O Problema das Hipertorres e Partições Polarizadas Finitas e Infinitas

Emerson Luiz do Monte Carmelo

Orientador: Prof. Dr. Walter Alexandre Carnielli

Dissertação apresentada ao Instituto de Matemática , Estatística e Ciências da Computação , UNICAMP como requisito parcial para obtenção do Título de MESTRE em Matemática.

Este exemplar corresponde à redação final de tese devidamente corrigida e defendida pelo Sr. Emerson Luiz do Monte Carmelo e aprovada pela Comissão Julgadora.

Campinas, 6 de outubro de 1995

FICHA CATALOGRAFICA ELABORADA PELA
BIBLIOTECA DO IMECC DA UNICAMP

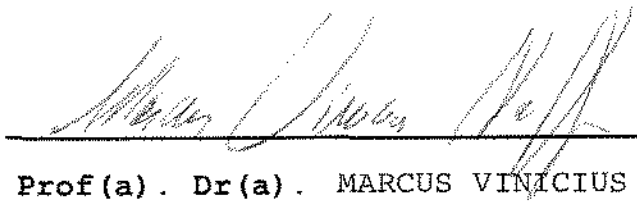
Monte Carmelo, Emerson Luiz do
M764p O Problema das hipertorres e particoes polarizadas finitas e infinitas. -- Campinas, [SP : s.n.], 1995.

Orientador : Walter Alexandre Carnielli
Dissertacao (mestrado) - Universidade Estadual de Campinas, Instituto de Matematica, Estatistica e Ciencia da Computacao.

1. Teoria dos grafos. 2. Otimizacao combinatoria. 3. Cobertura combinatoria. 4. Particoes (Matematica). 5. Teoria dos conjuntos. I. Carnielli, Walter Alexandre. II. Universidade Estadual de Campinas. Instituto de Matematica, Estatistica e Ciencia da Computacao. III. Titulo.

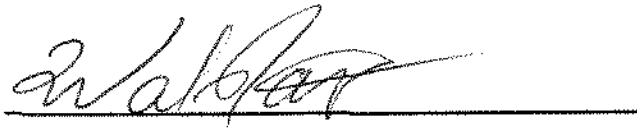
Tese defendida e aprovada em, 06 **de** 10 **de** 1995

Pela Banca Examinadora composta pelos Profs. Drs.



Prof(a). Dr(a). MARCUS VINICIUS SOLEDADE POGGI DE ARAGÃO

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



Prof(a). Dr(a). WALTER ALEXANDRE CARNIELLI

Índice

Introdução

Parte I Um resultado elementar , mas instrutivo, da chamada Teoria de Ramsey afirma que seis é o menor número de pessoas num grupo tal que: ou existem três pessoas que se conhecem mutuamente, ou existem três pessoas que são estranhas entre si (assumimos que a relação "conhecer" é simétrica, ou seja, se x conhece y, então y conhece x). Este valor da famosa função de Ramsey refere-se a um dos casos mais simples dentre os poucos valores conhecidos até o momento.

O problema de se determinar os valores exatos desta função parece ser bastante difícil , haja visto que, em mais de seis décadas de pesquisa, as soluções exatas foram obtidas apenas para alguns poucos e geralmente pequenos valores dos parâmetos do domínio.

A partir de 1971, passou-se a investigar variantes deste problema; o artigo[Ca3] apresenta uma versão cuja variante consiste na possibilidade da relação "conhecer" não ser necessariamente simétrica. Nesta versão, um problema similar ao descrito acima pode ser reformulado do seguinte modo:

> qual é o menor número de pessoas numa reunião que garanta a existência de dois grupos de três pessoas cada tal que: ou cada pessoa do primeiro grupo conhece todas do segundo grupo, ou cada pessoa do primeiro grupo não conhece nenhuma do segundo?

Este problema pode ser generalizado, gerando uma função que chamamos *função polarizada*. Como se trata de literatura recente, há vários problemas aparentemente complicados em aberto e cujos similares na clássica teoria de Ramsey já foram solucionados. Por exemplo, enquanto o valor do problema do parágrafo introdutório já foi estabelecido, continua em aberto a determinação exata do seu similar na função polarizada. Resolvemos parcialmente o problema: o valor está entre 10 e 19.

