Universidade Estadual de Campinas
Instituto de Matemática Estatística e Computação Científica
Departamento de Matemática Aplicada

Quadrados latinos e aplicações

Mateus Alegri
Mestrado em Matemática Aplicada

Orientador: **Prof. Dr. José Plínio de Oliveira Santos**

Trabalho financiado pela Capes

Campinas, agosto de 2006

Quadrados latinos e aplicações

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Mateus Alegri** e aprovada pela comissão julgadora.

Campinas, 4 de agosto de 2006.

Prof. Dr. **José Plínio de Oliveira Santos**
Orientador

Banca examinadora:
Prof. Dr. José Plínio de Oliveira Santos (IMECC/UNICAMP)
Prof. Dr. Paulo Mondek (UFMT)
Prof. Dr. Émerson do Monte Carmelo (UEM)

Dissertação apresentada ao Instituto de Matemática Estatística e Computação Científica, UNICAMP, como requisito parcial para a obtenção do título de **Mestre em Matemática Aplicada**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Alegri, Mateus
AL25q Quadrados latinos e aplicações / Mateus Alegri – Campinas, [S.P. :s.n.], 2006.

Orientador : José Plínio Oliveira dos Santos
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos de controle de erros (Teoria da informação). 2. Hipercubo. 3. Grupos de permutação. I. Santos, José Plínio Oliveira dos. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Latin squares and applications.

Palavras-chave em inglês (Keywords): 1. Error correcting codes (Information theory). 2. Hipercubes. 3. Permutation groups.

Área de concentração: Matemática Discreta

Titulação: Mestre em Matemática Aplicada

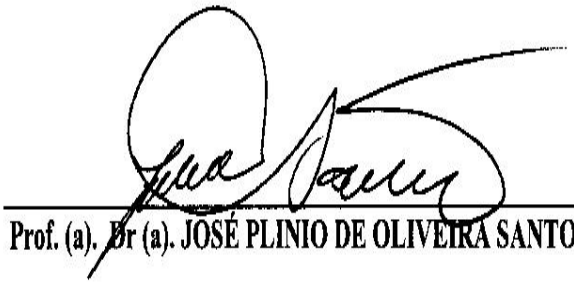
Banca examinadora: Prof. Dr. José Plínio Oliveira dos Santos (IMECC-UNICAMP)
Prof. Dr. Paulo Mondek (UFMT)
Prof. Dr. Emerson do Monte Carmelo (UEM)

Data da defesa: 04/08/2006

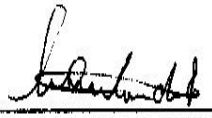
Programa de Pós-Graduação: Mestrado em Matemática Aplicada

Dissertação de Mestrado defendida em 04 de agosto de 2006 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



Prof. (a). Dr (a). JOSÉ PLINIO DE OLIVEIRA SANTOS



Prof. (a). Dr (a). PAULO MONDEK

Prof. (a). Dr (a). EMERSON LUIZ DO MONTE CARMELO

Agradecimentos

À Deus,

Aos meus pais Valdomiro e Júlia, a minha irmã.

À minha namorada Cristiane Baretta.

Ao meu orientador Prof. Dr. Plínio de Oliveira Santos.

Ao Prof. Dr Paulo Mondek.

Aos amigos de caminhada, Wellington Vieira, Fábio Bertolotto, Mayk Coelho, Gabriel Haeser, Moisés Cecconello, Ricardo Lópes, Fábio Dorini, e Luciana Elias, Maurício Yudi Miyamura, Luís Roberto Almeida.

Resumo

Neste trabalho estudaremos a estrutura dos quadrados latinos sob ponto de vista da matemática discreta. Faremos uma série de equivalências com outras estruturas tais como Teoria dos Grafos, Grupos, e sempre enfocando questões enumerativas. Certas propriedades de quadrados latinos, tais como ortogonalidade vão trabalhadas. E encerraremos com aplicações a teoria dos códigos algébricos.

Palavras chave: quadrados latinos; Quadrados latinos mutualmente ortogonais; MOLS; hipercubos; códigos MDS.

Abstract

In this work, we study the structure of latin squares on the discrete mathematics viewpoint. We do a lot of equivalences with some others structures, such that Graph theory, Groups, e ever we loking enumeration questions. Certains proprieties of latin squares, such ortogonality will be worked. And we finish with aplications to the Algebric Code Theory.

Key words: latin squares; mutually orthogonal latin squares; MOLS; hipercubes; MDS Codes.

Sumário

Capítulo 1

Introdução a teoria dos quadrados latinos

Vamos iniciar este trabalho dando algumas motivações a respeito da teoria dos quadrados latinos. Por exemplo vamos imaginar que que queremos plantar três variedades de plantas(0,1 e 2) em três campos e em três meses(denotados por A,M,J). Uma forma possível de arranjar tal experimento é:

campo/mês	A	M	J
A	0	1	2
B	0	1	2
C	0	1	2

Notemos que a variedade 0 é só testada no mês de abril,a variedade 1 em maio e a 2 em junho. Uma melhor estratégia seria uma representação em que cada variedade é testada em todos os meses e em todos os campos. Tal representação seria:

campo/mês	A	M	J
A	0	1	2
B	1	2	0
C	2	0	1

Suponhamos agora que nós temos 3 tipos de fertilizantes(também denotados por 0,1 e 2). Da mesma forma do anterior nós usaremos 2 quadrados, um para representar as variedades de plantas, outro para representar as variedades de fertilizantes. A pergunta agora é se é possível testar todas as nove combinações possíveis de variedades de planta/fertilizante exatamente uma vez? Na verdade a resposta é sim, e também o quadrado acima é um exemplo de um quadrado latino de ordem 3 e a resposta da pergunta é possível desde que exista um par de quadrados latinos com uma certa propriedade. De fato, quadrados desta forma apresentam uma estrutura combinatorial muito singular,e dela derivam-se muitas propriedades e aplicações. Ademais, há resultados que são influenciados por várias áreas dentro e fora da combinatória, essa teoria envolve a álgebra, geometria finita, estatística e outras. Entre elas à teoria dos códigos, criptografia, geometria finita e estatística.

A primeira vez de que se tem registro de que alguém pensou em quadrados latinos foi em 1639 em um jogo de cartas. O primeiro matemático que publicou um texto sobre quadrados latinos foi Leonhard Euler em 1783, texto que se referia à aplicações à estatística. O nome quadrados latinos se dá ao fato de que Euler usou letras latinas para os seus quadrados nesta obra.

Vamos, neste trabalho obter resultados e trabalharmos focados em questões enumerativas, que deveras é uma parte muito importante desta teoria. No segundo capítulo deste trabalho daremos os conceitos fundamentais de quadrados latinos;no terceiro faremos algumas construções e relaciona-

remos um quadrado latino à um grafo. No quarto capítulo abordaremos questões enumerativas e construtivas de uma estrutura chamada quadrados latinos mutualmente ortogonais;no quinto faremos uma exposição sobre as relações existentes entre a estrutura de grupos finitos e estrutura de quadrados latinos No sexto capítulo falaremos sobre uma generalização de quadrados latinos, que são os hipercubos. E no último capítulo entraremos em questões associadas à teoria dos códigos algébricos,como uma aplicação de tais conceitos estudados anteriormente.

Capítulo 2

Quadrados latinos:conceitos

Neste capítulos usaremos a referência [3], [4], [6], [7] e [8]

Definição 2.0.1 *Um quadrado latino de ordem n é uma quádrupla (R, C, S, L) onde R, C, S são conjuntos de cardinalidade n e L é uma aplicação $L : R \times C \longrightarrow S$ tal que para cada i de R e j de C, a equação $L(i, j) = x$ tem uma única solução, isto é, fixando qualquer duas coordenadas de (i, j, x) encontraremos a terceira de forma única.*

De forma, mentalmente, mais sintética um quadrado latino é um arranjo $n \times n$ onde em uma determinada linha i e coluna j o elemento $i * j$ não se repete nesta mesma linha e na mesma coluna.

Como $R, C, S = X$, abreviaremos a quádrupla $(X, X, X, *)$ para $(X, *)$. Um exemplo de um quadrado latino de ordem 3 é:

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array}$$

Proposição 2.0.1 *Para qualquer n, existe um quadrado latino de ordem n*

Demonstração: Para provar este simples resultado consideremos os inteiros $0, 1, ..., n-1$ como a primeira linha do quadrado $n \times n$,assim na próxima linha transladamos para a esquerda os elementos $1, 2, ..., n-1$ e podemos continuar este processo até a última linha sem que em cada linha i e a coluna j, o elemento $i * j$ não se repete nesta linha e coluna;

Desta forma, temos o quadrado latino:

$$L = \begin{matrix} 0 & 1 & \cdots & n-1 \\ 1 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ n-1 & 0 & \cdots & 1 \end{matrix}$$

□

Notemos que esse quadrado corresponde a tabela $(\mathbb{Z}_{\ltimes}, +)$. Tal fato nos leva a pensar na relação da teoria de quadrados latinos e a teoria dos grupos, existe um teorema que liga estas teorias, assunto que abordaremos um pouco mais à frente.

Capítulo 3

Enumeração e grafos

Neste capítulo faremos uso das referências [4],[7],[8] e [9].

A próxima questão a ser discutida é se dado $n > 1$ quantos quadrados latinos de ordem n existem. Para isto denotamos L_n como sendo o número de quadrados latinos distintos de ordem n e também l_n como sendo o número de quadrados latinos reduzidos de ordem n, onde um quadrado latino reduzido de ordem n é um quadrado latino onde a primeira linha e primeira coluna é arranjada da seguinte forma $012...n-1$.

É óbvio que utilizando L_n para calcular l_n o grau de liberdade das entradas de dos quadrados latinos caem muito e encontraremos $L_n = L_n(l_n)$;porém avaliar l_n não é nada fácil, decerto, como comentaremos em breve, o número l_n é um tanto caótico e não existe uma fórmula fechada para calculá-lo até agora.

Teorema 3.0.1 *Para cada $n > 1$ o número L_n é dado por:*

$$L_n = n!(n-1)!l_n$$

Demonstração: Dado um quadrado latino de ordem n, podemos permutar as suas n colunas de $n!$ maneiras, de modo que o quadrado resultante ainda

seja um quadrado latino. Analogamente depois de permutar as colunas podemos pemutar as últimas $n-1$ linhas de $(n-1)!$ maneiras. De maneira que cada um destes quadrados ainda vão ser quadrados latinos e distintos (como matrizes), isto é verdade desde que na permutação das linhas, a primeira não seja desarranjada. Então, começando com um quadrado latino reduzido de ordem n podemos fazer $n!$ permutações nas colunas e $(n-1)!$ nas linhas, que resultariam em $n!(n-1)!$ quadrados latinos de ordem n, e exatamente um destes vai ser reduzido. Assim $L_n = n!(n-1)!l_n$.

□

Porém encontrar uma fórmula explícita para L_n a partir de l_n, isto é, $L_n = L_n(l_n)$ ainda não é muito prático no sentido de que precisamos calcular previamente o número l_n, e este revela-se um problema desafiador.

De fato não existe ainda uma relação explícita entre $n-1$ e n. Para nos convencermos de tal caoticidade basta analisarmos a tabela:

n	l_n
2	1
3	1
4	4
5	56
6	9408
7	16942080
8	535281401856
9	377597570964258816
10	7580721483160132811489280
11	5.36×10^{33}
12	1.62×10^{44}
13	2.51×10^{56}
14	2.33×10^{70}
15	1.5×10^{86}

Até hoje são apenas conhecidos os valores exatos de l_n para $2 \leq n \leq 11$, e para $12 \leq n \leq 15$, existem apenas estimativas usando métodos probabilísticos para tal. Notemos que para l_{15} é avaliado como sendo $1,5 \times 10^{86}$, para termos idéia de tal magnitude, o número de átomos no universo visível é estimado em 4×10^{78}. Dessa maneira seria possível inscrever milhões de quadrados latinos reduzidos de ordem 15 em cada átomo do universo.

Continuando ainda na questão de enumeração de quadrados latinos, estudaremos suas relações com a teoria dos grafos, que de certo modo torna-se muito estreita.

Definição 3.0.2 *Um grafo G consiste em um conjunto de vértices V, conjunto de arestas E e uma aplicação associando cada aresta $e \in E$ a um par,*

a priori, não ordenado x,y(estes chamados de pontos finais).

A conexão entre a simples estrutura dos grafos e a instigante estrutura dos quadrados latinos, inicialmente não parece ser óbvia. Para atingir tal objetivo tomaremos bastante cuidado em conceitos, nos quais os seguiremos ao pé da letra. Necessitaremos de algumas definições,descritas logo abaixo:

Definição 3.0.3 *Um grafo bipartido é um grafo $G = (V, E)$ onde o conjunto de vértices V é particionado em dois conjuntos: $U = \{u_1, u_2, ..., u_m\}$ e $W = \{w_1, w_2, ..., w_n\}$, tal que toda aresta é do tipo $\{u_i, w_j\}$.*

Vamos agora construir um grafo bipartido a partir de um quadrado latino. Seja $\sharp U = \sharp V$ e U e W representam respectivamente, as linhas e colunas de um quadrado latino L de ordem n. Se o símbolo na posição (i, j) é k, então uma aresta de cor $k = 1, 2, ..., n$ junta os vértices i e j, e como L é um quadrado latino, claramente $L = (V = (U \cup V), E)$ é um grafo bipartido. De fato faremos uma apologia ao abuso de notação, hora referindo-se a L como um quadrado latino, hora referindo-se a $L = (V = (U \cup V), E)$ como um grafo bipartido. Ademais um grafo bipartido em que $\sharp U = \sharp V = n$ e todo vértice de U é ligado à todo todo vértice em W é representado $K_{n,n}$. No caso relevante à teoria dos quadrados latinos as arestas num $K_{n,n}$ são coloridas de uma das n cores tal que cada vértice tem exatamente uma aresta de cada cor incidindo nele.

Definição 3.0.4 *Um 1-Fator de um grafo G é um grafo cujo o conjunto de vértices é o próprio conjunto V e cujo o conjunto das arestas é um subconjunto de E tal que cada vértice tem exatamente uma aresta incidindo nele. Se E pode ser particionado em subconjuntos disjuntos tal que cada subconjunto decompõe G em um 1-Fator, G é dito ser 1-Favorável.*

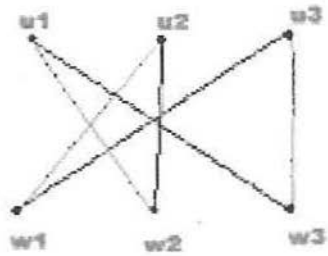


Figura 3.1: Grafo G e sua 1-fatoração.

O exemplo acima ilustra de um esquema de um grafo bipartido G e sua *1-fatoração* com $\sharp U = \sharp W = 3$.

Proposição 3.0.2 *A existência de um quadrado latino G de ordem n é equivalente a uma 1-fatoração de um grafo do tipo $K_{n,n}$*

Demonstração: Seja L um quadrado latino de ordem n e $U, W \subset V$ tal que $V = U \cup W$ e também U representa as linhas de L e W representa as colunas de L,digamos, $U = \{a_1, a_2, ..., a_n\}$ e $W = \{b_1, b_2, ..., b_n\}$. Se o símbolo na posição (i, j) é k, então uma aresta de cor k junta a_i a a_j. Assim cada vértice tem uma aresta de cada cor incidindo nele. Lembrando que L é um quadrado latino, cada símbolo k cria um *1-fator* monocromático,isto é, um *1-fator* cujas arestas são todas da mesma cor.

Reciprocamente, tomemos G um grafo do tipo $K_{n,n}$ cujas arestas são coloridas, cada uma, com uma das n cores e tal que exista uma fatoração de G em *1-fatores* monocromáticos. A construção de L segue a regra: colocamos o símbolo k na posição (i, j) de um quadrado $n \times n$ se existe uma aresta de

cor k juntando os vértices i e j; isto é sempre possível pois o grafo é do tipo $K_{n,n}$. E também é verdade que cada linha e coluna contém cada símbolo exatamente uma vez;pois se supomos que na linha i,k apareça duas vezes, como o grafo é *1-fatorável* isto não é possível,e analogamente no caso das colunas.

