso maior ($\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$ tem tamanho $31! \simeq 2^{113}$), aonde a busca exaustiva é totalmente inviável.

Muitos testes foram feitos, envolvendo composições dos elementos das classes, mas nenhum padrão foi ainda identificado na interação entre as diversas classes.

[1] Devido à estrutura aditiva dos anéis, o primeiro elemento de cada permutação pode sempre ser fixado em $(0, 0) = 0$, ou seja, toda classe contém sempre uma permutação que começa com 0.

10.1.1 Resultados para $\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$

Os resultados da análise exaustiva sobre $\mathbb{Z}_2 \times \mathbb{Z}_4$ estão mostrados na tabela 10.1. Note que o que está sendo] referido como "classe", na verdade corresponde a uma classificação simplificada, baseada exclusivamente nos valores de ambiguidade e no espectro diferencial. Esta classificação não corresponde exatamente àquela que seria imposta pela relação de equivalência CCZ, mas fica muito próxima dela e é simples o suficiente para permitir cálculos muito mais rápidos do que o que seria possível se a identificação da classe CCZ exata de cada permutação fosse incluída. O "representante de classe" mostrado na tabela corresponde ao menor elemento da classe, em ordem lexicográfica (apenas uma convenção).

A tabela 10.1 mostra que só há 20 classes possíveis, ou seja, toda permutação sobre $\mathbb{Z}_2 \times \mathbb{Z}_4$ produz apenas um dos 20 valores mostrados da dupla (ambiguidade, espectro diferencial). Note que alguns valores de ambiguidade aparecem repetidos, mas isto ocorre quando o espectro diferencial coerrespondente é diferente.

Observa-se que, das 20 classes possíveis, temos 3 que são APN (marcadas com um *), sendo uma delas correspondente à situação de ambiguidade mínima. Também pode-se notar que existe uma classe APN em que o espectro diferencial é composto apenas de 0s e 2s.

classe	"representante" da classe	espectro diferencial da classe ($[n_0, n_1, \ldots]$)	ambiguidade da classe
0	0 1 2 4 3 5 7 6 1	16 24 16 0 0 0 0 0 0	*16
1	0 1 3 5 2 7 4 6 0	16 26 12 2 0 0 0 0 0	18
2	0 1 2 4 5 7 6 3 0	18 22 14 2 0 0 0 0 0	20
3	0 1 3 4 2 6 5 7 1	20 16 20 0 0 0 0 0 0	*20
4	0 1 2 4 3 6 7 5 0	20 20 12 4 0 0 0 0 0	24
5	0 1 3 5 2 6 4 7 0	21 18 14 2 1 0 0 0 0	26
6	0 1 2 4 5 3 6 7 0	21 20 10 4 1 0 0 0 0	28
7	0 1 3 4 6 2 7 5 1	28 0 28 0 0 0 0 0 0	*28
8	0 1 3 4 2 5 7 6 0	24 16 12 0 4 0 0 0 0	36
9	0 1 3 5 2 4 6 7 0	31 2 18 2 3 0 0 0 0	42
10	0 1 2 4 5 3 7 6 0	32 0 20 0 4 0 0 0 0	44
11	0 1 2 3 4 6 7 5 0	31 2 20 0 1 2 0 0 0	46
12	0 1 2 5 4 7 6 3 0	34 0 16 0 6 0 0 0 0	52
13	0 1 2 4 5 6 7 3 0	36 0 12 0 8 0 0 0 0	60
14	0 1 2 3 4 5 7 6 0	35 2 12 0 5 2 0 0 0	62
15	0 1 4 5 2 7 6 3 0	35 0 16 0 4 0 0 0 1	68
16	0 1 3 2 4 5 7 6 0	39 0 8 0 8 0 0 0 1	84
17	0 1 2 3 4 7 6 5 0	43 0 0 0 12 0 0 0 1	100
18	0 1 2 3 5 6 7 4 0	45 0 0 0 8 0 0 0 3	132
19	0 1 2 3 4 5 6 7 0	49 0 0 0 0 0 0 0 7	196

Table 10.1: Caracterização das "classes" de ambiguidade para $\mathbb{Z}_2 \times \mathbb{Z}_4$.

10.1.2 Resultados para $\mathbb{Z}_2 \times \mathbb{Z}_{2^3}$

A tabela 10.2 mostra os resultados da análise exaustiva sobre $\mathbb{Z}_2 \times \mathbb{Z}_8$. Neste caso, o número de classes encontradas foi de 615, das quais 30 eram classes APN.