Para os casos finitos, a princípio, a determinação dos valores exatos desta nova função pode ser tãodifícil quanto seu similar na teoria clássica (ambas são problemas NP-completos). As primeiras cinco seções tratam deste problema.

O propósito deste trabalho é estudar, de um ponto de vista introdutório, duas classes de problemas extremos em combinatória finita e uma versão transfinita de uma delas

O capítulo I (seções 1 a 5) consta inicialmente de uma breve discussão sobre alguns conceitos combinatórios, tais como: planejamentos, quadrados latinos e apresentação de uma nova maneira de construir determinados planejamentos. A formulação da função polarizada encontra-se na segunda parte. As próximas duas seções descrevem resultados (na sua maioria originais) sobre limites inferiores e superiores para certas classes de parâmetros da função mencionada. A última seção deste capítulo estabelace uma conexão entre o *problema de Zarankiewicz* e a função polarizada.

Parte II O outro assunto abordado nesta monografia refere-se a um conhecido problema combinatório, também de caráter vetorial, que passamos a descrever.

> Qual é o número mínimo de torres de xadrez para satisfazer a propriedade seguinte: qualquer posição do tabuleiro pode ser atingida com um movimento de uma das torres ?

Não há dificuldade em ver que a resposta é 8. No entanto,a resposta não é tão fácil se considerarmos a mesma pergunta para tabuleiros de formato hipercúbicos no espaço n-dimensional. Esta situação particulariza um problema conhecido como *cobertura por hipertorres* . Embora estudada há décadas, conhecem-se apenas poucas classes de valores exatos para a função relacionada .

Este problema será abordado no capítulo II (seções 6 a 10) . Discutiremos brevemente alguns tópicos da teoria dos códigos em (6). Posteriormente, enfocaremos algumas estimativas de parâmetros da função associada à cobertura por hipertorres . Dedicamos maior atenção a uma nova proposta de ataque a tais problemas, conhecido como *método de cobertura usando matrizes* (parte 9), reservando a última seção deste capítulo a uma breve exposição dos avanços realizados neste problema através de recursos computacionais e otimização combinatória.

Não podemos deixar de mencionar o fato curioso: um caso específico desta função determina uma estratégia de apostas para ganhar na Loteria Esportiva com número mínimo de cartões.

Parte III O capítulo III apresenta um estudo sobre as versões transfinitas das partições encontradas no capítulo I (num certo sentido, extensões infinitárias da função polarizada). Tal assunto faz parte da teoria das partições

polarizadas. Em particular , dedicamos atenção especial ao Princípio de Ariadne, uma versão proposta por Carnielli e Di Prisco.

Este capítulo tem como escopo a apresentação de resultados relativos às partições polarizadas, dando ênfase a algumas comparações entre a teoria dos conjuntos ZF , a teoria de Ramsey infinita e o Princípio de Ariadne.

Para isto, um breve resumo de alguns tópicos de ZF é descrito na seção11. Em seguida, descrevemos alguns dos principais resultados da teoria de Ramsey infinita em 12.

A teoria das partições polarizadas é assunto das duas últimas seções, sendo que a parte 13 trata da classe destas partições definidas em produtos cartesianos de dimensão finita . E, finalmente, o Princípio de Ariadne é discutido na última , a qual tem como principal resultado deste capítulo: o Princípio de Ariadne é contraditório com o axioma da escolha.

A maioria dos trabalhos publicados sobre a teoria das partições polarizadas refere-se às partições definidas em produtos cartesianos de dimensão 2. Por outro lado, as referências bibliográficas das duas útimas seções são precursoras de um novo enfoque desta teoria, a saber :partições cuja dimensão pode ser maior que 2, ou mesmo transfinita. Como se trata de literatura recente, há vários problemas aparentemente difíceis em aberto e cujos similares na teoria de Ramsey infinita já foram solucionados.

Pressupomos, nesta dissertação, apenas familiaridade com alguns tópicos matemáticos elementares : construção de corpos finitos $GF(q)$ para q potência de primo, rudimentos da teoria de grupos e anéis, noções de espaço vetorial, elementos de teoria dos conjuntos.

Finalizando esta introdução, comentaremos a originalidade deste trabalho. O capítulo III é uma mera exposição. O mesmo acontece com as seções 6, 7 e 8 ; enquanto 9 apresenta algumas generalizações de teoremas já conhecidos. Resultados via métodos computacionais e a conexão entre o problema da cobertura por hipertorres e a Teoria dos Grafos (seção10) foram obtidos com a colaboração dos professores do DCC-Unicamp: Cid C. Souza e Marcus V.S.P. Aragão.