□

Para ilustrar este importante teorema, tomemos

$$L = \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

A equivalência do quadrado latino L traduzida na linguagem dos grafos já foi a feita na figura anterior.

Definiremos agora algo que é naturalmente relacionado aos quadrados latinos, a saber os $r \times n$ retângulos latinos.

Definição 3.0.5 *Dados inteiros r e n, com $r \leq n$, um $r \times n$ retângulo latino é um arranjo com r linhas e n colunas, tal que em cada linha e coluna os elementos não se repetem.*

Como um quadrado latino está relacionado a uma *1-fatoração* de um grafo $K_{n,n}$, um $r \times n$ retângulo latino também pode ser relacionado a um grafo $K_{r,n}$ de n cores distintas.

Usando este fato, nós iremos estabelecer um simple mas importante resultado: qualquer $r \times n$ retângulo latino ($r < n$) pode ser completado de modo que se torne um quadrado latino de ordem n pela adição de $n - r$ colunas.

Agora vamos identificar um $r \times n$ retângulo latino R com um grafo bipartido $G(R)$ com $\sharp U = \sharp W = n$ e em que a aresta$\{u_i, w_j\}$ está presente

Exemplo 3.0.1 *Tome o retângulo latino:*

$$R = \begin{matrix} 1 & 3 & 4 & 2 & 5 \\ 4 & 1 & 3 & 5 & 2 \\ 2 & 4 & 5 & 1 & 3 \end{matrix}$$

O retângulo R é equivalente a determinação de um 1-fator de um grafo bipartido associado, conforme a maneira descrita acima. No exemplo acima a linha (3 5 2 4 1) *é obtida como sendo a quarta linha de um apropriado 1-fator de um grafo $G(R)$ como mostra a figura abaixo:*

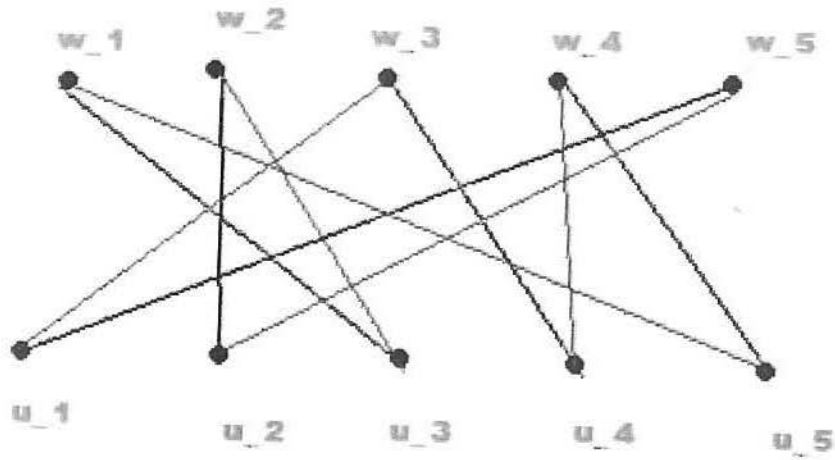


Figura 3.2: constuções de novas linhas de um quadrado latino a partir de 1-fatores de um grafo bipartipo G(R).

Observação 3.0.1 *No exemplo acima adicionamos uma linha a R que foi obtida pelo 1-fator do grafo correspondente $G(R)$; esta linha pode entrar em qualquer ordem nas demais que faltam, ainda fazendo do retângulo latino um*

quadrado latino; pois se adicionando uma linha tal que em uma coluna, o símbolo i apareça em duas colunas, então a aresta $\{u_i, w_a\}$ *ocorre em* $G(R)$*, mas essa não pode ocorrer pois R é um retângulo latino e a também está em R; o que queremos ressaltar é que a construção feita acima, é consistente sem que necessite impor ordem alguma nas linhas remanescentes.*

Na *1-fatoração* de um grafo bipartido, cada um dos $n - r$ *1-fatores* gera uma linha adicional no retângulo latino. Tomando estas linhas adicionais, levamos o retângulo latino à um quadrado latino. Como vimos, a construção descrita acima é feita de modo que a aresta $\{u_i, w_j\}$ está presente no grafo associado $G(R)$ se falta o elemento j na coluna i. Seguindo a estratégia as fatorações associadas ao grafo constitui uma maneira de adicionar $n - r$ linhas ao retângulo latino e transformando-o em um quadrado latino. Para provar que o quadrado resultante é um quadrado latino, precisamos de um lema.

Lema 3.0.1 *Em um* $r \times n$ *retângulo latino, com* $r < n$ *existe ao menos k símbolos não aparecendo em qualquer conjunto de* $k \leq n$ *colunas*

Demonstração: Tomemos $S_i, i = 1, 2, ..., n$ como o conjunto dos $n - r$ símbolos que não aparecem na coluna i de R.Cada símbolo ocorre exatamente 1 vez em cada linha de R, com o total de r ocorrências, de modo que cada símbolo é ausente em $n-r$ colunas. Se $k, 1 \leq k \leq n$, colunas são selecionadas, a associação com S_i vão conter no máximo $k(n - r)$ símbolos, ou seja, cada S_i tem $n-r$ símbolos e juntando com as k colunas temos o total de $k(n-r)$ símbolos não necessariamente distintos. Desde que cada símbolo ocorre $n-r$ vezes entre todas os conjuntos, nenhum símbolo ocorre mais do que $n-r$ vezes entre os $k's$ $S_i's$ selecionados. Em outras palavras o Lema diz que qualquer conjunto de k $u_i's$ são adjacentes a m dos $w_j's$ onde $k \leq m$ No exemplo 2.0.1 se

$k = 3$ as colunas 1,2 e 3 admitem quatro símbolos distintos ausentes, a saber: $5, 3, 1, 2$ e analogamente podemos tomar as outras possibilidades restantes. Agora vamos provar o mais importante teorema até agora.

□

Teorema 3.0.2 *Sejam $r < n$ um inteiros positivos. Dado um $r \times n$ retângulo latino, uma linha adicional pode sempre ser aderida a ele tornando-o um $(r + 1) \times n$ retângulo latino R'*

Demonstração: Consideremos o grafo bipartido $G(R)$ associado a R e notemos que para qualquer vértice u_i nós podemos sempre encontrar uma aresta que liga u_i a algum w_j. Para encontrar um *1-fator* de $G(R)$ usaremos indução finita sobre o conjunto de vértices $U \subset V$. Feito assim, poderemos adicionar uma nova linha ao retângulo latino, esta linha será, como já fora comentado, a *1-fatoração* encontrada. O caso $n = 1$ é absolutamente trivial.Assumiremos que para cada vértice em um conjunto de l $u_i's$, nós podemos encontrar uma aresta que liga u_{ia} a um único w_j. Agora tomemos um conjunto qualquer de cardinalidade $l + 1$ dos $u_i's$ e removemos uma aresta, digamos, (u_p, w_p). Então depois de remover os vértices u_p e w_p, as mesmas condições estão asseguradas, e por hipótese de indução finita, existe um *1-fator* envolvendo os l $u_i's$ que sobraram. Assumimos agora que alguma coleção de k dos $u_i's$ são adjacentes a k $w_j's$, onde $k < l$. Pela hipótese indutiva, uma aresta pode ser encontrada, tal que ela liga cada u_i à um único w_j. Assim sobraram $l + 1 - k$ dos $u_i's$ para se encontrar com os apropriados $w_j's$. Entre estes $l + 1 - k$ $u_i's$, qualquer subconjunto de cardinalidade h são adjacentes a não menos que h dos $w_j's$ remanescentes. Se não, este subconjunto de cardinalidade h junto com os $k's$ $u_i's$ já encontraram-se com os $w_j's$ correspondentes em menos de $h + k$ ocasiões, violando o lema anterior. Assim, por hipótese de indução,

estes remanescentes $l+1-k$ dos $u_i's$ também podem ser encontrados com os apropriados $w_j's$, e a *1-fatoração* de $G(R)$ está completa. Agora podemos estabelecer o esperado resultado que segue do teorema acima:

□

Corolário 3.0.1 *Se $r < n$ qualquer retângulo $r \times n$ pode ser completado a um quadrado latino de ordem n, pela adição de $n - r$ linhas.*

Nós estabelecemos resultados elementares que permeiam a teoria dos grafos, porém ainda nada citamos sobre essa teoria a respeito de enumeração de quadrados latinos. Para iniciar a questão enumerativa acima teremos que ter em mente as construções descritas anteriormente neste capítulo. Agora vamos continuar nossas considerações a respeito de questões sobre enumeração de quadrados latinos. No tópico as construções que devemos fazer são brevemente descritas. Consideremos R um $r \times n$ retângulo latino. Associemos a ele um grafo k-regular bipartido $G = G(R)$ com $V(G) = C \cup S$, onde $C = \{c_1, c_2, ..., c_n\}$, $S = \{s_1, s_2, ..., s_n\}$ e $E(G) = \{c_i s_j;$ coluna i contém símbolo $j\}$. Nós vamos chamar este grafo de fôrma de R. Claramente, muitos retângulos latinos admitem a mesma fôrma, por exemplo quando $k = n$, todo quadrado latino tem $K_{n,n}$ como fôrma.

Para qualquer fôrma G, denote por $N(G)$ o número de *1-fatoração* de G, ou equivalentemente o número de quadrados latinos reduzidos que tem G como fôrma. Calculamos $N(G)$ usando a recursão:

$$N(G) = \sum_F N(G - F) \qquad (1)$$

;onde a soma é feita sobre os *1-fatores* F de G que contém alguma aresta fixada de G.

Observação 3.0.2 *O cálculo descrito em (1) é meramente computacional, e é mostrado como uma forma simples e factível de se calcular $N(G)$. As contruções descritas logo após são tiradas da referência [7], onde é apresentado um embasamento teórico que possibilita a implementação de algoritimos para calcular l_{10} e l_{11}.*

Observemos também que se G_1 e G_2 são grafos isomorfos, $N(G_1) = N(G_2)$. Em outras palavras $N(G)$ é invariante sob classe de isomorfismo de G; desta forma, precisamos apenas aplicar (1) em um representante de uma classe de isomorfismo de G.

No próximo teorema, mostraremos que basta apenas conhecer o número $N(G)$, restritos aos bipartidos G de grau r, isto é, cada vértice de G se liga a k outros vértices do outro lado, para conhecer o número de retângulos latinos com n linhas e r colunas.

Definição 3.0.6 *Dados os inteiros n e r com $n \leq r$, denotamos $l(r, n)$ como sendo o número de $r \times n$ retângulos latinos*

Teorema 3.0.3 *A seguinte igualdade vale:*

$$l(r, n) = 2nr!(n - r)! \sum_{G} \frac{N(G)}{\sharp Aut(G)}$$

, onde $Aut(G)$ é o grupo de automorfismos de G **Demonstração:** *Consideremos G uma fôrma como descrita na teoria acima, de fato G é bipartido e tem $2n$ vértices, e também cada vértice se liga a r outros vértices. Muitos retângulos latinos tem a mesma fôrma G, como por exemplo basta mudar a ordem de entrada dos símbolos por coluna, desde que ainda isto seja factível. Pelo Corolário 2.0.1, $n - r$ linhas podem ser adicionadas à um retângulo latino tornando ele um quadrado latino de ordem n. Olhando agora para o número $N(G)$, consideremos um quadrado latino reduzido de ordem n, posso*

adicionar $n-r$ *linhas à ele de* $(n-r)!$ *maneiras, bastando apenas permutar as últimas* $n-r$ *linhas.Olhando agora para a fôrma* G *de grau* k*, temos* $(2nr)!$ *possibilidades de ligação de arestas;e pelos comentários acima, a menos de classe de isomorfismo,* $l(r,n) = 2nr!(n-r)!\sum_{G} \frac{N(G)}{\sharp Aut(G)}$

□

No caso $k = n$ *teremos* $l(n,n) = 2nn!\frac{N(K}{\sharp Aut(K_{n,n})}$*. Logo abaixo temos uma tabela completa para* $n = 1, 2, ..., k$ *e* $k = 1, 2, ..., 10$

n	k	$l(k,n)$	n	k	$l(k,n)$
1	1	1	7	1	1
2	1	1		2	309
	2	1		3	35792
3	1	1		4	1293216
	2	1		5	11270400
	3	1		6	16942080
4	1	1		7	16942080
	2	3	8	1	1
	3	4		2	2119
	4	4		3	1673792
5	1	1		4	420909504
	2	11		5	27206658048
	3	46		6	335390189568
	4	56		7	535281401856
	5	56		8	535281401856
6	1	1			
	2	53			
	3	1064			
	4	6552			
	5	9408			
	6	9408			

n	K	$l(n,k)$
9	1	1
	2	16687
	3	103443808
	4	207624560256
	5	112681643083776
	6	12952605404381184
	7	224382967916691456
	8	377597570964258816
	9	377597570964258816
10	1	1
	2	148329
	3	8154999232
	4	147174521059584
	5	746988383076286464
	6	870735405591003709440
	7	177144296983054185922560
	8	429203942159185427300352O
	9	75807214831601328114892800
	10	75807214831601328114892800

Como comentamos, estes métodos são para efeitos computacionais, para especificamente os cálculos de l_1 até l_{11}, em que cada instância requer alguns dias de cálculos em um sistema bem potente para os dias de hoje. Para obter o número total de retângulos latinos, não necessariamente reduzidos basta multiplicar $l(n,k)$ por $\frac{n!(n-1)!}{(n-k)!}$. A demonstração deste fato segue abaixo, notemos que esta é uma generalização do teorema 2.0.2, e a sua

demonstração é feita nos mesmos moldes.

Teorema 3.0.4 *O número total de retângulos latinos $L(n,k)$ em função de $l(n,k)$ é dado por:*

$$L(n,k) = \left(\frac{n!(n-1)!}{(n-k)!}\right) l(n,k)$$

Demonstração: Consideremos R um retângulo latino de ordem $k \times n$, a partir de R podemos fazer permutações nos símbolos das n colunas de maneira que resultariam em $n!$ novos retângulos latinos, e é claro também podemos permutar as $(n-1)$ deste retângulo completado(a um quadrado latino), dentre as $(n-1)!$; o que resultariam em $\frac{n!}{(n-k)!}$ novos retângulos, de modo que os retângulos resultantes ainda sejam retângulos latinos. É claro também que apenas um destes novos retângulos seja reduzido;desta maneira teremos para cada n e $k \leq n$,

$$L(k,n) = (\frac{n!(n-1)!}{(n-k)!}) l(n,k)$$

□

3.1 Estruturas computacionais

Agora vamos comentar sobre algumas estimativas feitas a partir das construções desenvolvidas neste capítulo. Suponhamos que nós queremos gerar um quadrado latino aleatório com colunas $R_1, ..., R_n$ pelo seguinte processo:R_1 é a primeira coluna de um quadrado latino reduzido. Para $i = 2, ..., n$,R_i é escolhido uniformemente de forma aleatória entre todas as extensões de $[R_1, ..., R_{i-1}]$ em que tem i na primeira posição. Para $i = 1, ..., n-1$,tomemos e_i sendo o número total de extensões de $[R_1, ..., R_{i-1}]$. Então é facil mostrar

que $e_1e_2...e_n$ é um estimador imparcial para $l(n,n)$. (Este é um exemplo de um método originalmente creditado à Knuth.)

As próximas construções deste capítulo são feitas a partir de artigos que se dispõe a calcular o número l_{11} determinísticamente;e mostrar que o número de quadrados latinos de ordem n é divisível por $f!$, onde é um inteiro próximo de $\frac{n}{2}$, e também dar uma fórmula para o número de quadrados latinos em termos de permanentes de $(+1,-1)$-matrizes.