Observa-se que não existe uma classe APN em que o espectro diferencial é composto apenas de 0s e 2s, como no caso de $\mathbb{Z}_2 \times \mathbb{Z}_4$. No entanto, aquela possibilidade de heurística ainda pode ser melhor explorada em domínios maiores. Uma outra observação que pode levar a uma heurística útil em casos mais difíceis é que a tabela mostra que, para cada classe APN encontrada, logo abaixo havia uma classe 3-uniforme com espectro diferencial muito semelhante. Logo, uma boa possibilidade de busca parece ser tentar encontrar permutações 3-uniformes (mais fáceis), para depois "refiná-las" com um método por busca heurística adequado (como, por exemplo, Tabu search ou Simulated annealing).

classe	"representante" da classe	espectro diferencial da classe ($[n_0, n_1, \ldots]$)	ambiguidade da classe
0	0 1 3 5 8 14 9 4 10 6 13 7 15 12 2 11	54 132 54 0 0 0 0 0 0 0 0 0 0 0 0 0	*54
1	0 1 2 4 7 8 13 9 5 3 15 10 14 6 12 11	52 140 44 4 0 0 0 0 0 0 0 0 0 0 0 0	56
2	0 1 2 4 8 15 7 13 10 12 3 6 11 9 14 5	57 128 53 2 0 0 0 0 0 0 0 0 0 0 0 0	59
3	0 1 2 4 7 9 14 12 10 13 3 11 15 6 8 5	55 134 48 2 1 0 0 0 0 0 0 0 0 0 0 0	60
4	0 1 2 4 7 10 3 12 5 11 15 6 8 14 9 13	60 120 60 0 0 0 0 0 0 0 0 0 0 0 0 0	*60
5	0 1 2 4 7 6 11 14 3 10 12 8 5 9 15 13	59 124 55 2 0 0 0 0 0 0 0 0 0 0 0 0	61
6	0 1 2 4 9 14 12 3 10 13 6 5 15 11 7 8	61 118 61 0 0 0 0 0 0 0 0 0 0 0 0 0	*61
7	0 1 2 4 3 8 13 10 9 11 15 7 14 12 6 5	58 128 50 4 0 0 0 0 0 0 0 0 0 0 0 0	62
8	0 1 2 4 7 11 6 14 3 10 12 8 5 9 15 13	62 116 62 0 0 0 0 0 0 0 0 0 0 0 0 0	*62
9	0 1 2 3 7 10 5 11 6 4 14 8 13 9 12 15	59 126 51 4 0 0 0 0 0 0 0 0 0 0 0 0	63
10	0 1 2 4 10 15 3 12 9 6 8 11 14 7 5 13	63 114 63 0 0 0 0 0 0 0 0 0 0 0 0 0	*63
11	0 1 2 3 5 11 14 12 7 8 15 6 13 10 4 9	60 124 52 4 0 0 0 0 0 0 0 0 0 0 0 0	64
12	0 1 2 4 7 8 5 15 3 13 9 12 10 14 11 6	64 112 64 0 0 0 0 0 0 0 0 0 0 0 0 0	*64
13	0 1 2 3 5 7 11 10 9 14 6 15 13 8 12 4	61 122 53 4 0 0 0 0 0 0 0 0 0 0 0 0	65
14	0 1 2 4 3 10 15 12 9 11 6 8 14 7 13 5	65 110 65 0 0 0 0 0 0 0 0 0 0 0 0 0	*65
15	0 1 2 3 5 8 12 15 4 14 10 6 11 9 7 13	60 126 48 6 0 0 0 0 0 0 0 0 0 0 0 0	66
16	0 1 2 4 7 5 8 12 3 9 14 13 6 11 15 10	66 108 66 0 0 0 0 0 0 0 0 0 0 0 0 0	*66
17	0 1 2 3 5 8 12 15 7 14 4 11 10 6 9 13	63 118 55 4 0 0 0 0 0 0 0 0 0 0 0 0	67
18	0 1 2 4 7 3 9 12 13 10 5 8 14 6 15 11	67 106 67 0 0 0 0 0 0 0 0 0 0 0 0 0	*67
19	0 1 2 3 5 8 11 9 6 10 15 7 14 4 13 12	62 122 50 6 0 0 0 0 0 0 0 0 0 0 0 0	68
20	0 1 2 4 3 9 15 14 8 12 7 5 10 13 6 11	68 104 68 0 0 0 0 0 0 0 0 0 0 0 0 0	*68
	(...)		
614	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	225 0 0 0 0 0 0 0 0 0 0 0 0 0 0 15	1800

Table 10.2: Caracterização das "classes" de ambiguidade para $\mathbb{Z}_2 \times \mathbb{Z}_8$.

10.2 Busca de APNs em $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ com backtracking

No caso das permutações sobre $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$, uma análise exaustiva pura e simples fica inviável. Então aqui o foco passa a ser encontrar uma permutação (pelo menos) que seja APN.

Para isto, foi preparado um backtracking para percorrer todas as permutações no domínio. O backtracking fixa o primeiro elemento de todas as permutações em 0 e passa (em tese) sobre todas as possibilidades de diferenças ($\Delta_a(x) = f(x+a) - f(x)$) para cada posição da linha $a = 1$ em sequência.

Um parâmetro u define a "uniformidade" desejada. Por exemplo, $u = 3$ é para buscas por uma permutação 3-uniforme e $u = 2$ é para buscas por APNs. O backtracking é podado com base neste parâmetro u: antes de um valor d qualquer ser posicionado em qualquer entrada $(1, j)$ de $\Delta_1(x)$ (na linha para $a = 1$), são analisadas as posições que serão atingidas por este d na matriz $\Delta_a(x)$ inteira (para todos os valores de $a = 2, \ldots, n$). Se em qualquer linha a quantidade de repetições de qualquer número for maior do que u (ou seja, se o posicionamento deste d implicar em que a u uniformidade não possa ser cumprida), todo o ramo correspondente a este d é podado e passa-se ao próximo candidato para aquela posição $(1, j)$.

A poda do backtracking com base na u-uniformidade desejada é bastante eficiente e já reduz enormemente o espaço de busca, levando à produção de permutações nas respectivas classes APNs para $\mathbb{Z}_2 \times \mathbb{Z}_8$ (espaço de busca $\simeq 2^{40}$) em milésimos de segundo, em um laptop comum. No entanto, é claro, este nível de otimização é insuficiente para o domínio $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$ (espaço de busca $\simeq 2^{113}$).

10.2.1 Otimização do backtracking: heurísticas

Na implementação das buscas, define-se um n como sendo o número de elementos de cada permutação (no caso de $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$, $n = 32$). Na verdade, cada par ordenado de $\mathbb{Z}_2 \times \mathbb{Z}_{2^4}$ é mapeado para um único inteiro de forma natural ($(0,0) = 0, (0,1) = 1, \ldots, (1,15) = 31$).

Diversas heurísticas foram tentadas, com base na observaçãoo dos resultados obtidos nas análises exaustivas de $\mathbb{Z}_2 \times \mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_8$. Duas dentre elas funcionaram e possibilitaram a obtenção de resultados concretos importantes sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ (note que, neste caso, $n = 32$):

1. "Antes da coluna central de $\Delta_a(x)$, nunca há um valor repetido de diferenças na linha $n/4$"
   - ou seja, as "u" repetições só podem aparecer na segunda metade da linha $a = n/4$
   - esta heurística possibilitou a obtenção de uma permutação 3-uniforme
   - os resultados obtidos com o backtracking otimizado com esta heurística estão apresentados na subseção 10.2.3.
2. "Na metade superior da matriz $\Delta_a(x)$, nunca há um valor de diferença maior ou igual a $n/2$"

- ou seja, na metade de cima de $\Delta_a(x)$ só aparecem valores menores do que $n/2$ ($n = 32$, no caso de $\mathbb{Z}_2 \times \mathbb{Z}_{16}$) e na metade de baixo só aparecem valores $\geq n/2$
- esta heurística possibilitou a obtenção de uma permutação 4-uniforme muito peculiar, com um padrão que talvez possa ser aproveitado para, com otimização heurística, chegar a uma permutação 2-uniforme (APN)
- o padrão encontrado fica evidente na matriz λ, que fica subdividida em 4 sub-regiões quadradas de mesmo tamanho, duas em cima e duas embaixo, com a segunda sub-região de cima e a primeira de baixo compostas somente de zeros, em uma forma semelhante a "ladrilhos" entre regiões nulas e não nulas
- os resultados obtidos com o backtracking otimizado com esta heurística também estão na subseção 10.2.3.

10.2.2 Otimização do backtracking: automorfismos

Uma outra otimização tentada sobre o backtracking já implementado com a poda descrita na subseção 10.2.1 consistiu em eliminar os ramos que, após aplicação dos automorfismos aos elementos já colocados da permutação, produziam uma tabela $\Delta_a(x)$ com um número maior de repetições em cada linha do que o permitido pelo parâmetro u.

Isto é equivalente a mapear com os automorfismos e ver se a permutações transformadas (pelos automorfismos) não produziam tabelas proibidas. Ou seja, se qualquer cõpia automórfica do que está colocado na tabela $\Delta_a(x)$ produzir uma configuração que não poderá ser u-uniforme (por já ter repetições demais de algum valor em qualquer linha), toda a árvore que está embaixo da permutação atual (ou o que já foi colocado dela) já pode ser descartada. Esta otimização não produziu melhora significativa em relação ao backtracking otimizado com a heurística descrita em 10.2.1 e acabou sendo desconsiderada.

10.2.3 Resultados para $\mathbb{Z}_2 \times \mathbb{Z}_{16}$

Inicialmente, é apresentado o melhor resultado obtido com a heurística que levou a uma permutação 4-uniforme com um padrão de "ladrilhos" na sua matriz λ (ver subseção 10.2.1 acima). A permutação encontrada foi: [2]

$$p_{4u} = \texttt{[0 1 2 3 4 6 8 10 13 9 11 14 5 15 7 12 16 19 22 26 30 18 25 17 31 29 24 23 21 20 28 27]} \tag{10.1}$$

O espectro diferencial (4-uniforme) associado a esta permutação é:

$$[n_0, n_1, n_2, n_3, n_4, n_5, n_6, n_7, \ldots] = [554, 128, 139, 98, 73, 0, 0, 0, \ldots]$$

O valor de ambiguidade associado a este espectro é de 871 e a deficiência correspondente vale $n_0 = 554$.