A determinação de $l(n,k)$, especialmente no caso $k=n$,é buscado a muito tempo. O número de quadrados latinos reduzidos de ordem até 5 foi conhecido por Euler e Cayley. MacMahon usou um diferente método para encontrar os mesmos números, mas obteve um valor errado no caso $n=5$. O número de quadrados latinos reduzidos de ordem 6 foi encontrado por Frolov e mais tarde por Tarry. Frolov também deu um valor incorreto do número de quadrados latinos reduzidos de ordem 7. Norton enumerou os quadrados latinos de ordem 7, mas incompletamente;este foi corrigido por Sade e Saxena. Para $n=8$, $l(8,8)$ foi encontrado por Wells, e $l(9,9)$ foi determinado por Bammel e Rothstein.

O valor l_{10} foi primeiramente encontrado em 1990 pelo matemático amador Eric Rogoyski, trabalhando em seu computador em casa, e no ano de 1991 por Brendan D. MAcKay. Antes de sua morte em 2002, Rogoyski trabalhou muitos anos em quadrados de ordem 11, obtendo avanços computacionais, que agora possibilitam calcular de $n=1$ até $n=11$ de forma moderadamente rápida.

Agora vamos descrever explicitamente o algoritmo. A construção a ser brevemente descrita agora é muito parecida com a feita após o Corolário 2.0.1. Na verdade esta vai incrementar de forma ímpar a anterior. Dado um $k \times n$ retângulo latino R, nós podemos definir um grafo bipartido $G(R)$

com vértices $C \cup S$, onde $C = \{c_1, c_2, ..., c_n\}$ representa as colunas de R e $S = \{s_1, s_2, ..., s_n\}$ representa os símbolos. Existe uma aresta de c_i para s_j se somente se o símbolo j aparece na coluna i de R. Então $G(R)$ é regular de grau k. Claramente $G(R)$ não determina R em geral, desde que ele não registra a ordem de entrada dos símbolos em cada coluna;este comentário foi largamente abordado nas descrições feitas anteriormente.

Dado um grafo regular bipartido G de vértices $C \cup S$ de grau k, tomemos $m(G)$ como sendo o número de *1-fatorações*. Obviamente $m(G)$ é invariante sob classe de isomorfismo de G. Assim tomemos $Aut(G)$ como sendo o grupo de automorfismo de G e tomemos B(k,n) como sendo o conjunto consistindo de um representante das classes de isomorfismo do grafo bipartido G sobre $C \cup S$ de grau k.

Assim nós podemos reformular o teorema 2.0.5 desta maneira:

Teorema 3.1.1 *O número de $k \times n$ retângulos latinos é dado por:*

$$l(k,n) = 2nk!(n-k)! \sum_{G \in B(k,n)} \frac{m(G)}{\sharp Aut(G)}$$

O número de quadrados latinos reduzidos de ordem n é dado por:

$$l_n = k!(n-k)! \sum_{G \in B(k,n)} \frac{m(G)m(\overline{G})}{\sharp Aut(G)}$$

, onde $1 \leq k < n$, e $\overline{G}$ é o complemento de G em $K_{n,n}$

Observação 3.1.1 *Para termos algumas noções sobre a magnitude e caoticidade do número de grafos em $B(k,11)$, notemos que alguns termos dessa sequência são $1, 14, 4196, 2806508 e 78322916$, para $k = 1, ...5$, respectivamente. O tempo de execução da implementação para $k = 5$ é de 2 anos(para um processador PentiumIII de 1 GHZ), mas pode ser completado em aproximadamente 2 meses se forem disponibilizados o uso de 3 GB de memória.*

Agora discutiremos algumas proriedades de divisibilidade de l_n. Obtendo o mesmo valor para l_n usando a parte 2 do teorema anterior, para diferentes valores de k, nós podemos conferir a validade dos resultados obtidos a partir do uso de um simples teorema:

Teorema 3.1.2 *Para cada inteiro* $n \geq 1$,

l_{2n+1} *é divisível pelo* $mdc(n!(n-1)!l_n, (n+1)!)$ *e* l_{2n} *é divisível por* $n!$.

Demonstração: Consideremos l_{2n+1} primeiro. Definamos uma relação de equivalência no conjunto de quadrados latinos reduzidos de ordem $2n+1$ tal que cada classe de equivalência ou tem o tamanho $n!(n+1)l_n$ ou $(n+1)!$. Seja $R = (r_{ij})$, um quadrado latino de ordem $2n+1$ e tomemos $A = (r_{ij})$ um menor principal de $R = (r_{ij})$ de ordem n.

Se A é um quadrado latino, então os quadrados equivalentes a R são aqueles obtidos por possíveis trocas de A por outros quadrados latinos, permutando as n linhas parciais $(l_{i,n+1}, ..., l_{i,2n+1})$ para $1 \leq i \leq n$ e também permutando as $n-1$ colunas parciais $(l_{n+1,j}, ..., l_{2n+1,j})$ para $2 \leq j \leq n$ então permutando as colunas $n+1, n+2, ..., 2n+1$ colocando elas em ordem natural. Estas $n!(n-1)!l_n$ operações são fechadas sob composição e dados diferentes quadrados latinos, a classe de equivalência tem tamanho $n!(n-1)!l_n$.

Se A não é um subquadrado latino, os quadrados equivalentes a L são aqueles obtidos aplicando uma das $(n=1)$ isomorfismos em que cada permutação fixa cada um dos pontos $1, 2, ..., n$. Nenhum isomorfismo desta forma pode ser um automorfismo de um quadrado em que A não é um subquadrado. Logo os quadrados obtidos são diferentes e essa classe de equivalência tem $(n-1)$ elementos.

O caso de l_{2n} é igual exceto ao segundo argumento que dá $(n-1)!$ permutações.

□

Ainda continuando na questão de enumerabilidade de quadrados latinos, vamos demonstrar uma nova fórmula para o número l_n, agora ultilizando a teoria de permanentes.

Por definiçao, dada uma matriz $X \in R^{n\times n}$,

$$Per(X) = \sum_{\sigma\in S_n} T_\sigma$$

, onde S_n é o grupo das permutações de ordem n e $T_\sigma = x_{1\sigma(1)}x_{2\sigma(2)}...x_{n\sigma(n)}$.Na verdade, calcular $Per(X)$ é como o determinante da matriz X sem os sinais da permutação.

Teorema 3.1.3 *Seja $p(z)$ um polinômio mônico qualquer(com coeficientes em $\mathbb{R}$)de grau n e seja também M_n a família das matrizes $n \times n$ sobre $\{-1, +1\}$. Então*

$$l_n = 2^{-n^2} \sum_{X\in M_n} p(Per(X))\pi(X)$$

Demonstração: Seja $X = (x_{ij})$ uma matriz $n \times n$ em M_n, pela definição de permanentes, $Per(X) = \sum_{\sigma\in S_n} T_\sigma$, onde S_n é o grupo das permutações de ordem n e $T_\sigma = x_{1\sigma(1)}...x_{n\sigma(n)}$. Se o polinômio $p(Per(X))$ é expandido em termos dos monômios em x_{ij}, então os únicos monômios envolvendo todo x_{ij} vem do produto $T_{\sigma 1}T_{\sigma 2}...T_{\sigma n}$, onde as permutações $\sigma_1, \sigma_2, ..., \sigma_n$ são as linhas de um quadrado latino. Então o coeficiente de um único monômio com cada x_{ij} tendo grau ímpar é o número de quadrados latinos de ordem n. Multiplicando por $\pi(X)$, volta a ser o esperado monômio sem os indesejáveis sinais negativos, e somente um tem grau par em cada x_{ij}. Agora somando sobre todos os $X \in M_n$, e multiplicando por 2^{-n^2}, (pois $\sharp M_n = 2^{n^2}$), os monômios indesejáveis se cancelam.

□

No próximo capítulo vamos abordar a questão de quadrados latinos mutuamente ortogonais, que de fato é a questão mais importante deste trabalho. As razões são evidentes quando se tenta aplicar esta teoria; na teoria dos códigos algébricos. Vamos mostrar que conseguiremos alcançar um código algébrico corretível se conseguirmos um conjunto de quadrados latinos mutualmente ortogonais; e exibiremos certas condições para conseguir tal conjunto.

Capítulo 4

Quadrados latinos mutualmente ortogonais

Para capítulo usaremos as referências [4], [6], [9] e [12]

Neste capítulo nós vamos proceder construindo conjunto de quadrados latinos mutualmente ortogonais, tão grande(em cardinalidade) quanto possível. Para iniciar nossa explanação vamos começar dando uma motivação sobre tal conteúdo.

Para começar nossas considerações a respeito de quadrados latinos ortogonais, vamos inicialmente comentar o problema dos 36 oficiais,levantado por Euler, seguido de uma conjectura de sua autoria. Este problema concerne em um arranjo de 36 oficiais de 6 diferentes patentes e 6 diferentes regimentos em um quadrado de ordem 6;o problema é saber se existe apenas um oficial em cada uma das posições e em um regimento.

É claro que a solução requer dois quadrados latinos de ordem 6, em que um os símbolos representam os postos, e outro os regimentos. Suponhamos que estes 36 militares são divididos em 6 patentes:6 são tenentes, 6 capitães, 6 majores, 6 coronéis e 6 brigadeiros;e cada um destes militares

estão lotados nos seguintes postos: 1ºinfantaria, 2ºinfantaria, 25ºinfantaria, 2ºarmada, 1ºcavalaria e 101ºdivisão aérea. Se nós concatenarmos os dois dados quadrados o melhor que poderemos encontrar neste sentido é um par de quadrados latinos mutualmente ortogonais a menos de um subquadrado 2×2 em que há repetição. Agora vamos dar algumas definições a cerca desta estrutura:

Definição 4.0.1 *Dadas duas matrizes $n \times n$, $A = (a_{i,j})$ e $B = (b_{i,j})$ a matriz concatenada $C = A \odot B$ é a matriz $n \times n$ $C = (a_{i,j}, b_{i,j})$, onde cada entrada agora são pares vindo de A e B.*

Definição 4.0.2 *Um par de quadrados latinos de ordem n, $L_1 = (l_{ij})$ e $L_2 = (m_{ij})$ são ortogonais quando concaternarmos $L_1 \odot L_2$ cada par (l_{ij}, m_{ij}) ocorre uma vez em $L_1 \odot L_2$.*

De fato Euler estava correto em acreditar que não havia um par de quadrado latinos ortogonais de ordem 6, porém,ele foi mais além, conjecturando:

Conjectura 4.0.1 *(Euler)Seja n um inteiro da forma $2(2k-1)$, não existe um par de quadrados latinos ortogonais de ordem n.*

Tal conjectura foi refutada, como vamos ver mais a frente, ou seja, existe sempre quadrados latinos ortogonais de ordem n para $k > 2$. De fato esta conjectura foi apenas quebrada na década de 50. Mas em 1900 Tarry conseguiu provar, por um método exaustivo, que de fato não existia um par de quadrados latinos mutualmente ortogonais de ordem 6. Assim o problema dos 36 oficiais não admite solução.

Agora vamos estender o conceito de quadrados latinos mutualmente ortogonais para conjuntos mutualmente ortogonais.

Definição 4.0.3 *Seja $A = L_1, ...L_k$ um conjunto de quadrados latinos de ordem n. A é dito ser um conjunto mutualmente ortogonal se para cada $i \neq j$, L_i é ortogonal a L_j;e tal conjunto é denotado por MOLS(mutually orthogonal latin squares).*

Agora vamos encontrar conjuntos de MOLS cujas cardinalidades maiores possíveis. Para isto consideremos $N(n)$ como sendo o número máximo possível de MOLS de ordem n. E agora vamos dar uma limitação superior para a função $N(n)$.

Proposição 4.0.1 *Para cada $n \geq 2$, $N(n) \leq n - 1$*

Demonstração: *Os n símbolos de qualquer quadrado latino L_1pode ser permutado de qualquer maneira sem afetar a sua ortogonalidade com o quadrado L_2.Assim nós podemos reordenar os símbolos na primeira linha de cada quadrado para ser da forma:$(0, 1..., n-1)$. Suponhamos que*

$$L_1 = \begin{array}{cccc} 0 & 1 & \cdots & n-1 \\ x & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{array} \qquad L_2 = \begin{array}{cccc} 0 & 1 & \cdots & n-1 \\ y & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{array}$$

são dois membros do conjunto. Nem o símbolo x, nem y podem ser 0, de modo que L_1 e L_2 são quadrados latinos. Além do mais $x \neq y$, pois se $x = y = i$, o par (i, i) já existe na primeira linha de $L_1 \odot L_2$. Então existem no máximo $n - 1$ símbolos que podem aparecer na primeira posição da segunda linha destes quadrados que estão num conjunto ortogonal. Logo $N(n) \leq n - 1$.

□

No exemplo abaixo mostraremos um conjunto de 3 *MOLS de ordem* 4. *Um conjunto de* $n-1$ *MOLS de ordem* n *é chamado de um conjunto completo.*

Exemplo 4.0.1 *Considere os quadrados latinos:*

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{array} \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{array}$$

Por simples inspeção,eles formam um conjunto completo. Note que a cota $N(4) = 3$ *é atingida. Há uma classe infinita onde o limite superior acima,*$N(n) \leq n-1$ *é atingido, como descrito na seção seguinte.*

4.1 Potências Primas

Nesta seção vamos considerar a construção conjuntos de MOLS de ordem n *tal que* $n = p^m$, *com* p *primo. As construções que faremos estão intimamente ligadas à teoria dos corpos, pois se um conjunto de característica* p , *digamos,* F_p, *munido de operações* $+$ *e* $.$, *é corpo então* p *é primo. Este fato é o que revela a importância de* p *ser primo para nossas contruções;de fato as propriedades de corpo nos permitem dividir elementos não nulos, e é disso que nós precisamos agora.*

O primeiro resultado da seção mostra que para um $q = p^m$, *pode-se facilmente construir um conjunto completo de MOLS de ordem* q. *Esta construção é creditada ao famoso estatístico-matemático indiano R.C.Bose(1901-1987) obtida em 1938. A construção é a seguinte:coloca-se os elementos das linhas e das colunas de um quadrado latino* $q \times q$ *elementos de* F_q. *Para o*

polinômio $f(x,y)$ com coeficientes em F_q, colocamos o elemento $f(a,b)$ na intercecção da linha a com a coluna b do quadrado. Tal polinômio representa o quadrado. A fórmula de interpolação de Lagrange que cada quadrado M $q \times q$ (não necessariamente latino), é possível encontrar um polinômio $f_M(x,y)$ que o represente.Vamos agora enunciar o teorema fundamental desta seção:

Teorema 4.1.1 *Para q uma potência prima, o conjunto de polinômios da forma $f(x,y) = ax + y$ com $a \neq 0 \in F_q$ representa um conjunto completo de MOLS de ordem q.*

Observação 4.1.1 *Nesta observação vamos fazer a construção de um corpo finito;de fato isto é de extrema importância pois trabalharemos nesta seção e no capítulo de teoria dos códigos algébricos com corpos finitos.*

Dado um número primo p e $n \in Z, n \geq 1$, e considere Z_p um corpo com p elementos e $\Omega_p = \overline{F_p}$ seu fecho algébrico. tomemos $f_n(x) = x^{p^n} - x \in F_p[x]$ e também:

$F_{p^n} = \{x \in \Omega_p / x^{p^n} = x\}$

Primeiramente notemos que $\sharp F_{p^n} = p^n$, pois $\frac{df}{dx} = p^n x^{p^n - 1} - 1$, mas $p^n = 0$(pois F_q tem característica p), assim $\frac{df}{dx} = -1$, o que implica q $f_n(x)$ não tem raízes múltiplas em Ω_p e $f_n(x)$ tem todas as suas raízes em Ω_p pois ele é algebricamente fechado.

Também é importante ressaltar que F_{p^n} é corpo, e que se $x \in F_p$, $x^p = x$(pelo pequeno teorema de Fermat), assim, $x^{p^n} = x$ Se $F \sqsubseteq \Omega_p$ e $\sharp F = p^n$, então $F = F_{p^n}$ Usando o fato de que $(F \setminus 0, \circ)$ é grupo e $\sharp F \setminus 0 = p^n - 1$, implica que qualquer $x \in F$, $x^{p^n} = x$, logo $x \in F_{p^n}$, assim, $F \sqsubseteq F_{p^n}$, mas $\sharp F_{p^n} = p^n = \sharp F$, o que prova que $F = F_{p^n}$.

Outro fato importante é que F_{p^n} é uma extensão de corpos simples e o grau da extensão é n, isto é F é um espaço vetorial sobre F_p de dimensão n,

assim se α *gera* $F \setminus 0$, $[\alpha] = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$,$[F_{p^n} = F_p[\alpha] : F_p] = m$;*então* $dim_{F_p} F_{P^n} = m$ *se e somente se*$F_{p^n} \approx F_p^m$ *o que implica m=n, deste modo o grau do polinômio minimal de* α *sobre* F_p *é n, seja* $f(x)$ *esse polinômio ,* $f(x) \in F_p[x]$ *é irredutível. Se* $q(x) \in F_p[x]$ *irredutível, mônico de grau n e se existe* $\beta \in \Omega_p$ *tal que* $q(\beta) = 0$ *implica que*$[F_p[\beta] : F_p] = n$ *implicando* $\sharp F_p[\beta] = p^n$, *ou* F_{p^n} *é uma extensão simples de corpos.*

Demonstração: *Vamos mostrar primeiramente que se* $a \neq 0$, *o polinômio* $f(x, y) = ax + y$ *representa um quadrado latino de ordem q. Suponha que algum símbolo ocorre duas vezes na coluna* y_1, *digamos na posição* (x_1, y_1) *e* (x_2, y_1). *Então* $ax_1 + y_1 = ax_2 + y_1$, *e* $ax_1 = ax_2$. *Desde que* $a \neq 0$ *e usando o fato de que* F_q *é corpo para q potência de primo, então,* $x_1 = x_2$ *e então* (x_1, y_1) *e* (x_2, y_1) *são o mesmo ponto. Analogamente, se* $ax_1 + y_1 = ax_1 + y_2$, *então* $y_1 = y_2$. *Logo o polinômio* f_a *representa um quadrado latino de ordem q.*

Para mostrar que se $a \neq b$ *então* f_a *e* f_b *representam quadrados latinos ortogonais, suponhamos que* (x_1, y_1) *e* (x_2, y_2) *são duas posições exibindo o mesmo par ordenado e depois de concatenar temos:*

$$ax_1 + y_1 = ax_2 + y_2$$

$$bx_1 + y_1 = bx_2 + y_2$$

Assim teremos $ax_1 - by_1 = ax_2 - bx_2$, *e então como* $a \neq b$, $x_1 = x_2$ *e da expressão acima resulta* $y_1 = y_2$. *Isto mostra que os quadrados* f_a *e* f_b *são ortogonais.*

□

A construção acima descrita pode sempre ser usada para construir conjuntos de MOLS de uma dada ordem q, como por exemplo:

Exemplo 4.1.1 *Seguindo a construção acima, considere os quadrados* L_1 *e* L_2*:*

$$L_1 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix} \qquad L_2 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}$$

L_2 *é representado pelo polinômio* $x + y$*, enquanto* L_1 *é representado por* $2x + y$*, ambos sobre o corpo* Z_3*. O próximo exemplo ilustra o caso da menor potência prima* q *que não é um número primo,* $q = 4$*.*

Exemplo 4.1.2 *Para construir um conjunto completo de* 3 *MOLS de ordem* 4*, nós precisaremos atuar sobre o corpo* $F_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$*. Onde* α *denota uma raíz de um polinômio irredutível sobre* F_2*,* $x^2 + x + 1$*, como descrito na última observação. Aplicando o teorema acima, obtemos:*

$$\begin{matrix} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \end{matrix} \qquad \begin{matrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \end{matrix}$$

$$\begin{matrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \end{matrix}$$

que são representados , respectivamente, pelos polinômios $x + y$*,* $\alpha x + y$*,* $(\alpha + 1)x + y$ *sobre* Z_4 *de* 4 *elementos. Note que se trocarmos* α*,* $\alpha + 1$ *por* 2 *e* 3 *nós teremos os mesmos* 3 *MOLS do exemplo 3.0.2.*

4.2 potências não primas

Tendo efetivamente calculado $N(n) = 1$ *quando* n *é uma potência prima, vamos agora considerar a construção de conjuntos de MOLS de ordem* n*, para um* n *arbitrário. Notemos que essa nova situação é muito diferente da outra, pelo simples fato que se* q *não é primo,* F_q *é apenas um anel com unidade e não um corpo, e assim não herdamos as importantes propriedades da teoria de corpos finitos;assim teremos que tratar este problema de uma outra maneira.*

Para começar a nossa reflexão, lembremos do problema proposto por Euler em 1779 dos 36 *oficiais. É claro que este problema tem uma solução se, e somente se, existe um par de quadrados latinos de ordem* 6*;e, de fato,* $n = 6$ *é o primeiro não-primo, que não é potência de um primo. Assim se tentarmos construir um par de MOLS de ordem* 6*, teríamos que trabalhar sobre o anel* Z_6 *que obviamente não é corpo;assim tentaríamos trabalhar com a família de polinômios* $ax + y$ *para* $a \neq 0 \in Z_6$ *aí chegaríamos num impasse pois não conseguiríamos cancelar os elementos da forma* $(a - b) \neq 0 \in Z_6$ *pois em* Z_6 *os seus elementos inversíveis são apenas os que são primos com* 6*, no caso* 1 *e* 5 *apenas;* Z_6 *é um anel com característica* 6 *com divisores de zero.*

Euler não encontrou a solução para o problema dos 36 *oficiais e falhou também em querer generalizar este fato em 1782(é a conjectura no início deste capítulo).*

Então pela conjectura de Euler $N(n) = 1$ *para* $n = 2(2k + 1)$*, para* $k \geq 0$*. Como sabemos este fato só é verdade pra* $k = 0, 1$*. Este certamente, é um fato intrigante, pois existem* 408 *quadrados latinos de ordem* 6*, e nenhum par deles é ortogonal!*

Agora para potências não-primas como $n = 10, 12, 15, 20, ...$ *nós usa-*

remos uma estratégia um tanto natural, que é uma espécie de "colagem" de MOLS de ordem menores. Nos usaremos o chamado produto de Kronecker de matrizes para tal feito.

Definição 4.2.1 *Seja $A = (a_{ij})$ um quadrado latino de ordem m e $B = (b_{ij})$ um quadrado latino de ordem n. Então o produto de Kronecker de A e B é o quadrado $mn \times mn$ $A \otimes B$, dado por*

$$A \otimes B = \begin{matrix} (a_{11}, B) & (a_{12}, B) & \cdots & (a_{1m}, B) \\ (a_{21}, B) & (a_{22}, B) & \cdots & (a_{2m}, B) \\ \vdots & \vdots & & \vdots \\ (a_{m1}, B) & (a_{m2}, B) & \cdots & (a_{mn}, B) \end{matrix}$$

onde cada entrada a de $A, (a, B)$ é uma matriz $n \times n$ dada por:

$$(a, B) = \begin{matrix} (a, b_{11}) & (a, b_{1,2}) & \cdots & (a, b_{1,n}) \\ (a, b_{2,1}) & (a, b_{2,2}) & \cdots & (a, b_{2,n}) \\ \vdots & \vdots & & \vdots \\ (a, b_{n1}) & (a, b_{n,2}) & \cdots & (a, b_{nn}) \end{matrix}$$

Tomando um exemplo do produto de Kronecker, para $m = 2, n = 3$:

$$A = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad B = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}$$

Então o produto de Kronecker requer a construção de um quadrado de ordem 6 cujos os elementos são pares ordenados:

$$
\begin{array}{cccccc}
00 & 01 & 02 & 10 & 11 & 12 \\
01 & 02 & 00 & 11 & 12 & 10 \\
02 & 00 & 01 & 12 & 10 & 11 \\
10 & 11 & 12 & 00 & 01 & 02 \\
11 & 10 & 10 & 01 & 02 & 00 \\
12 & 10 & 11 & 02 & 00 & 01
\end{array}
$$

É claro que que nós podemos trocar os símbolos $00, 01, 02, 10, 11, 12$*pelos símbolos* $0, 1, 2, 3, 4, 5$ *para obter um quadrado latino de ordem* 6*.*

Agora nós iremos aplicar o produto de Kronecker para construção de conjuntos de MOLS.

Teorema 4.2.1 *Se existem um par de MOLS de ordem* n *e um par de MOLS de ordem* m*, então existe um par de MOLS de ordem* mn*.*

Demonstração: *Sejam* A_1, A_2 *um par de MOLS de ordem* m *e* B_1, B_2 *outro par de MOLS de ordem* n*. Consideremos os quadrados* $C = A_1 \otimes B_1$ *e* $D = A_2 \otimes B_2$*. Provaremos que* C *e* D *são quadrados latinos. Suponhamos que um elemento de* C*,* (a, b) *repita numa mesma coluna, digamos,* j*. Como* B_1 *é um quadrado latino, isto é impossível. Da mesma forma, suponhamos que um mesmo elemento, que será denotado por* (a, b)*, ocorra duas vezes numa mesma linha. Como o dado quadrado* A_1 *é um quadrado latino, torna tal ocorrência impossível. Portanto* C_1 *é um quadrado latino; e de forma análoga se prova o mesmo para* C_2*.*

Vamos agora mostrar que C_1 *e* C_2 *formam um par de quadrados latinos ortogonais. Consideremos um par* $((a_{ij}, b_{kl}), (a_{pq}, b_{rt}))$ *vindos de* $A_1 \otimes B_1$ *e* $A_2 \otimes B_2$*, respectivamente; e suponhamos que este par se repete em* $C_1 \otimes C_2$*. Porém os pares* (a_{ij}, a_{pq}) *e* (b_{kl}, b_{rt}) *ocorrem apenas uma vez em*

$A_1 \otimes A_2$ *e* $B_1 \otimes B_2$*, respectivamente. Desta forma concluimos que o par* C_1, C_2 *formam um conjunto de quadrados latinos ortogonais.*

□

Exemplo 4.2.1 *Neste exemplo vamos construir um par de MOLS,* C_1, C_2 *de ordem* 12 *a partir de MOLS de ordem* 3 *e* 4*, que neste caso são:*

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \qquad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{array}$$

e também:

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 0 & 2 & 0 \end{array}$$

$C_1 =$

00	01	02	03	10	11	12	13	20	21	22	23
01	00	03	02	11	10	13	12				
02	03	00	01	12	13	10	11				
03	02	01	00	13	12	11	10				
10	11	12	13	20				00			
11	10	13	12								
12	13	10	11								
13	12	11	10								
20				00				10			
21											
22											
23											

$C_2 =$

00	01	02	03	10	11	12	13	20	21	22	23
02	03	00	01	12	13	10	11				
03	02	01	00	13	12	11	10				
01	00	03	02	11	10	13	12				
20	21	22	23	00				10			
22	23	20	21								
23	22	21	20								
21	20	23	22								
20				00				10			
10											

Agora nós vamos demonstrar alguns teoremas que garantem a existência de pelo menos um par de MOLS de uma dada ordem n.

Proposição 4.2.1 *Se $n \equiv 0, 1$ ou $3(mod4)$, temos $N(n) \geq 2$.*

Demonstração: *Se $n \equiv 0, 1, 3(mod4)$,então ou n é ímpar ou n é divisível por 4. Nesse caso, dada $q = q_1...q_r$, a fatoração de n em em potências primas distintas, então $Q_i \geq 3$, logo $q_i - 1 \geq 2$para cada $i = 1, ..., r$. Aplicando o Teorema3.2.1 e o Teorema3.1.1, pode-se construir pelo menos dois MOLS de ordem n.*

□

Resta analisar o caso $n \equiv 2(mod4)$, na conjectura de Euler. Assim para $n = 2(2k+1)$, a menor potência prima na fatoração de n é 2, e sabemos que $N(2) = 1$. Então o produto de Kronecker não é efetivo nesse caso. Porém fora provado que $N(10) \geq 2$ e também que $N(14) \geq 3$ e $N(18) \geq 3$. O caso geral foi provado pela primeira vez em 1960 por Bose, Shrikhande e Parker enunciado abaixo:

Teorema 4.2.2 *Para todo n, exceto 2 e 6, existe um par de MOLS de ordem n.*

Observação 4.2.1 *A demonstração deste teorema requer muitos resultados que foram tomados, especificamente, na referência [13]. Nós devemos provar $N(n) \geq 2$ para $n > 6$. Pelo teorema 13.2.2 da referência [13] é suficiente provar para o caso $n = 4t + 2$. O lema seguinte reduz a prova apenas à um número finito de valores de n.*

Lema 4.2.1 *Se $N(4t + 2) \geq 2$ para $10 \leq 4t + 2 \leq 726$, então $N(n) \geq 2$ para todo $n > 6$.*

Com o uso do Lema anterior precisaremos apenas provar que existem um par de MOLS de ordem n para $n \leq 726$. Embora este importante resultado é remetido à casos particulares, sabemos que, para estes casos, é perfeitamente possível encontrar tais pares. Porém não é simples, para isto, há de se fazer implementações computacionais.

Provaremos agora algo mais específico, como:

Teorema 4.2.3 *Tome $q_1q_2...q_r$ a fatoração de n em distintas potências primas como $q_1 < q_2 < ... < q_r$. Então $N(n) \geq q_1 - 1$*

Demonstração: *Para cada potência prima q_i na fatoração de n, podemos, pelo teorema3.1.1 construir um conjunto de $q_i - 1$ MOLS de ordem q_i. Então para cada $i \geq 2$, temos $q_i - 1 > q_1 - 1$ MOLS de ordem q_i, e repetindo o uso do produto de Kronecker teremos $q_1 - 1$ MOLS de ordem n.*

Motivados pela conjectura de Euler e na sua generalização, MacNeish conjecturou em 1922 um caso mais geral:

Conjectura 4.2.1 *Se $q_1...q_r$ é a fatoração de n em distintas potências primas com $q_1 < ... < q_r$, então $N(n) = q_1 - 1$*

Porém nós sabemos hoje que essa conjectura é falsa pra muitos valores de n, mas ainda há muitos outros valores em que permanece desconhecido se $N(n) = q_1 - 1$. Por exemplo, para $n \leq 100$, a conjectura de McNeish está aberta para $n = 63, 77, 99$.

Em cima desta conjectura existe uma outra que parecida com a conjectura de Euler, que diz que para n exceto 6 e potências de primos é possível alcançar $N(n) = q_1 - 1$. Assim veremos na tabela abaixo:

	0	1	2	3	4	5	6	7	8	9
0	-	-	1	2	3	4	1	6	7	8
10	2	10	5	12	3	4	15	16	3	18
20	4	5	3	22	4	24	4	26	5	28
30	4	30	31	5	4	5	5	36	4	4
40	7	40	5	42	5	6	4	46	5	48
50	6	5	5	52	4	5	7	7	5	58
60	4	60	4	6	63	7	5	66	5	6
70	6	70	7	72	5	5	6	6	6	78
80	9	80	8	82	6	6	6	6	7	88
90	6	7	6	6	6	6	7	96	6	8

A tabela acima traz os números $N(n)$, onde a entrada na linha x e na coluna y corresponde a $N(x + y)$.

Na tabela acima podemos ver que a conjectura citada acima está errada para muitos casos. Então existem muitos casos onde o número de MOLS dado pelo produto de Kronecker e pelo teorema3.1.1 foi excedido. Muitas outras técnicas são usadas para conseguir encontrar mais pares de MOLS, e uma delas vamos usar agora;que se trata da teoria de modelos transversais.

Proposição 4.2.2 *Para $m, n > 1$,$N(mn) \geq min\{N(n), N(m)\}$.*

Demonstração: *Basta usar o produto de kronecker para quadrados de ordem* m *e* n

□

Muitas outras técnicas são usadas para conseguir encontrar mais pares de MOLS, e uma delas vamos usar agora; que se trata da teoria de modelos transversais.