[2] Lembre que estamos adotando um mapeamento natural de $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ para $\mathbb{Z}_{32}$, em que $(0,0) \to 0, (0,1) \to 1, \ldots, (1,15) \to 31$.

a \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	2	2	2	3	12	2	3	7	10	8	5	4	3	3	4	4	4	7	8	14	14	11	15	14	15	8	15	5
2	2	2	2	3	4	4	5	15	14	5	10	1	2	13	9	5	6	7	8	8	11	15	6	12	9	10	13	13	7	7	4	8
3	3	3	4	5	6	7	1	1	1	12	4	9	7	1	10	6	10	11	12	15	3	13	4	7	8	8	12	5	6	12	7	11
4	4	5	6	7	9	3	3	4	8	6	12	14	11	2	11	7	14	15	3	7	1	11	15	6	6	7	4	4	11	15	10	15
5	6	7	8	10	5	5	6	11	2	14	1	2	12	3	12	8	2	6	11	5	15	6	14	4	5	15	3	9	14	2	14	3
6	8	9	11	6	7	8	13	5	10	3	5	3	13	4	13	10	9	14	9	3	10	5	12	3	13	14	8	12	1	6	2	7
7	10	12	7	8	10	15	7	13	15	7	6	4	14	5	15	12	1	12	7	14	9	3	11	11	12	3	11	15	5	10	6	14
8	13	8	9	11	1	9	15	2	3	8	7	5	15	7	1	14	15	10	2	13	7	2	3	10	1	6	14	3	9	14	13	6
9	9	10	12	2	11	1	4	6	4	9	8	6	1	9	3	1	13	5	1	11	6	10	2	15	4	9	2	7	13	5	5	4
10	11	13	3	12	3	6	8	7	5	10	9	8	3	11	6	13	8	4	15	10	14	9	7	2	7	13	6	11	4	13	3	2
11	14	4	13	4	8	10	9	8	6	11	11	10	5	14	2	15	7	2	14	2	13	14	10	5	11	1	10	2	12	11	1	13
12	5	14	5	9	12	11	10	9	7	13	13	12	8	10	4	2	5	1	6	1	2	1	13	9	15	5	1	10	10	9	12	12
13	15	6	10	13	13	12	11	10	9	15	15	15	4	12	7	9	4	9	5	6	5	4	1	13	3	12	9	8	8	4	11	10
14	7	11	14	14	14	13	12	12	11	1	2	11	6	15	14	3	12	8	10	9	8	8	5	1	10	4	7	6	3	3	9	9
15	12	15	15	15	15	14	14	14	13	4	14	13	9	6	8	11	11	13	13	12	12	12	9	8	2	2	5	1	2	1	8	1
16	16	18	20	23	26	28	17	23	18	20	29	25	16	21	21	31	16	30	28	25	22	20	31	25	30	28	19	23	16	27	27	17
17	19	21	24	27	30	19	25	21	16	31	28	23	31	29	20	20	17	31	29	26	24	22	17	28	26	30	22	30	26	19	16	21
18	22	25	28	31	21	27	23	19	27	30	26	22	23	28	25	23	18	16	30	28	26	24	20	24	28	17	29	24	18	24	20	22
19	26	29	16	22	29	25	21	30	26	28	25	30	22	17	28	26	19	17	16	30	28	27	16	26	31	24	23	16	23	28	21	23
20	30	17	23	30	27	23	16	29	24	27	17	29	27	20	31	30	20	19	18	16	31	23	18	29	22	18	31	21	27	29	22	24
21	18	24	31	28	25	18	31	27	23	19	16	18	30	23	19	18	22	21	20	19	27	25	21	20	16	26	20	25	28	30	23	25
22	25	16	29	26	20	17	29	26	31	18	21	21	17	27	23	22	24	23	23	31	29	28	28	30	24	31	24	26	29	31	24	27
23	17	30	27	21	19	31	28	18	30	23	24	24	21	31	27	29	26	26	19	17	16	19	22	22	29	19	25	27	30	16	26	29
24	31	28	22	20	17	30	20	17	19	26	27	28	25	19	18	21	29	22	21	20	23	29	30	27	17	20	26	28	31	18	28	31
25	29	23	21	18	16	22	19	22	22	29	31	16	29	26	26	19	25	24	24	27	17	21	19	31	18	21	27	29	17	20	30	18
26	24	22	19	17	24	21	24	25	25	17	19	20	20	18	24	17	27	27	31	21	25	26	23	16	19	22	28	31	19	22	17	30
27	23	20	18	25	23	26	27	28	29	21	23	27	28	16	22	28	30	18	25	29	30	30	24	17	20	23	30	17	21	25	29	16
28	21	19	26	24	28	29	30	16	17	25	30	19	26	30	17	27	21	28	17	18	18	31	25	18	21	25	16	19	24	21	31	19
29	20	27	25	29	31	16	18	20	21	16	22	17	24	25	16	25	31	20	22	22	19	16	26	19	23	27	18	22	20	23	18	26
30	28	26	30	16	18	20	22	24	28	24	20	31	19	24	30	24	23	25	26	23	20	17	27	21	25	29	21	18	22	26	25	20
31	27	31	17	19	22	24	26	31	20	22	18	26	18	22	29	16	28	29	27	24	21	18	29	23	27	16	17	20	25	17	19	28

Table 10.3: Tabela de diferenças $\Delta_{p_{4u},a}(x)$ para a permutação 4-uniforme sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ dada pela eq. 10.1.