Para a prova do próximo teorema e de outros vamos primeiro definir o que é um modelo transversal.

Definição 4.2.2 *Um modelo transversal com* k *grupos de tamanho* n *e índice* λ*, denotado por* $T[k, \lambda; n]$*,é uma tripla* (X, G, A) *onde:*

i.X *é um conjunto de* kn *elementos;*

ii.$G = \{G_1, ..., G_k\}$ *é uma família de* k *conjuntos de cardinalidade* n *que forma uma partição de* X*;*

iii.A *é uma família de conjuntos de cardinalidade* k *ou simplesmente blocos tal que cada elemento em* A *intercepta cada grupo* G_i *em exatamente um elemento, e quqlquer par de elementos de grupos diferentes ocorrem em exatamente* λ *blocos em* A*.*

A conexão entre modelos transversais e conjuntos de MOLS é dada no seguinte resultado:

Teorema 4.2.4 *A existência de modelo transversal* $T[k, 1; n]$ *é equivalente a existência de um conjunto de* $k - 2$ *MOLS de ordem* n*.*

Demonstração: *Primeiramente assumimos a existência de um* $T[k, 1; n]$ *grupos* $G_1, ..., G_k$*, cujos elementos são: com* $G_h = \{x_{h1}, ..., x_{hn}\}, \quad h = 1, ..., k$ *Para um inteiro* h *com* $1 \leq h \leq k - 2$*, definimos um quadrado de ordem* n*,* $A^{(h)} = (a_{ij}^{(h)})$ *desta maneira:como* $\lambda = 1$*, para cada* $1 \leq i, j \leq n$*, então existe*

um único bloco B em $T[k, 1; n]$ que contém os elementos $x_{k-1,i}$ e $x_{k,j}$. O bloco B contém exatamente um elemento de G_k, digamos x_{hm}. Agora, definamos

$$a_{ij}^{(h)} = m$$

Para mostrar que o quadrado $A^{(h)} = (a_{ij}^{(h)})$ é um quadrado latino de ordem n, suponhamos que duas entradas na linha i são iguais. Então tem-se $(a_{ij}^{(h)}) = (a_{il}^{(h)}) = m, j \neq l$. Então existem dois blocos B_1 e B_2, tais que:

$$\{x_{hm}, x_{k-1,i}, x_{kj}\} \subset B_1 \text{ e } \{x_{hm}, x_{k-1,i}, x_{kl}\} \subset B_2$$

Desde que $x_{kj} \neq x_{kl}$ e também apenas um elemento de cada grupo pode ocorrer em cada bloco,teremos $\lambda \geq 2$, o que contradiz nossas hipóteses. Então o quadrado $A^{(h)} = (a_{ij})^{(h)}$ não tem elementos repetidos por linha, assim, por argumentos similares, temos que $A^{(h)} = (a_{ij})^{(h)}$ é um quadrado latino, para cada $h = 1, ..., k-2$.

Mostraremos agora que a família dos quadrados latinos $A^{(h)}$ são ortogonais. De fato assumindo que para algum $h \neq l$, $A^{(h)}$ e $A^{(l)}$ não são ortogonais. Então existem pares (i, j) e (u, v), tais que

$$(a_{ij}^{(h)}) = (a_{uv}^{(h)}) = d \text{ e } (a_{ij}^{(l)}) = (a_{uv}^{(l)}) = e$$

Isto implica na existência de blocos B_1, B_2, B_3, B_4 com

$$\{x_{hd}, x_{k-1,i}, x_{kj}\} \subset B_1 \text{ e } \{x_{hd}, x_{k-1,u}, x_{kv}\} \subset B_2$$

$$\{x_{le}, x_{k-1,i}, x_{kj}\} \subset B_3 \text{ e } \{x_{le}, x_{k-1,u}, x_{kv}\} \subset B_4$$

Como $\lambda = 1$, têm-se que $B_1 = B_3$ e $B_2 = B_4$. Destaq forma temos:

$$\{x_{hd}, x_{k-1,i}, x_{kj}, x_{le}\} \subset B_1 \text{ e } \{x_{hd}, x_{k-1,u}, x_{kl}, x_{le}\} \subset B_2$$

Assim x_{hd}, x_{le} ocorrem ao mesmo tempo em B_1 e B_2, o que é uma contradição. Segue que $A^{(h)}$ e $A^{(l)}$ são ortogonais.

Reciprocamente começando com um conjunto de $k-2$ MOLS de ordem n, nós podemos, refazendo a construção anterior e construir um $T[k,1;n]$.

□

Agora vamos dar um exemplo que ilustra o uso do teorema anterior:

Exemplo 4.2.2 *Consideremos um modelo transversal $T[4,1;3]$, dado por:*

$$G_1 : x_{11}x_{12}x_{13}$$

$$G_2 : x_{21}x_{22}x_{23}$$

$$G_3 : x_{31}x_{32}x_{33}$$

$$G_4 : x_{41}x_{42}x_{43}$$

e os blocos são dados por:

$$B_1 : x_{11}x_{21}x_{31}x_{41}$$

$$B_2 : x_{11}x_{22}x_{32}x_{42}$$

$$B_3 : x_{11}x_{23}x_{33}x_{43}$$

$$B_4 : x_{12}x_{21}x_{32}x_{43}$$

$$B_5 : x_{12}x_{22}x_{33}x_{41}$$

$$B_6 : x_{12}x_{23}x_{31}x_{42}$$

$$B_7 : x_{13}x_{21}x_{33}x_{42}$$

$$B_8 : x_{13}x_{22}x_{31}x_{43}$$

$$B_9 : x_{13}x_{23}x_{32}x_{41}$$

, pelo teorema3.2.6 vamos construir um par $A_{(1)}$ e $A_{(2)}$ de MOLS de ordem 3. *Deste modo vamos determinar o símbolo de coordenada $(1,1)$ para isto consideremos os elementos x_{31}, x_{41} de $T[4,1;3]$, notemos que eles ocorrem no*

bloco B_1, juntamente com x_{11}, x_{43}. Então o elemento de coordenada $(1,1)$ de $A^{(1)}$ é 1 e é o mesmo também em $A_{(2)}$. Determinado todos esses elementos têm-se:

$$A^{(1)} = \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 0 \\ 2 & 3 & 1 \end{matrix} \qquad A^{(2)} = \begin{matrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{matrix}$$

Agora vamos aplicar a teoria dos modelos transversais para construções de conjuntos de MOLS de ordem maior , vindo de conjuntos de MOLS de ordens menores. Para positivos inteiros k e λ definimos $T[k,\lambda]$ por

$$t(k,\lambda) = \{n| \ \ um \ \ T[k,\lambda;n] \ \ existe\}$$

Por exemplo, o teorema1.2.1 nos dá $q-1$ MOLS de ordem q para qualquer q potência prima q , então $q+1 \in T(k,1)$ para qualquer q potência de primo, $q \geq k-1$

Teorema 4.2.5 *Se $0 \leq s \leq t$, então*

$$N(mt+s) \geq min\{N(m), N(m+1), N(t)-1, N(s)\}$$

Observação 4.2.2 *Para a prova deste teorema considremos um resultado provado por Street em 1987:*

Teorema 4.2.6 *Seja s,m,t inteiros tais que $0 \leq s \leq t, 1 \leq m,t \in T(k+1,1)$, e $s,m,m+1 \in T(k,1)$ então $mt+s \in T(k,1)$*

Demonstração: *Se $N(m) \geq k-2$, então $m \in T(k,1)$*
$N(m+1) \geq k-2$, então $m+1 \in T(k,1)$
$N(t) \geq k-2$, então $t \in T(k+1,1)$
$N(s) \geq k-2$, então $s \in T(k,1)$

Portanto, pelo teorema anterior(Street), $mt + s \in T(k, 1)$*, logo*

$$N(mt + s) \geq k - 2$$

Capítulo 5

Grupos e quadrados latinos

Para este capítulo vamos fazer uso das referências: [1],[2], [4], [11] e [12].

Agora vamos relacionar a teoria dos quadrados latinos com a teoria dos grupos. Vamos encontrar certas condições para que certos quadrados latinos herdem as propriedades dessa teoria completa. Como já vimos um quadrado latino nem sempre é equivalente à tabela de um grupo com uma certa operação, digamos, •;porém a tabela de um grupo sempre tem a estrutura de um quadrado latino. Basta notar que os elementos do grupo nunca se repetem nas mesmas linhas e colunas de um quadrado, pois a operação • é binária e ele é associativo. Porém poderemos caracterizar um quadrado latino da seguinte forma:

Proposição 5.0.3 *Um quadrado latino L de ordem n é equivalente a uma tabela de um quasi-grupo $(A, \bullet)$ com n elementos*

Observação 5.0.3 *Na verdade um quasi-grupo finito é um quadrado latino;*

É claro que se todo quadrado latino fosse a tabela de um grupo, as nossas considerações aqui seriam bem rápidas, pois a teoria dos quadrados latinos herdariam todos os axiomas de grupo da teoria dos Grupos, que é completa

do ponto de vista da lógica matemática. Porém como já é o esperado vamos enunciar um corolário do último teorema:

Corolário 5.0.1 *A tabela de multiplicação de um grupo finito de ordem n é um quadrado latino de ordem n*

A recíproca deste corolário nem sempre é verdade, isto é, existem quadrados latinos que não representam tabelas de grupos de ordem n. Porém para distinguir como isto é possível usaremos ferramentas muito usadas na teoria dos grupos. Primeiramente se M denota um conjunto com n elementos distintos, a função $f : M \to M$ injetora(1-1), f é dita ser uma permutação. E sendo f e g permutações definidas em um conjunto M, então $h = f \circ g$ é também uma permutação de M. Denotaremos uma permutação f usando duas linhas de notação, onde a primeira linha é listada os elementos de M e a segunda as suas respectivas imagens imagens. Por exemplo $M = 1, 2, 3$, com a permutação $f : M \to M$ definida por:$f(1) = 2, f(2) = 3, f(3) = 1$. A esta permutação nos asssociamos a representação:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Agora pelo próximo teorema teremos condições de julgar quando um quadrado latino tem a estrutura de um grupo.

Observação 5.0.4 *Este teorema faz uma forte referência ao teorema de Cayley(1878), onde é afirmado que todo grupo finito de ordem n é isomorfo à um subgrupo de permutações do S_n.*

Na prova do teorema, na condição suficiente, nós trabalharemos com os elementos do quadrado latino em questão como se fosse elementos do S_n.

Teorema 5.0.7 *Um quadrado latino é a tabela de um grupo se, e somente se, a composição de duas linhas é ainda uma linha do quadrado.*

Demonstração: *Seja L um quadrado latino de ordem n então L é isomorfo a um subgrupo de permutações do S_n. Assim vamos proceder por indução sobre n.*

Se $n = 2$, representamos L da seguinte maneira:

$$\begin{array}{ccc} \bullet & a_1 & a_2 \\ a_1 & a_1^2 & a_1a_2 \\ a_2 & a_2a_1 & a_2^2 \end{array}$$

assim,

$$\begin{pmatrix} a_1 & a_2 \\ a_1^2 & a_1a_2 \end{pmatrix} \bullet \begin{pmatrix} a_1 & a_2 \\ a_1^2 & a_1a_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_{j1} & a_{j2} \end{pmatrix}$$

para $a_{j1}, a_{j2} \in \{a_1^2, a_1a_2\}$. Como $\sharp L = 2$, temos $a_1^2 = a_2^2 = e$, onde e é o elemento neutro de L Se $a_1a_2 = a_2a_1 = a_1a_{j1} = a_1^2$ então $a_{j2} = a_1a_2$, temos a primeira linha Agora se $a_1a_2 = a_2$, temos$a_{j1} = A_2a_1$ e $a_2^2 = a_1$, então $a_{j2} = a_2^2$, temos a segunda linha;e os outros casos a demonstração é direta e segue o resultado. Deste modo extendendo por indução temos para um quadrado latino de ordem n:

$\bullet$	a_1	a_2	...	a_n
a_1	a_1^2	a_1a_2	...	a_1a_n
a_2	a_2a_1	a_2^2	...	a_2a_n
$\vdots$				
a_n	a_na_1	a_na_2	...	a_n^2

e compondo as linhas i e j, temos:

$$\begin{pmatrix} a_1 & a_2 & ... & ... & a_i & a_n \\ a_ia_1 & a_ia_2 & ... & a_i^2 & ... & a_ia_n \end{pmatrix} \bullet \begin{pmatrix} a_1 & a_2 & ... & a_j & ... & a_n \\ a_ja_1 & a_ja_2 & ... & a_j^2 & ... & a_ja_n \end{pmatrix} = \begin{pmatrix} a_1 & ... & a_2 \\ a_{k1} & ... & a_{kn} \end{pmatrix}$$

, assim $a_{k1} = a_ia_k$*, e usando a hipótese indutiva, temos* $L_i \bullet L_j = L_k$

Na prática é fácil aplicar o teorema para mostrar que um tal quadrado latino não é a tabela de um grupo, para isto basta encontrar duas linhas e calcular a composta e verificar que esta composta não está no quadrado latino. Veremos isto no exemplo a seguir:

Exemplo 5.0.3 *Consideremos o quadrado latino*

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \\ 3 & 1 & 2 & 5 & 4 \\ 4 & 3 & 5 & 2 & 1 \\ 5 & 4 & 1 & 3 & 2 \end{array}$$

Agora calculando

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \bullet \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$

onde a permutação resultante não é nenhuma linha do quadrado latino.

Para mostrarmos que um quadrado latino de ordem n tem estrutura de grupo, pelo Teorema4.0.1, temos que testar as n^2 *composições possíveis. Note que isto é muito mais simples do que testar as* n^3 *igualdades do tipo:*$a \bullet (b \bullet c) = (a \bullet b) \bullet c$.

Um quadrado latino linha é um quadrado de ordem n em que cada linha é uma permutação de n elementos. Observemos também que um qua-

drado latino é um quadrado latino linha, mas a recíproca nem sempre é verdadeira. Consideremos agora o quadrado R de ordem 3,

$$\begin{array}{ccc} 2 & 1 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 2 \end{array}$$

Cada linha de R pode ser vista como a imagem de uma permutação, digamos,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Assim $(f_1, f_2, f_3) := R$, e de forma análoga podemos usar a mesma representação para qualquer quadrado que é latino por linha.

Agora estamos prontos para converter o conjunto de todos os quadrados latinos linha de ordem n em um grupo. Denotamos por RL_n o conjunto de todos os quadrados latinos linha de ordem n;e definamos também a seguinte operação $\bullet : RL_n \times RL_n \to RL_n$, tal que $M = \{1, ..., n\}, AB = (h_1, ..., h_n)$, onde $A = (f_1, ..., f_n), B = (g_1, ..., g_n)$, e $h_i(x) = f_i(g_i(x))$

Proposição 5.0.4 *$(RL_n, .)$ é um grupo de ordem $(n!)^n$*

Demonstração: *Sejam:*

$A = (f_1, ..., f_n)$, $B = (g_1, ..., g_n)$ e $C = (h_1, ..., h_n)$ elementos em RL_n

(i)A operação é associativa, pois:$A(BC) = A(h_1g_1, ..., h_ng_n) = (f_1(h_1g_1), ..., f_n(h_ng_n) = (AB)C$

(ii)para todo $A \in RL_n$ existe $E \in RL_n$ tal que $AE = EA = A$, basta tomar a matriz $E = (e, e, ..., e)$, onde e é a permutação identidade.

(iii)Para qualquer $A \in RL_n$ existe $B \in RL_n$ tal que $AB = BA = E$, basta tomar $B = (f_1^{-1}, ..., f_n^{-1})$.

por (i), (ii), e (iii), temos que RL_n é um grupo com a operação $\bullet$, agora, $\sharp RL_n = (n!)^n$, pois dado $A = (f_1, ..., f_n)$ têm-se $n!$ possibilidades em cada entrada de A, e como A tem n entradas, segue o resultado.

□

Provaremos agora uma série de teoremas que são úteis na construção de conjuntos de quadrados latinos mutuamente ortogonais.

Teorema 5.0.8 *Sejam $R \in RL_n$ e $E = (e, ..., e)$, assim E e R são ortogonais se, e somente se, R é um quadrado latino.*

Demonstração: *Como $R \in RL_n$, é suficiente provar que as colunas de R são permutações. Fixado j, basta provar que $a_{ij} \neq a_{kj}$ sempre que $i \neq k$. Na concatenação de R por E temos que o par (a_{ij}, j) aparece na linha i e coluna j, enquanto o par (a_{ik}, j) aparece na coluna k e linha i. Como R e E são ortogonais e $(i, j) \neq (k, j)$ temos $(a_{ij}, j) \neq (a_{ik}, j)$ e assim $a_{ij} \neq a_{kj}$, como queríamos.*

A outra implicação segue do fato de que, sendo R um quadrado latino, tomando o elemento a_{ij} de R, (A_{ij}, j) só pode ocorrer uma vez, e portanto R e E são mutuamente ortogonais.

Teorema 5.0.9 *Seja $\{A_1, ..., A_n\}$ um conjunto de quadrados latinos linha mutuamente ortogonais, assim para qualquer quadrado latino linha X, o conjunto $\{XA_1, ..., XA_m\}$ é um conjunto de quadrados latinos linha mutuamente ortogonais.*

Demonstração: *Vamos demonstrar que se A é ortogonal a B então XA é ortogonal a XB, desta forma suponhamos que o par (u, v) ocorre na linha n e coluna p e também na linha n e coluna q quando XA é concatenado com XB. Assim $x(m, p)$ elemento de X, $u = a(m, x(m, p)) = a(n, x(n, q))$*

e $v = b(m, x(m, p)) = b(n, x(n, q))$*, mas o par* $(a(n, x(n, q)), b(n, x(n, q)))$ *só ocorre uma vez, pois* A *é ortogonal a* B*.*

Proposição 5.0.5 *Sejam* A *e* B *dois quadrados latinos linha,* A *e* B *são ortogonais se, e somente se, existe um quadrado latino* L *tal que* $AL = B$

Demonstração: *Consideremos* $L = A^{-1}B$*, como* A *é ortogonal a* B*, pelo Teorema 5.0.13* L *é ortogonal a* E*; de modo que* L *é um quadrado latino.*

Reciprocamente, seja L *um quadrado latino tal que* $AL = B$*. Pela Proposição 4.0.12,* L *é ortogonal a* E*. Usando o teorema 5.0.13,* AL *é ortogonal a* AE*, e assim* B *é ortogonal a* A*.*

Proposição 5.0.6 *Seja* A *um quadrado latino e* m *o menor inteiro positivo tal que* A^m *não é latino, assim* $\{A, A^2, ..., A^{m-1}\} = B$ *é um conjunto ortogonal de quadrados latinos linha.*

Demonstração: *Para* j, m*,* A^j *é um quadrado latino, tomemos* $A^k \in B$*,* A^j *é ortogonal à* A^k*pois existe um quadrado latino* L*tal que* $A^j = LA^k$*, sem perda de generalidade, consideremos* j, k*, assim* $L = A^{j-k}$ *um quadrado latino.*

Corolário 5.0.2 *Se* $A, A^2, ..., A^{m-1}$ *forma um conjunto de MOLS se, e somente se todos são quadrados latinos*

Demonstração: *A condição necessária segue imediatamente do teorema anterior, a recíproca segue do fato:* A*,* A^j *são ortogonais, existe um* L*, quadrado latino tal que* $A^j = AL$ *o que acarreta* $L = A^{j-1}$*.*

Corolário 5.0.3 *Se* $A, A^2, ..., A^{m-1}$ *são quadrados latinos, então* $m - 1$ *quadrados consecutivos da coleção* $A^{-m+1}, A^{-m+2}, ..., A, ..., A^{m-1}$ *formam um conjunto de MOLS.*

Agora vamos provar o principal teorema desta seção:

Teorema 5.0.10 *Se L é um quadrado latino de ordem n, com $n = p_1^{e_1}...p_r^{e_r}$, onde $p_1 < p_2 < ... < p_r$ são primos, então o conjuto*

$$\{L, L^2, ..., L^{p_1-1}\}$$

é conjunto de MOLS de ordem n.

Demonstração: *Observemos que todos os positivos inteiros menores ou iguais a $p_1 - 1$ são relativamente primos com n, temos que $L, ..., L^{p_1-1}$ são quadrados latinos. Pelo corolário 5.0.2, eles são mutuamente ortogonais.*

Corolário 5.0.4 *Se n é primo, existe um conjunto de potências de quadrados latinos contendo um conjunto completo de $n - 1$ MOLS de ordem n*

Corolário 5.0.5 *Se n é ímpar, então existe um conjunto de potências de quadrados latinos contendo ao menos dois MOLS de ordem n*

Note que para n primo, o corolário4.0.4 nos dá um conjunto de $n-1$ MOLS de ordem n, que de fato ilustra a efeticividade da idéia de procurar conjuntos de potências de quadrados latinos para encontrar conjuntos de MOLS.

Exemplo 5.0.4 *Neste exemplo vamos utilizar o teorema anterior para construir um conjunto $\{L, L^2\}$ contendo dois MOLS de ordem 10:*

$$L = \begin{array}{cccccccccc} 1 & 3 & 4 & 2 & 6 & 7 & 5 & 9 & 10 & 8 \\ 10 & 2 & 5 & 4 & 4 & 8 & 6 & 7 & 1 & 9 \\ 9 & 10 & 3 & 5 & 8 & 1 & 2 & 4 & 6 & 7 \\ 7 & 9 & 1 & 4 & 10 & 5 & 3 & 2 & 8 & 6 \\ 3 & 8 & 10 & 7 & 5 & 2 & 9 & 6 & 4 & 1 \\ 5 & 1 & 8 & 9 & 2 & 6 & 4 & 10 & 7 & 3 \\ 8 & 4 & 6 & 10 & 1 & 9 & 7 & 5 & 3 & 2 \\ 2 & 7 & 9 & 6 & 3 & 10 & 1 & 8 & 5 & 4 \\ 4 & 6 & 2 & 8 & 7 & 3 & 10 & 1 & 9 & 5 \\ 6 & 5 & 7 & 1 & 9 & 4 & 8 & 3 & 2 & 10 \end{array}$$

$$L^2 = \begin{array}{cccccccccc} 1 & 4 & 2 & 3 & 7 & 5 & 6 & 10 & 8 & 9 \\ 9 & 2 & 4 & 5 & 3 & 7 & 8 & 6 & 10 & 1 \\ 6 & 7 & 3 & 8 & 4 & 9 & 10 & 5 & 1 & 2 \\ 3 & 8 & 7 & 4 & 6 & 10 & 1 & 9 & 2 & 5 \\ 10 & 6 & 1 & 9 & 5 & 8 & 4 & 2 & 7 & 3 \\ 2 & 5 & 10 & 7 & 1 & 6 & 9 & 3 & 4 & 8 \\ 5 & 10 & 9 & 2 & 8 & 3 & 7 & 1 & 6 & 4 \\ 7 & 1 & 5 & 10 & 9 & 4 & 2 & 8 & 3 & 6 \\ 8 & 3 & 6 & 1 & 10 & 2 & 5 & 4 & 9 & 7 \\ 4 & 9 & 8 & 6 & 2 & 1 & 3 & 7 & 5 & 10 \end{array}$$

Estes quadrados provêm um contra-exemplo para a conjectura de Euler concernindo na não existência de pares de MOLS de ordem 10*, além disso* $L^3 = E$ *e logo,* $L^2 = L^{-1}$ *e sabendo que se* A *é um quadrado latino* A^{-1} *também o é. Pelo corolário4.0.4,* L *e* L^2 *são ortogonais.*

Capítulo 6

Hipercubos ortogonais

Neste capítulo usaremos resultados extraídos das seguintes referências: [2], [4], [6] e [9].

Nós vamos agora definir um conceito natural, que permeia a teoria dos quadrados latinos, na verdade esta é uma extensão da teoria já vista. De fato nós vamos generalizar as definições de quadrados latinos, até agora olhamos para um quadrado latino como se fosse algo imerso numa extrutura planar, no entanto, generalizemos esta teoria para uma extrutura de tês ou mais dimensões;(sempre fazendo ressalvas de que o corpo que trabalhamos é finito, etes são espaços vetoriais finitos). Além do mais a associação formal entre conjuntos de MOLS e de estruturas geométricas de dimensão 2 *é conhecida como planos afins e planos projetivos. Porém a associação destes arranjos de altas dimensões não é tão obvia, de fato desde que se queira herdar as propriedades dos quadrados latinos.*

Definição 6.0.3 *Seja X um conjunto com n elementos. Dizer que o hipercubo de ordem de ordem n e do tipo j é um arranjo formado pelo produto cartesiano $n \times n \times \ ... \times n$ (d vezes), tal que: esses n^d elementos estão num conjunto de n elementos e tal que se fixarmos j coordenadas($0 \leq j \leq d-1$)*

cada um dos n símbolos aparecem n^{d-j-1} vezes no sub-arranjo.

Observação 6.0.5 *Alguns matemáticos consideram que um hipercubo é sempre de ordem $j = d - 1$;porém aqui nós abrangeremos esta definição, pois acreditamos que ela é um pouco restritiva em se fazer uma análise mais cuidadosa na teoria dos hipercubos latinos mutuamente ortogonais.*

Tal definição vem de forma natural guardando as definições de quadrados latinos(que no caso são planares), pois se para $d = 2$, fixarmos uma coordenada os n símbolos restantes é um permutação dos n símbolos, e isso é bem rasoável se pensarmos em um quadrado latino como um elemento de RL_n analogamente para $d > 2$;vamos exemplificar esta definição agora:

Exemplo 6.0.5 *seja $L_1 = (a_{ij})$ e $L_2 = (b_{ij})$ dados por:*

$$L_1 = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix}$$

$$L_2 = \begin{matrix} 1 & 2 & 3 & \quad & 1 & 3 & 2 & \quad & 1 & 2 & 3 \\ 3 & 1 & 0 & \quad & 3 & 2 & 1 & \quad & 2 & 3 & 1 \\ 2 & 3 & 1 & \quad & 2 & 1 & 3 & \quad & 3 & 1 & 2 \end{matrix}$$

Em $L_1 = (a_{ij})$ se fixarmos a primeira coordenada, então quando $x = 1$ e $x = 2$, temos a terceira linha que é $3, 1, 2$, analogamente se fixarmos na segunda coordenada $y = 2, 3$, teremos a primeira coluna que é $1, 2, 3$. Para $L_2 = (b_{ij})$, se fixarmos as primeira e segunda coordenadas, digamos x e y, para $x = 1, 2$ e $y = 1, 2$ teremos $1, 3, 2$ qué é uma permutação de ordem 3;e de fato, temos que L_1 e L_2 são hipercubos do tipo $j = d - 1$.

Este Exemplo acima ilustra casos simples, porém casos ordem $d > 3$ o grau de dificuldade cresce consideravelmente. Como era de esperado extenderemos naturalmente o conceito de "quadrados latinos mutuamente ortogonais a hipercubos mutuamente ortogonais".

Definição 6.0.4 *Dois hipercubos são ditos ortogonais se, quando concatenados, cada um dos n^2 pares aparecem n^{d-2} vezes. E um conjunto de $t \geq 2$ hipercubos é dito ser ortogonal se eles são dois a dois ortogonais.*

Análogo a teoria dos quadrados latinos mutuamente ortogonais, adotávamos a abreviação para tal conjunto como MOLS, aqui adotaremos MOHC, em inglês, mutually orthogonal hipercubes. E como é de se esperar, quando $d = 2$, este caso se reduz a MOLS. Vamos exemplificar esta nova definição:

Exemplo 6.0.6 *Para $n = 3$ e $d = 3$, consideremos os hipercubos:*

$$\begin{array}{cccccc} 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 \\ 2 & 0 & 1 & 2 & 0 & 1 \end{array}$$

$$\begin{array}{cccccc} 0 & 1 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 & 1 & 2 \end{array}$$

$$\begin{array}{cccccc} 0 & 1 & 2 & 2 & 0 & 1 \\ 1 & 2 & 0 & 0 & 1 & 2 \\ 2 & 0 & 1 & 1 & 2 & 0 \end{array}$$

Assim se o primeiro cubo é concatenado com o segundo, os pares $00, 01, 02, ..., 22$ só ocorrem 3 vezes. Observemos também que se qualquer duas das três coordenadas são fixadas, cada um dos três símbolos ocorrem

uma vez nas posições especificadas, assim o cubo 2 é do tipo 2;e no caso do primeiro cubo, se na primeira e segundas coordenadas fazemos $x = y = 0$*, o símbolo* 0 *ocorre em todas as* 3 *posições, consequetemente o primeiro cubo é do tipo* 1*.*

6.1 Conjuntos ortogonais de hipercubos

Como fizemos no capítulo 4, aqui também nós queremos encontrar meios para construir conjuntos de MOHC de cardinalidades tão grandes quanto possível. Mas para isso teremos, primeiramente que estabelecer uma limitação superior para a cardinalidade de um conjunto de MOHC.

Porém, antes disso teremos que provar um lema importante, e definir alguns conceitos relevantes. Seja $H_1, H_2, ..., H_t$ *um conjunto de MOHC de ordem* n*, de dimensão* d*, e do tipo* j*. Para* $H_q, q = 1, ..., t$*, definimos uma matriz* $n^d \times n$ $N_q = (n_{x1,x2,...,xd;s})$*, onde* $n_{x1,x2,...,xd;s} = 1$ *se o* s*-ésimo símbolo ocorre na posição* $(x_1, x_2, ..., x_d)$*,* $x_1 = 1, 2, ...n, ..., x_d = 1, 2, ..., n$ *de* H_q *e* 0 *caso contrário. Acomodando as matrizes* $N_1, ..., N_t$ *lado a lado, teremos uma matriz* $n^d \times nt$ $M = (N_1|N_2|...|N_t)$*. Para estas considerações, enunciaremos o lema a seguir:*

Lema 6.1.1 *Para* $k, l = 1, 2, ..., t$*,*

$$N_k^T N_l = \begin{array}{l} N^{d-1} I_n, sek = l \\ N^{d-2} J_n, sek \neq l \end{array}$$

onde I_n *denota a matriz identidade de ordem* n*, e* J_n *é também uma matriz de ordem* n*, tal que, todas as suas entradas são* 1*, e* N_k^T *representa a transposta de* N_k*.*

Demonstração: *Se* $k = l$*; consideremos um elemento na posição* (i, i) *de* N_k^T*;a* i*-ésima linha de* N_k^T *e a* i*-ésima coluna de* N_k *tem a entrada* 1

em exatamente n^{d-1} posições, correspondendo a ocorrências do símbolo i no hipercubo H_k. Logo a entrada na posição (i,i) de N_k^T é n^{d-1}. Desde que os símbolos i e j não podem ocupar as mesmas posições em H_k, se $i \neq j$ a menos das entradas de N_k^T que são nulas.

Se $k \neq l$; da ortogonalidade dos hipercubos H_k e H_l, os símbolos i e j vão coincidir n^{d-2} vezes. Logo, para $k \neq l$, $N_k^t N_l = n^{d-2} J_n$, o que completa a demonstração.