Com a segunda heurística, foi possível chegar ao melhor resultado obtido nesta parte do trabalho, com a obtenção da seguinte permutação 3-uniforme:

$$p_{3u} = \texttt{[0 1 2 3 5 7 9 12 15 4 11 14 30 18 22 27 6 10 8 13 20 29 28 24 23 19 17 26 21 16 31 25]} \tag{10.2}$$

O espectro diferencial (3-uniforme) associado a esta permutação é:

$$[n_0, n_1, n_2, n_3, n_4, n_5, n_6, n_7, \ldots] = [368, 348, 184, 92, 0, 0, 0, \ldots]$$

O valor de ambiguidade associado a este espectro é de 460 e a deficiência correspondente vale $n_0 = 368$.

a \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	4	4	4	2	0	2	3	0	1	1	1	0	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	4	1	3	3	2	3	3	2	2	1	1	3	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	4	0	3	3	2	3	4	2	1	2	2	4	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	1	3	4	1	4	4	1	1	1	4	1	0	2	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	1	4	3	1	4	4	1	2	1	1	2	2	0	4	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	1	4	1	3	2	2	3	3	3	1	2	4	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	1	0	2	1	2	2	4	1	1	3	3	4	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	3	3	3	0	1	2	3	2	3	2	1	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	4	3	1	4	3	3	1	1	4	2	2	1	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	2	4	2	1	3	3	3	2	2	3	1	4	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	2	4	0	2	2	1	1	2	1	4	4	1	3	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	4	2	0	1	4	1	1	1	4	4	1	4	3	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	1	0	1	4	2	2	1	2	4	3	2	3	3	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	2	1	3	1	1	2	2	3	3	2	3	3	1	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	3	3	0	1	1	1	0	3	2	0	2	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	2	1	3	2	1	3	0	3	1	2	3	1	2	2
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	3	2	3	2	1	2	1	3	1	2	2	3	3
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	1	2	1	3	3	4	2	2	2	4	1	2	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	1	0	2	2	3	1	2	4	1	4	2	3	1
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	1	2	1	2	3	2	0	0	4	0	4	3	3
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	4	3	3	2	1	3	1	4	1	2	2	0	2	2
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	0	1	2	1	3	4	1	3	2	2	4	1	4
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	1	4	0	2	2	1	2	1	3	3	1	3	3	2
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	2	4	2	2	1	0	1	2	2	4	2	2	3
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	3	1	3	3	1	2	1	2	2	0	4	1	2
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	1	4	2	2	3	1	4	3	1	2	1	0	1	2
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	0	2	2	1	4	1	3	1	2	3	3	4	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	3	4	0	4	0	0	2	3	2	1	2	1	3	2
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	1	3	2	4	1	4	2	1	3	2	2	0	1	0	2
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	1	4	2	2	2	4	3	3	1	2	1	2	1
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	3	2	2	1	3	1	2	1	2	3	2	3	0	2

Table 10.4: Tabela de $\lambda_{a,b}(p_{4u})$ para uma permutação 4-uniforme sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ dada pela eq. 10.1. (Notar o aspecto de "ladrilho" formado pelos zeros.)