Agora depois de provarmos este lema técnico estamos aptos para provar o teorema mais importante, até agora, desta seção:

Teorema 6.1.1 *O número máximo de MOHC de uma dada ordem n, de dimensão d e do tipo j é limitada superiormente por:*

$$\frac{1}{n-1}(n^d - 1 - \sum_{n=1}^{j} \frac{d!}{(d-k)!k!}(n-1)^k)$$

Demonstração: *Num hipercubo do tipo j, se todos os elementos menos um são conhecidos em algum subarranjo, definido, fixando k coordenadas, o elemento desconhecido pode ser determinado conforme o resto do subquadrado. Desde que todos os hipercubos são do tipo j, e desde que cada posição no hipercubo corresponde a uma linha de M, estas linhas correspondem a outros elementos do subarranjo que são conhecidos.*

Suponhamos que um elemento é visto como o último num subarranjo definido fixando k coordenadas. Então as restantes $d-k$ coordenadas pode ser assumidas com um valor fixado, digamos, n. Assim existem $\frac{d!}{(d-k)!k!}(n-1)^k$ posições no hipercubo em que exatamente k coordenadas tem o valor n;assim para um dado k, $\frac{d!}{(d-k)!k!}(n-1)^k$ linhas são fixadas. Agora, somando sobre k temos no mínimo $\sum_{n=1}^{j} \frac{d!}{(d-k)!k!}(n-1)^k)$ linhas linearmente dependentes em M. Em contrapartida isto nós dá $n^d - \sum_{n=1}^{j} \frac{d!}{(d-k)!k!}(n-1)^k)$ linhas

linearmente independentes em M. De fato, olhando para o posto de M, dentotado por $\rho(M)$, temos:

$$\rho(M) \leq n^d - \sum_{n=1}^{j} \frac{d!}{(d-k)!k!}(n-1)^k$$

E segue do lema anterior que:

$$MM^T = \begin{matrix} n^{d-1}I_n & n^{d-2}J_n & ... & n^{d-2}J_n \\ n^{d-2}J_n & n^{d-1}I_n & ... & n^{d-2}J_n \\ \vdots & \vdots & & \vdots \\ n^{d-2}J_n & n^{d-2}J_n & ... & n^{d-1}I_n \end{matrix}$$

Para encontrar os autovalores da matriz MM^T, usamos a simetria que esta matriz afortunadadmente apresenta. Consequentemente temos que os autovalores da matriz MM^T são: tn^{d-1}, n^{d-1} e 0 com respectivas multiplicidades $1, t(n-1), et-1$. Como a soma das multiplicidades de autovalores é o posto da matriz MM^T, que é o mesmo da matriz M, temos:

$$tn - t + 1 = \rho(MM^T) = \rho(M) \leq n^d - \sum_{n=1}^{j} \frac{d!}{(d-k)!k!}(n-1)^k$$

o que conclui a demonstração.

□

Vamos agora enunciar dois corolários que seguem imediatamente do último teorema:

Corolário 6.1.1 *Para um hipercubo de ordem n, de dimensão d e do tipo 1, o número máximo MOHC, neste caso é:*

$$N_d(n) \leq \frac{n^d - 1}{n - 1} - d$$

Corolário 6.1.2 *Existem no máximo*

$$(n-1)^{d-1} + (\sum_{k=d-1}^{j+1} \frac{d!}{(d-k)!k!}(n-1)^{k-1})$$

hipercubos mutualmente ortogonais de ordem n, do tipo j e de dimensão d.

Para demonstra isto basta o binômio de Newton.

6.2 Potências primas, considerando agora altas dimensões

Como no capítulo 4, construimos conjuntos completos de MOLS de ordem n para n uma potência de um número primo. Agora vamos generalizar este fato para hipercubos. Nós agora extendemos a construção algébrica em termos de polinômios com mais que duas variáveis sobre o corpo F_q, onde um $q = p^m$, com p primo. Feito isto a interpretação geométrica que antes era de retas no plano(para $d = 2$), agora vem de planos num espaço de dimensão $d = 3$, e, hiperplanos em espaços de dimensão maior que $d > 3$. Porém aqui vamos apenas restringirmos ao caso $d = 3$.

Consideremos a família de polinômios $f_{a,b,c}(x, y, z) = ax + by + cz$, com $a, b, c \in F_q$ e associemos cada hipercubo de um conjunto de MOHC de ordem n a um polinômio $f_{a,b,c}(x, y, z)$. Escolhendo coeficientes não nulos, podemos dividir esse polinômio por um dos a, b ou c e obter uma unidade em F_q como coeficiente. Tal operação vai fazer uma permutação nos símbolos do hipercubo, porém esta operação deixará as propriedades de ortogonalidade intactas.

Teorema 6.2.1 *Para um q potência de um número primo, o conjuto dos polinômios da forma:*

$$f_{a,1,c}(x,y,z) = ax + y + cz$$

$$f_{a,1,0}(x,y,z) = ax + y$$

$$f_{1,0,c}(x,y,z) = x + cz$$

representa um conjunto completo de $\frac{(q^3)}{(q-1)} - 3$ *MOHC de ordem* q.

Demonstração:

Para $a, c \in F_q$ *com* $ac \neq 0$ *existem* $(q-1)^2$ *polinômios da forma* $ax + y + cz$. *Os casos onde pelo menos uma constante é zero geram:* $q - 1$ *polinômios restantes das três formas acima, de um total de*

$$(q-1)^2 + 3(q-1) = \frac{(q^3)}{(q-1)} - 3$$

polinômios.

Agora provaremos que estes polinômios correspondem a hipercubos. Consideremos inicialmente os polinômios da forma $f_{a,1,c}(x,y,z) = ax+y+cz$ *onde* $ac \neq 0$. *Fixemos* $z = z_0$, *dos* q^3 *símbolos do cubo,* q^2 *vão ter coordenadas da forma* (x, y, z_0), *e este pontos do polinômio geram as imagens* $ax + y + cz_0$. *A adição da constante* cz_0 *funciona como um traslação das imagens do polinômio* $ax+y$; *conforme vimos no capítulo 4, teorema 4.1.1, este polinômio representa um quadrado latino, que neste caso,* $f_{a,1,c}(x,y,z)$ *produz um cubo do tipo* 2.

Os outros polinômios dão cubos do tipo 1. *De fato, se fixarmos* $x = x_0, y = y_0$ *no polinômio* $f_{a,1,0}(x,y,z) = ax+y$, *o símbolo igual a* ax_0+y_0 *ocorre em* q *posições* (x_0, y_0, z) *que geram cubos de ordem 1;de forma análoga, todos os polinômios restantes determinam cubos de ordem* 1. *Para mostrar a*

ortogonalidade, consideremos as posições ocupadas pelos símbolos s_1 *no cubo* C_1 *e* s_2 *no cubo* C_2*. Estas posições vão satisfazer as duas equações:*

$$a_1x + b_1y + c_1z = s_1$$

$$a_1x + b_2 + yc_2z = s_2$$

A solução deste sistema com duas equações dá a ocorrência do par ordenado (s_1, s_2) *quando* C_1 *é concatenado com* C_2*. Dadas as constantes dos* $\frac{(q^3)}{(q-1)} - 3$ *polinômios, é claro que estas constantes são linearmente independentes;assim a matriz destes coeficientes:*

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$$

tem posto completo. E lembrando que para $T : V \to W$ *linear, temos* $dim\rho(T)+dimker(T) = dimV$*;no nosso caso temos que a dimensão do núcleo desta matriz é* 2*;logo, o núcleo desta matriz tem* q *elementos. Olhando para o sistema acima, ele tem* q *soluções e assim, qualquer par ordenado de símbolos ocorrem o mesmo número de vezes quando dois cubos são concatenados.*

□

Capítulo 7

Aplicação dos quadrados latinos à teoria dos códigos

Neste último capítulo vamos utilizar as referências [5], [6] e [11].

Vamos agora começar, neste capítulo, a fazer aplicações da teoria dos quadrados latinos. Consideremos a teria dos códigos algébricos. A teoria dos códigos estuda métodos de transferência de informação, esta é uma subárea da teoria da informação, que o próprio nome já diz, estuda quanta informação se obtém em um determinado evento. Para o estudo desta importante área da engenharia, diversas ferramentas matemáticas,probabilísticas e computacionais são empregadas. Estamos interessados aqui em discutir algumas aplicações de quadrados latinos à teoria dos códigos. Um dos problemas centrais da transmissão de informação diz respeito a possibilidade de se acarretar erros nas mensagens. Estes erros ocorrem na transmissão de informações sobre canais que apresentam erros na mensagem enviada de uma fonte de saída, ou seja o erro acontece na chegada da mensagem.

Para começarmos nossas considerações sobre o problema de transmissão, precisaremos apenas de uns coceitos algébricos, tais como construções

de corpos finitos, como já vimos anteriormente neste trabalho. Tal teoria é chamada de teoria dos códigos corretores de erros ou teoria dos códigos algébricos. Usamos o termo "corretores de erros" pois como já citamos a mensagem codificada provavelmente chega com erros e teremos de achar modos para reaver a mensagem original de forma mais precisa possível. Deste modo queremos mostrar que quando usamos MOLS na construção de alguns códigos, eles herdam proporiedades que permitem "resgatar" a mensagem original pelo destinatário;para tal vamos primeramente definir alguns objetos e dar alguns exemplos.

Definição 7.0.1 *Um código q-ário C de comprimento n é um conjunto de vetores com n coordenadas onde cada coordenada é um elemento de Z_q, um corpo com q elementos.*

Vamos agora exibir alguns exemplos de códigos:

Exemplo 7.0.1 *$C_1 = \{000, 111\}$ é um código binário de comprimento 3. Analogamente os conjuntos $C_2 = \{00000, 01100, 10110\}$ e $C_3 = \{0000, 0111, 0222, 1012, 1201, 1120$ são, respectivamente, um código binário de comprimento 5 e um ternário de comprimento 4.*

Definição 7.0.2 *Uma palavra código em um código q-ário C é um vetor deste código.*

Neste ponto, podemos ver, alguma conexão entre o código C_3 e um conjunto de 2 MOLS de ordem 3, no caso consideremos a terceira e a quarta coordenadas em cada palavra código, e associemos à:

$$\begin{array}{cccccc} 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 & 2 & 0 \end{array}$$

Como sabemos $\mathbb{F}_{\shortparallel}^{\ltimes}$ é um espaço vetorial sobre F_q, dizemos que um código C é linear se C é um subespaço de $\mathbb{F}_{\shortparallel}^{\ltimes}$. Como exemplo o código C_1 que é linear sobre o corpo $\mathbb{F}_{\not\in}$ e o código C_2 que não é linear. A linearidade de um código desempenha um papel importante em muitas situações. De fato se um dado código é linear, ele herda todas as propriedades da álgebra abstrata e da álgebra linear.

Definição 7.0.3 *Seja $d : \mathbb{Z}_{\shortparallel}^{\ltimes} \times \mathbb{Z}_{\shortparallel}^{\ltimes} \to \mathbb{R}$ a função de duas variáveis dada por: $d(x, y)$ que é o número de coordenadas em que x difere de y.Esta função d é chamada distância de Hamming.*

É claro que esta função satisfaz os três axiomas de métrica, logo d é uma métrica. As próximas definições mostraram a importância da distância Hamminiana na teoria dos códigos. Para começar definimos

$$d(C) = min\{d(c_1, c_2)|c_1, c_2 \in C, C_1 \neq c_2\}$$

; este de certo, é um parâmetro do código C, que é um dos mais importates para analisá-lo. Como exemplo temosC_1, $d(C_1) = 3$.

Um parâmetro relacionado é o peso de uma palavra código. Definimos $wt(c)$ como sendo o número de coordenadas não nulas de c. Um resultado simples é que dados duas palavras código c_1, c_2 de um código linear C, temos:

$$d(c_1, c_2) = wt(c_1 - c_2)$$

Esta caracterização é efetiva e muito útil no cálculo do peso de um código linear, de fato,

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

Na prática é muito mais fácil calcular o minimo dos pesos das palavras códigos de um código. O próximo resultado faz uma ligação entre a distância $d(C)$ de um código e sua capacidade de detecção e correção de erros.

Teorema 7.0.2 *(i) Em um código C pode ser detectado acima de s erros se $d(C) \geq s+1$*

(ii) Em um código C pode ser corrigido acima de t erros se $d(C) \geq 2t+1$

Demonstração: *(i) Suponhamos que $d(C) \geq s+1$ e que durante a transmissão de uma palavra código c, s erros ou menos são introduzidos, mas como $d(C) \geq s+1$ essa palavra não pode ser interpretada como outra, logo o erro pode ser detectado.*

(ii) Agora assumimos que $d(C) \geq 2t+1$ e que uma palavra código x ´é transmitida e recebida como outra distinta, digamos y, contendo t erros ou menos;assim $d(x,y) \leq t$. Se uma palavra código c diferente de x, segue que $d(c,y) \geq t+1$;pois se $d(c,y) \leq t$, têm-se:

$$d(x,c) \leq d(x,y) + d(y,c) \leq 2t$$

o que contradiz a hipótese de que $d(C) \geq 2t+1$.

□

Observação 7.0.1 *Seja um código C com a distância mínima $d = d(C)$, tome $\frac{(d-1)}{2}$ e $d \geq 2t+1$. Assim, em C pode ser corrigido até $[\frac{(d-1)}{2}]$ erros de uma palavra código onde $[m]$ denota a função maior inteiro.*

Como um exemplo do teorema acima é que os códigos C_1, C_2 e C_3 podem respectivamente ser detectados 2,1 e 2 erros e corrigidos 1,0 e 1 erros, respectivamente.

Vamos agora começar a discutir alguns importantes problemas na área da teoria dos códigos. Um código C é dito do tipo (n, M, d) se ele for um código q-ário de comprimento n, com M palavras código e com distância mínima d. Se C é um subespaço de F_q^n de dimensão $k \leq n$, $M = q^k$. Vamos

usar a notação $[n, k, d]$ para representar códigos lineares de comprimento n, de dimensão k, e com distância mínima d.

Na teoria dos códigos temos uma fonte que envia os códigos para um determinado destino. Porém como assumimos que o erro pode ser acarretado na transmissão; deveras a palavra-código pode chegar ao seu destino e ser interpretada como outra. Este é um problema sério da teoria da informação. Pode ser rasoavelmente contornado se concernimos que esta palavra-código pode chegar com erros e delimitamos ele em torno de uma vizinhança. Dentro dela toda palavra-código seria reconhecida como o seu centro, neste caso a original. Em outras palavras, dada uma palavra código c e outra abitrariamente próxima x, onde decodificamos x por c. Queremos que a distância $d(x, c)$ seja o menor possível.

Matematicamente falando para qualquer palavra código x, dado um $r > 0$, qualquer elemento do conjunto $S_r(x) = \{y \in C | d(x, y) \leq r\}$ é decodificado como x na recepção. Este conjunto chamado esfera de centro em x e raio r. Na teoria da informação sempre se quer transmitir muitas diferentes mensagens, assim o número de palavras-código é pretendido ser o maior possível para um dado comprimento n. Sendo C linear o valor $\frac{k}{n}$ é chamada razão de um código. Este parâmetro da a medida de quanto de informação está contida em cada palavra código comparado com o comprimento do código. Claramente quanto maior esta razão mais vetores de Z_q^n são incorporados ao código. Assumindo que é mais difícil transmitir palavras-código longas contendo muitas coordenadas do que transmitir palavras curtas contendo poucas coordenadas, uma razão alta permite que o comprimento n pode ser diminuído para um determinado M.

Deste modo, para um (n, M, d) código C, n deve ser tão pequeno quanto possível, com d e M tão grandes o maior possível. Desafortunada-

mente, estes objetivos são contraditórios. Retornemos agora aos MOLS e MOHC, estes são usados para construir certos códigos ótimos, não os mais desejados, porém os melhores possíveis. Mais a frente vamos ver que o problema de enumeração de certos códigos maximais é equivalente a problemas de enumeração de quadrados latinos.

7.1 Obtendo códigos de MOLS

Queremos agora maximizar o número de palavras código num dado código q-ário com um dado comprimento n e uma dada distância mínima d. Para este fim denotemos $A_q(n,d)$ como sendo o maior valor de M tal que exista um (n,M,d) código q-ário. Como era esperado este é um problema díficil em parte, e também não existe uma fórmula para cálcula-lo. Para alguns valores de q,n,d, $A_q(n,d)$ é ainda desconhecido, porém com o uso de MOLS podemos encontrar para muitos valores de q,n,d, o número $A_q(n,d)$.