a \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	2	2	2	3	3	5	7	3	16	4	4	5	21	4	14	5	23	9	15	12	15	12	14	9	11	11	15	10	29
2	2	2	3	4	4	5	6	8	12	10	19	20	8	9	26	22	2	3	28	16	8	11	11	11	10	7	4	6	10	9	23	17
3	3	4	5	6	7	8	11	15	15	26	23	24	13	30	27	23	7	26	21	31	4	10	7	9	3	2	15	5	4	22	27	31
4	5	6	7	9	10	13	2	2	31	30	27	29	18	31	28	24	30	19	20	27	3	6	5	2	14	13	14	15	17	26	25	20
5	7	8	10	12	15	4	5	18	19	18	16	2	19	16	29	26	23	18	16	26	15	4	14	13	9	12	8	28	21	24	30	11
6	9	11	13	1	6	7	21	22	23	23	5	3	20	17	31	28	22	30	31	22	13	13	9	8	8	6	21	16	19	29	5	4
7	12	14	2	8	9	23	25	26	28	12	6	4	21	19	17	30	18	29	27	20	6	8	4	7	2	19	25	30	24	4	14	3
8	15	3	9	11	25	27	29	31	1	13	7	5	23	21	19	17	17	25	25	29	1	3	3	1	31	23	23	19	15	13	13	15
9	4	10	12	27	29	31	18	4	2	14	8	7	25	23	22	20	29	23	18	24	12	2	13	30	19	21	28	10	8	12	9	14
10	11	13	28	31	17	20	7	5	3	15	10	9	27	26	25	25	27	16	29	19	11	12	26	18	17	26	3	3	7	8	8	10
11	14	29	16	19	22	9	8	6	4	1	12	11	30	29	30	16	20	27	24	18	5	25	30	16	22	1	12	2	3	7	4	8
12	30	17	20	24	11	10	9	7	6	3	14	14	17	18	21	19	31	22	23	28	18	29	28	21	13	10	11	14	2	3	2	1
13	18	21	25	13	12	11	10	9	8	5	1	1	22	25	24	3	26	21	17	9	22	27	17	12	6	9	7	13	14	1	11	12
14	22	26	14	14	13	12	12	11	10	8	4	6	29	28	8	7	25	31	14	13	20	16	8	5	5	5	6	9	12	10	6	7
15	27	15	15	15	14	14	14	13	13	11	9	13	16	12	12	11	19	12	2	11	25	7	1	4	1	4	2	7	5	5	1	6
16	6	9	6	10	31	22	19	28	24	31	22	28	7	14	9	14	10	7	10	6	17	26	29	20	24	17	26	20	9	2	7	2
17	10	7	11	17	24	21	31	27	20	29	31	23	2	13	3	27	11	8	11	8	19	28	16	23	29	24	29	4	13	6	12	23
18	8	12	18	26	23	17	30	23	18	22	26	18	1	7	16	31	12	9	13	10	21	31	19	28	20	27	13	8	1	11	17	24
19	13	19	27	25	19	16	26	21	27	17	21	17	11	20	20	29	13	11	15	12	24	18	24	19	23	11	1	12	6	16	18	25
20	20	28	26	21	18	28	24	30	22	28	20	27	24	24	18	18	15	13	1	15	27	23	31	22	7	15	5	1	27	17	19	26
21	29	27	22	20	30	26	17	25	17	27	30	8	28	22	23	9	1	15	4	2	16	30	18	6	11	3	10	22	28	18	20	28
22	28	23	21	16	28	19	28	20	16	21	11	12	26	27	14	2	3	2	7	7	23	17	2	10	15	8	31	23	29	19	22	30
23	24	22	17	30	21	30	23	19	26	2	15	10	31	2	7	1	6	5	12	14	26	1	6	14	4	29	16	24	30	21	24	16
24	23	18	31	23	16	25	22	29	7	6	13	15	6	11	6	13	9	10	3	1	10	5	10	3	25	30	17	25	16	23	26	19
25	19	16	24	18	27	24	16	10	11	4	2	22	15	10	2	12	14	1	6	17	14	9	15	24	26	31	18	27	18	25	29	22
26	17	25	19	29	26	18	13	14	9	9	25	31	14	6	1	8	5	4	22	21	2	14	20	25	27	16	20	29	20	28	16	27
27	26	20	30	28	20	15	1	12	14	16	18	30	10	5	13	6	8	20	26	25	7	19	21	26	28	18	22	31	23	31	21	18
28	21	31	29	22	1	3	15	1	21	25	17	26	9	1	11	15	24	24	30	30	28	20	22	27	30	20	24	18	26	20	28	21
29	16	30	23	3	5	1	4	24	30	24	29	25	5	15	4	10	28	28	19	3	29	21	23	29	16	22	27	21	31	27	31	5
30	31	24	4	7	3	6	27	17	29	20	28	21	3	8	15	5	16	17	8	4	30	22	25	31	18	25	30	26	22	30	15	9
31	25	5	8	5	8	29	20	16	25	19	24	19	12	3	10	4	21	6	9	5	31	24	27	17	21	28	19	17	25	14	3	13

Table 10.5: Tabela de diferenças $\Delta_{p_{3u},a}(x)$ para uma permutação 3-uniforme sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ dada pela eq. 10.2.