Primeiramente vamos provar este fácil resultado:

Exemplo 7.1.1 *i.Para qualquer q, $A_q(n,1) = q^n$.*
ii.Para qualquer q, $A_q(n,n) = q$.

Sendo $d = 1$, todas as palavras-código são distintas então o maior número de palavras código é o próprio espaço Z_q^n, logo M^n Para provar ii., suponhamos C um código q-ário (n,M,n). Neste código, qualquer duas palavras código deve diferir nas n coordenadas;segue que $M \leq n$. Agora consideremos os q vetores da forma:$(a,..,a)$ para $a = 0,1,...,q-1$, logo $A_q(n,n) = q$.

No próximo teorema vamos considerar códigos de comprimento 4 e $d = 3$:

Proposição 7.1.1 *Para todo* $q \geq 2$, $A_q(4,3) \leq q^2$

Demonstração: *Consideremos* C *um código q-ário* $(4, M, 3)$, *e* $x = (x_1, x_2, x_3, x_4)$ *e* $y = (y_1, y_2, y_3, y_4)$ *duas palavras-código distintas em* C. *Então obrigatoriamente os pares* $(x_1, x_2) \neq (y_1, y_2)$ *ou,* x *e* y *devem diferir em no máximo as duas últimas coordenadas, fazendo* $d(C) \leq 2$, *o que é uma contradição, logo* $M \leq q^2$

□ *Vamos agora dar um exemplo envolvendo MOLS e códigos:*

Exemplo 7.1.2 *Consideremos o seguinte par de MOLS de ordem* 3*:*

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 0 & 2 & 0 \end{array}$$

A partir destes MOLS de ordem 3, *construiremos um código* $(4, 9, 3)$. *Primeiramente fazemos uma certa ordenação das posições destes quadrados latinos. Construimos primeiramente, um arranjo* 4×9 *tais que as primeiras duas colunas são coordenadas relativas às* 9 *posições de um quadrado de ordem* 3, *a saber* (i, j), $i \leq j$. *Construiremos agora a terceira coluna colocando os símbolos do primeiro quadrado latino na sequência abaixo da coluna do arranjo. Procendo desta forma teremos nove palavras-código de comprimento* 4*:*

$$
\begin{array}{cccc}
0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 \\
0 & 2 & 2 & 2 \\
1 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
1 & 2 & 0 & 1 \\
2 & 0 & 2 & 1 \\
2 & 1 & 0 & 2 \\
2 & 2 & 1 & 0
\end{array}
$$

Observemos que este código, pelo Exemplo 6.0.2, pode detectar dois erros e corrigir 1.

No próximo resultado vamos mostrar a conexão entre um código q-ário$(4, q^2, 3)$ *e um par de MOLS de ordem* q.

Teorema 7.1.1 *Existe um código q-ário* $(4, q^2, 3)$ *se, e somente se, existe um par de MOLS de ordem* q.

Demonstração: *Para provarmos este resultado, mostremos que o o seguinte conjunto:*

$$C = \{i, j, a_{ij}, b_{ij} | (i, j) \in S_q^2\}$$

é um código $(4, q^2, 3)$ *se, e somente se,* $A = (a_{ij}), B = (b_{ij})$ *formam um par de MOLS de ordem* q. *Para isto consideremos os* q^2 *pares da forma* (i, a_{ij})*;eles são distintos se, e somente se,* $A = (a_{ij})$ *é um quadrado latino de ordem* q*.Analogamente, fazemos o mesmo para* B. *Assim temos que os* q^2 *pares* (a_{ij}, b_{ij}) *são distintos se, e somente se,* A *e* B *são ortogonais.*

□

E seguem os corolários:

Corolário 7.1.1 *Para todo $q \geq 2, A_q(4,3) = q^2$ se, e somente se, existe um par de MOLS de ordem q.*

Corolário 7.1.2 *Para $q \neq 2, 6$, existe um código q-ário $(4, q^2, 3)$*

Corolário 7.1.3 *Para $q \neq 2, 6, A_q(4,3) = q^2$.*

Estes últimos resultados seguem de resultados de capítulos anteriores e, é claro faz sombra a conjectura de Euler. De fato se q é uma potência prima, então os códigos acima podem ser construídos, a partir de MOLS de ordem q;e também apenas para fazermos a ligação, como vimos na seção de potências primas e nas suas observações, tais códigos vão ser lineares, desde que um anel $\mathbb{F}_{\text{ı}}$ é corpo se, e só se, p é primo, e estendemos este corpo naturalmente para um espaço vetorial $\mathbb{F}_{\text{ı}}^{\ltimes}$.

Vamos agora exibir uma importante limitação para um código quaisquer:

Teorema 7.1.2 *Para todo q, s, temos $A_q(s,d) \leq q^{s-d+1}$*

Demonstração: *Se nós deletarmos as últimas $d-1$ coordenadas de cada palavra-código em C, então restão apenas vetores de comprimento $s-d+1$, e eles devem ser distintos. Logo $M \leq q^{s-d+1}$.*

□

Códigos em que $A_q(s,d) = q^{s-d+1}$ são chamados códigos MDS, neologismo derivado do inglês: maximum distance separable. Códigos MDS são considerados códigos ótimos, pois não existe um código de comprimento s, de mínima distância $s-1$ que contenha mais de n^2 palavras-código. Muitos destes códigos podem ser construídos a partir de MOLS. Vamos agora provar outro interessante teorema que relaciona MOLS e códigos:

Teorema 7.1.3 *Existe um código q-ário $(s, q^2, s-1)$, se e somente se, existem $s-2$ MOLS de ordem q.*

Demonstração: *Vamos supor a existência de um código $(s, q^2, s-1)$, então duas palavras-código vão ter no máximo uma coordenada igual;assim podemos construir q^2 pares da forma (i, a_{ij}) onde cada $(a_{ij}) = A$ vai ser um dos $s-2$ quadrados, e que vão ser quadrados latinos e ortogonais. Ademostração deste fato é similar à prova do teorema6.1.3;a recíproca se faz construtivamente de forma análoga.*

□

Resta agora enunciar o último corolário desta seção:

Corolário 7.1.4 *Se q é uma potência prima e $s \leq q+1$, então $A_q(s, s-1) = q^2$ e existe um código MDS q-ário $(s, q^2, s-1)$.*

7.2 Códigos ótimos

Nesta seção vamos considerar o problema de maximizar o número de palavras-código de um dado comprimento n, e de uma mínima distância d. Mostraremos que em muitos casos o problema pode ser resolvido usando conjuntos de MOLS. Desde modo podemos concluir que a existência deste códigos ótimos está intimamente ligada à existência de conjuntos de MOLS. Este problema pode ser resolvido, ou melhor, a maximalidade é atingida desde que encontremos conjuntos de MOLS de cardinalidades tão altas tanto quanto possível. De novo, o conjunto de MOLS de uma determinada ordem vem a ser a chave do nosso estudo.

Vamos agora nos concentrar em códigos lineares. Para isto, consideremos q um potência prima, fixamos um comprimento n e uma dimensão

k, e definimos uma função $d_{max}(n,k;q)$ como sendo o maior d em todos os códigos $[n,k]$ lineares sobre o corpo $\mathbb{F}_{\shortparallel}$. Uma forma de computar $d_{max}(n,k;q)$ é construir todos os códigos e testar um a um as suas distâncias mínimas d. Porém com existem muitos subespaços próprios de $\mathbb{F}_{\shortparallel}^{\ltimes}$ (mais precisamente são:$n+\frac{n!}{(n-2)!2!}+...+\frac{n!}{(n-1)!}$ subespaços próprios), esperamos que haja uma forma de avaliar este número de forma não exaustiva, porém não existe esta forma milagrosa para o caso geral. No entanto, em muitos casos conseguimos chegamos aos melhores valores possíveis usando conjuntos de MOLS e MOHC. Para isto, vamos definir alguns objetos úteis.

Definição 7.2.1 *Uma matriz geradora de um código linear C do tipo $[n,k]$ é uma matriz $k \times n$ cujas linhas formam uma base para C.*

Exemplo 7.2.1 *Consideremos*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Esta matriz tem posto 3, logo o código linear binário C obtido por G, tem 8 palavras- código $W_1,...,W_8$, que são obtidos desta forma:

$$W_1 = 0R_1 = 0\ 0\ 0\ 0\ 0$$

$$W_2 = R_1 = 1\ 0\ 0\ 1\ 0$$

$$W_3 = R_2 = 0\ 1\ 0\ 0\ 1$$

$$W_4 = R_3 = 0\ 0\ 1\ 1\ 1$$

$$W_5 = R_1 + R_2 = 1\ 1\ 0\ 1\ 1$$

$$W_6 = R_1 + R_3 = 1\ 0\ 1\ 0\ 1$$

$$W_7 = R_2 + R_3 = 0\ 1\ 1\ 1\ 0$$

$$W_8 = R_1 + R_2 + R_3 = 1\ 1\ 1\ 0\ 0$$

Onde R_i são as linhas de G. A mínima distância deste código, $d_C = 2$, assim nós construimos um código binário linear $[5, 3, 2]$.

Vamos agora enunciar um teorema que une a teoria de hipercubos do espaço com a teoria dos códigos.

Teorema 7.2.1 *O código C, (a, a, q) é um código linear da forma:*

$$[\frac{(q^a - 1)^2}{(q-1)}, 2a, q^{2a-1} - 2q^{a-1}]$$

A demonstração deste teorema, necessita de conceitos como quadrados de frequência não estudados neste trabalho. Porém nos podemos checar que a dimensão de um código linear é $2a$ vendo que a matriz geradora G tem posto $2a$.

Agora consideremos um novo código C', (a, a, q) construído a partir de C usando a matriz identidade I_{2a} como a menor principal e completando com G, produzindo uma nova matriz geradora G' para C'. Deste modo teremos o seguinte corolário:

Corolário 7.2.1 *O código $C'(a, a, q)$ é um código linear sobre Z_q do tipo*

$$[\frac{(q^a - 1)^2}{(q-1)}, 2a, q^{2a-1} - 2q^{a-1} + 2]$$

7.3 Códigos maximais e enumeração de quadrados latinos

Sabemos que um código C contendo $q^n - 1$ palavras-código de comprimento n, em q símbolos com cada par destas palavras diferindo em pelo menos

duas coordenadas é um código MDS. Podemos construir códigos, no caso com $n = 3$*, tais que cada código representa um quadrado latino, neste caso específico isto é possível e factível. Para tal consideremos:*

$$C = \begin{matrix} 000 & 101 & 202 \\ 011 & 112 & 210 \\ 022 & 120 & 221 \end{matrix}$$

Este é um exemplo de código MDS, se permutarmos os seus símbolos corresponderemos aos doze quadrados latino existentes de ordem 3*. Porém este exemplo não induz uma regra geral. Nesta seção encontraremos condições para associar o número de códigos MDS ao número* L_q*. Para isto definimos o número* $L(q, n)$ *como sendo o número de códigos MDS de comprimento* n*, em* q *símbolos distintos. Como exemplo dessa função de duas variáveis temos o seguinte lema:*

Lema 7.3.1 *(i)* $L(1, n) = 1, n > 1$

(ii) $L(2, n) = 2, n > 1$

(iii) $L(q, 2) = q!, q \geq 1$

Demonstração: *(i)Sendo* $q = 1$*, temos apenas uma palavra-código, e sendo* C *um código MDS, tem-se* $L(1, n) = 1, n > 1$*.*
(ii)Análogo ao item (i).
(iii)Com q *palavras código e sendo* C *um código MDS temos apenas* $q!$ *possibilidades que são as permutações dos símbolos nas coordenadas de uma dada palavra-código.*

□

Agora faremos algumas considerações envolvendo códigos MDS com hiprecubos. Como vimos em capítulos anteriores um hipercubo r*-dimensional*

de ordem q e do tipo $r-1$, também chamado de cubos de permutação, pode ser visto como uma função:

$$f : \{1, .., q\}^r \to \{0, 1, ..., q-1\}$$

tal que se a e b diferem em exatamente uma coordenada então $f(a) \neq f(b)$. Denotamos por $P(q, r)$ o número de hipercubos r-dimensionais de ordem q. O próximo resultado vai estabelecer uma relação bem singular entre $P(q, r)$ e $L(q, n)$.

Teorema 7.3.1 *Para cada $n \geq 3$, $L(q, n) = P(q, n-1)$.*

Demonstração: *Suponhamos que temos um hipercubo f $(n-1)$-dimensional de ordem q. Então construiremos um código MDS de comprimento n, com $q^n - 1$ palavras-código da seguinte forma: Tomemos*

$$C = \{(i_1, ..., 1_{n-1}, f(i_1 + 1, ..., i_{n-1} + 1)) | 0 \leq i_1 \leq q-1, ..., 0 \leq i_{n-1} \leq q-1\}$$

A correspondência $f \to C$ é $1-1$, sabendo que f também é, e sobre o conjunto de códigos MDS com comprimento n, baseado nos q símbolos;o q completa a demonstração.

□

Daremos agora um exemplo que ilustra o teorema acima.

Exemplo 7.3.1 *Consideremos um código tal que as palavras-código são dadas por:*

0000	0101	0202	1001	1102	1200	2002	2100	2201
0011	0112	0210	1012	1110	1211	2010	2111	2212
0022	0120	0221	1020	1121	1222	2021	2122	2220

e consideremos agora o hipercubo de ordem 3*:*

$$\begin{array}{ccc} 012 & 120 & 201 \\ 120 & 201 & 012 \\ 201 & 012 & 120 \end{array}$$

cujas entradas corresponde à quarta coordenada da palavra-código acima. Notemos também que este hipercubo é do tipo 2*, como estudado no teorema acima.*

Podemos generalizar o caso de quadrados latinos reduzidos de ordem q *por esta dada função* f*, assim sendo, um quadrado latino é reduzido se* $f(1, ..., i, 1..., 1) = i-1, i = 1, ..., q$*. Denotemos* $P'(q, r)$ *como sendo o número de hipercubos reduzidos* r*-dimensionais de ordem* q*;deste modo generalizamos o caso dos quadrados latinos reduzido, pelo corolário a seguir:*

Corolário 7.3.1 *Temos:*

i.Para $r \geq 2, P(q, r) = q!((q-1)!)^{r-1}P'(q, r)$

ii.Para $n \geq 3, q!((q-1)^{n-2})$ *divide* $L(q, n)$

Notemos que no caso $r = 2$ *temos exatamente* $L_q = q!(q-1)!l_q$*. Deste último corolário notemos também que o número de códigos MDS distintos de comprimento* n *nos* q *símbolos é muito grande para* $n \geq 3$*.*

Referências Bibliográficas

[1] *Armstrong,M.A. Groups and Symmetry,Springer,New York, (1988)*

[2] *Dean,R.A.(1990),Classical Abstract Algebra,Harper and Row,New York*

[3] *Grass, J.L. Graph theory and it´s applications,CRC Press,1•ed, (1998).*

[4] *Hall, M.,Combinatorial Theory,John Wiley and Sons,New York, (1986).*

[5] *Hamming, R.W.(1950). Error detecting and error correcting codes,Bell System Tech.Journal-29,147-169.*

[6] *Laywine, C.F., Mullen, G. L.. Discrete Mathematics Using Latin Squares,Wiley-interscience publication,New York,(1998).*

[7] *McKay, B. D. and I. M. Wanless, Latin squares of order eleven. Preprint 2004. http://cs.anu.edu.au/ bdm/papers/ls11.pdf.*

[8] *McKay,B. D. and E. Rogoyski, Latin squares of order ten, Electron. J. Combinatorics,* **2***, (1995)*

[9] *Roberts,F.S. Applied Combinatorics,Prendice Hall,englewood Cliffs,New Jersey,(1984)*

[10] *Siu,M.K. Which latin squares are Cayley tables?,American Math. Mon.***98***(1991), 625-627.*

[11] Van Lint, J.H.,Wilson,R. M. A course in combinatorics,Cambridge University Press, 3•ed, (1996).

[12] Wilson,R.M.. Concerning the number of muttually orthogonal latin squares,Discrete math ***9****(1974), 181-198*