a \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	3	3	3	3	3	0	1	0	2	1	2	2	0	2	3	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0
2	0	0	3	2	3	1	2	1	3	2	3	3	1	0	0	0	1	1	0	1	1	0	1	1	0	0	1	0	1	0	0	0
3	0	0	1	2	3	2	1	3	1	1	1	1	0	1	0	3	0	0	0	0	0	1	1	2	1	0	2	2	0	0	1	2
4	0	0	3	1	0	2	2	1	0	1	1	0	0	2	2	1	0	1	1	1	2	0	0	0	1	1	1	2	1	1	2	2
5	0	0	1	0	2	1	0	1	2	1	1	1	2	1	1	2	3	0	3	2	0	1	0	1	1	0	2	0	1	1	1	0
6	0	1	0	1	1	2	2	1	2	2	0	1	0	3	0	0	1	1	0	1	1	2	3	2	0	0	0	0	1	1	1	2
7	0	0	2	1	3	0	2	1	2	1	0	0	2	0	2	0	0	1	1	2	1	1	0	1	1	2	1	1	1	1	2	0
8	0	3	0	3	0	1	0	1	0	1	0	1	0	3	0	3	0	2	0	2	0	1	0	3	0	3	0	1	0	2	0	2
9	0	0	2	0	2	0	0	1	2	1	2	0	3	1	2	0	0	0	2	1	1	1	1	2	1	1	0	1	1	2	1	1
10	0	0	0	3	0	1	0	2	2	1	2	2	1	1	0	1	1	2	1	1	1	0	0	0	0	2	3	2	1	1	0	1
11	0	2	1	1	2	1	1	1	2	1	0	1	2	0	1	0	3	0	1	1	1	0	2	0	1	1	0	1	0	2	3	0
12	0	1	2	2	0	0	1	1	0	1	2	2	0	1	3	0	0	2	2	1	1	2	1	1	1	0	0	0	2	1	1	1
13	0	3	0	1	0	1	1	1	1	3	1	2	3	2	1	0	0	2	1	0	0	2	2	0	1	2	1	1	0	0	0	0
14	0	0	0	0	1	3	3	2	3	1	2	1	3	2	3	0	1	0	0	0	1	0	1	0	0	1	1	0	1	1	0	1
15	0	3	2	0	2	2	1	2	0	1	0	3	3	3	3	3	1	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0
16	0	0	2	0	0	0	3	3	0	3	3	0	0	0	2	0	0	2	0	1	2	0	2	0	2	0	2	0	2	1	0	2
17	0	0	1	1	1	0	1	1	2	0	1	3	1	2	0	0	1	1	0	1	1	1	0	3	2	0	0	2	1	3	0	2
18	0	2	0	0	0	0	0	1	2	1	1	1	2	2	0	0	1	2	3	1	1	1	1	2	1	0	2	1	1	0	1	2
19	0	1	0	0	0	0	1	0	0	0	0	3	2	2	0	1	2	2	2	3	2	2	0	1	2	2	1	2	0	1	0	0
20	0	2	0	0	0	1	0	1	0	0	0	0	0	1	0	3	0	1	3	1	2	1	2	1	3	0	2	3	3	0	1	1
21	0	1	1	1	1	0	1	0	1	1	1	1	0	0	0	1	1	2	2	0	2	0	3	1	0	1	1	2	3	1	3	0
22	0	0	3	1	0	0	0	2	1	0	1	1	1	0	1	1	2	1	0	2	1	2	1	3	0	0	1	1	3	1	1	1
23	0	2	2	0	1	1	2	1	0	0	1	0	1	0	2	1	2	1	0	1	0	2	1	1	3	0	2	0	0	1	3	1
24	0	1	0	2	0	1	3	1	0	1	3	1	0	2	0	1	2	1	1	1	0	0	1	3	0	3	1	0	0	1	1	1
25	0	1	2	0	1	0	1	0	0	1	2	1	1	0	2	2	2	1	3	1	0	0	2	0	3	1	1	2	0	1	0	1
26	0	1	1	0	1	1	1	0	1	2	0	0	0	1	3	0	2	1	1	1	3	1	1	0	0	3	1	2	1	2	0	1
27	0	1	0	0	0	1	1	1	1	0	1	0	1	1	1	1	1	0	3	1	3	2	1	1	0	1	3	0	2	0	2	2
28	0	3	0	1	0	0	0	0	0	1	0	1	0	0	0	2	0	1	1	0	3	3	2	0	3	1	2	1	2	1	3	1
29	0	1	0	2	2	3	0	0	0	0	1	0	0	0	0	1	2	0	0	1	0	2	1	2	2	1	0	2	2	3	2	2
30	0	0	0	2	2	1	1	1	2	1	0	0	0	0	0	2	1	2	1	0	1	1	2	0	1	2	1	1	1	1	3	2
31	0	0	0	2	1	3	1	0	2	1	1	0	1	1	1	0	1	2	0	3	1	2	0	0	2	3	0	1	1	1	0	1

Table 10.6: Tabela de $\lambda_{a,b}(p_{3u})$ para uma permutação 3-uniforme sobre $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ dada pela eq. 10.2.

Bibliography

[1] D. Panario, A. Sakzad, B. Stpars, D. Thomson e Q. Wang, "Ambiguity and Deficiency of permutations over Finite Fields with linearized difference map", IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5616-5626, sep. 2013.

[2] https://en.wikipedia.org/wiki/Quartic_function . Accessed in 03/14/2016.

[3] R. Lidl e H. Niederreiter, "Finite Fields", 2nd ed., Cambridge Univ. Press, 1997.

[4] K. Ireland, M. Rosen, "A Classical Introduciton to Modern Number Theory", 2nd ed., Springer, 1990.

[5] SAGE Mathematical Software 2010, free software available at: `http://www.sagemath.org/`

[6] D. Panario, A. Sakzad, B. Stpars, e Q. Wang, "Two new measures for permutations: Ambiguity and Deficiency", IEEE Trans. Inf. oory, vol. 57, no. 11, pp. 7648-7657, Nov. 2011.

[7] D. Panario, B. Stpars e Q. Wang, "Ambiguity and Deficiency in Costas Arrays and APN permutations", in: Latin 2010, LNCS 6034, pp. 397-406, 2010.

[8] G.L. Mullen, D. Panario (Eds.), Handbook of Finite Fields, in: Discrete Math. Ser., Chapman e Hall/CRC, 2013.

[9] R. Lidl e H. Niederreiter, "Finite Fields", 2nd ed., Cambridge Univ. Press, 1997.

[10] C. Blondeau e K. Nyberg, "Perfect nonlinear functions and Cryptography", Finite Fields and their Appls., vol. 32, pp. 120-147, 2015.

[11] K. Nyberg, "Differentially uniform mappings for cryptography", in: EUROCRYPT '93, pp. 55–64, 1994.

[12] K. Drakakis, R. Gow e G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays", Discrete Appl. Math., vol. 157, no. 15, pp. 3320-3326, 2009.

[13] M. Brinkmann e G. Leander, "On the classification of APN functions up to dimension five", Des. Codes Cryptogr., 49 (1-3), pp. 273-288, 2008.

[14] K.A. Blinhaning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe, "An APN permutation in dimension six", in: Finite Fields: Theory e Applications, in: Contemp. Math., vol. 518, pp. 33–42, Amer. Math. Soc., 2010.

[15] E. Cornet, "The Dillon-Wolfe Function for Cryptography", M.Sc. Thesis, 2012.

[16] C. Blondeau, "La cryptanalyse différentielle et ses généralisations", Cryptography and Security, Université Pierre et Marie Curie - Paris VI, 2011. French. <tel-00649842>

[17] V. Zinoviev, C. Carlet, P. Charpin, "Codes, bent functions and permutations suitable for DES-like cryptosystems", Designs, Codes and Cryptography, 15(2):125-156, 1998.

[18] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", in: A. Menezes, S.A. Vanstone (Eds.), CRYPTO, in: Lect. Notes Comput. Sci., vol. 537, pp. 2–21, Springer, 1990.

[19] M. Matsui, "Linear cryptanalysis method for DES cipher", in: Advances in Cryptology -EUROCRYPT'93, ser. Lecture Notes Comput. Sci., New York, NY, USA: Springer, vol. 765, pp. 386-397, 1994.

[20] J. Daemen, V. Rijmen, "AES Proposal", National Institute of Standards and Technology, Rijndael, 2000.

[21] J. Daemen, V. Rijmen, "The design of Rijndael: AES - o Advanced Encryption Standard", New York, Springer, 2002.

[22] J.L. Massey, "SAFER K-64: a byte-oriented block-ciphering algorithm", in: R.J. Anderson (Ed.), Fast Software Encryption, FSE'93, in: Lect. Notes Comput. Sci., vol. 809, pp. 1–17, Springer, 1994.

[23] J.F. Voloch, "Symmetric cryptography and algebraic curves", in: Algebraic Geometry and its Applications, vol. 5 de Ser. número oory Appl., 135–141, World Sci. Publ., Hackensack, NJ, 2008.

[24] G. Bertoni, J. Daemen, M. Peeters e G. Van Assche, "The Keccak sponge function family", `http://keccak.noekeon.org/`, 2012.

[25] K. Drakakis, R. Gow e G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays", Discrete Appl. Math. 157 (15), 3320–3326, 2009.

[26] C. Blondeau, A. Canteaut e P. Charpin, "Differential properties of power functions", Int. J. informação e Coding oory, Vol. 1, No. 2, pp. 149-170, 2010.

[27] C. Blondeau, A. Canteaut e P. Charpin, "Differential properties of $x \mapsto x^{2^t-1}$", IEEE Trans. então Inf. oory, vol. 57, no. 12, pp. 8127-8137, Dec. 2011.

[28] C.J. Shallue, I.M. Wanless, Permutation polynomials and orthomorphism polynomials of degree six, Finite Fields e their Applications 20 (2013), 84-92.

[29] Y. Yu, M. Wang, Permutation polynomials and their differential properties over residue class rings, Discrete Applid Mathematics, vol. 161, issue 18, pp. 3104-3108, Dec. 2013.

[30] J.F. Dillon, APN polynomials: an update, The 9th International Conference on Finite Fields and Applications, Dublin, Ireland, July 2009.

[31] J.L. Massey, SAFER K-64: A byte-oriented block-ciphering algorithm, Fast Software Encryption, pp. 1-17, 1993.

[32] K. Drakakis, R. Gow, G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, Discrete Applied Mathematics, vol. 157, pp. 3320-3326, 2009.

[33] Maomatical Software 2010, free software available at: `http://www.sagemath.org/`

[34] `http://people.math.carleton.ca/ daniel/`

[35] `http://people.math.carleton.ca/ brett/`

[36] `http://people.math.carleton.ca/ wang/`