O capítulo I (em particular as seções 3 , 4 e 5) consta essencialmente de modestos resultados originais, com dependência de nosso conhecimento sobre o tema. Quanto aos demais resultados apresentados neste trabalho, procuramos citar as fontes bibliográficas.

Capítulo I

Função Polarizada

1 Teoria dos Planejamentos

Neste capítulo vamos assumir que todos os conjuntos mencionados são finitos e que todos os parâmetros são números naturais positivos. Inicialmente, apresentaremos alguns conceitos combinatórios:

1.1 Conceitos

Definição 1.1 Sejam V um conjunto de cardinalidade v ($|V| = v$) e β uma família de subconjuntos de V. Os elementos de V (respectivamente de β) recebem o nome de *pontos* (respectivamente *blocos* ou *linhas*).

Um *planejamento* com parâmetros (v, k, λ) consiste em um par $P = (V, \beta)$ tal que:

i) qualquer bloco tem cardinalidade k ,

ii) qualquer $2-$subconjunto (subconjunto de tamanho 2) de V está contido em exatamente λ blocos de β.

Eliminaremos a notação conjuntista (vírgulas e chaves) dos blocos quando não houver perigo de confusão.

Exemplo 1.2 Sejam $V = \{0, 1, \ldots, 6\}$ e
$\beta = \{\ 013\ , 124,\ 235,\ 346,\ 045,\ 156,\ 026\ \}$
Por simples inspeção, verifica-se que (V, β) é um planejamento $(7,\ 3,\ 1)$.

Definição 1.3: Diz-se que $P = (V, \beta)$ é um *planejamento resolúvel* (v, k, λ) quando:

i) P é um planejamento (v, k, λ) ;

ii) a família de blocos β pode ser dividida em classes tais que cada classe é uma partição de V.

Uma classe de β que particiona V recebe o nome de *classe de paralelas.*

Exemplo 1.4: Sejam $V = \{0, 1, \ldots, 8\}$ e β a família de 3-subconjuntos:

$$\begin{array}{cccc} b_1 = 036 & b_4 = 048 & b_7 = 057 & b_{10} = 012 \\ b_2 = 147 & b_5 = 156 & b_8 = 138 & b_{11} = 345 \\ b_3 = 258 & b_6 = 237 & b_9 = 246 & b_{12} = 678 \end{array}$$

O par (V, β) é um planejamento resolúvel $(9, 3, 1)$. onde os blocos de cada coluna acima estabelecem uma classe de paralelas .

Definição 1.5: Sejam $l \geq 2$ e $m \geq 1$. A tripla $T = (V, G, \beta)$ é uma *configuração transversal* (l, m) quando: $|V| = lm$; G particiona V em l grupos $G_1, G_2, \ldots, G_l$, onde $|G_i| = m$ para $1 \leq i \leq l$; β uma família de l-subconjuntos de V tal que :

i) cada bloco contém um único ponto de cada bloco de G .

ii) cada 2-subconjunto $\{x, y\}$ de V, onde x e y pertencem a grupos distintos de G, está num único bloco de β.

Exemplo 1.6 : Utilizando o exemplo acima e denotando:

$$\beta_1 = \{b_i,\ 1 \leq i \leq 9\} \qquad G_1 = \{0, 1, 2\} \qquad G_2 = \{3, 4, 5\} \qquad G_3 = \{6, 7, 8\}$$

obtemos $(V, \{G_1, G_2, G_3\}, \beta_1)$ uma configuração transversal $(3, 3)$.

Definição 1.7 : Seja $A = (a_{ij})$uma matriz quadrada de ordem m cujas entradas a_{ij} estão em $E = \{0, 1, \ldots, m-1\}$. A é um *quadrado latino* de ordem m se cada elemento de E ocorre exatamente uma vez em cada linha e em cada coluna de A ,ou ainda, todas as linhas e colunas de A são permutações de E.

Exemplo 1.8 : Denotando $E = \{0, 1, 2\}$, considere as matrizes:

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

As duas últimas são quadrados latinos de ordem 3.

Definição 1.9 Sejam duas matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$. Denotamos por $A*B$ a matriz *concatenação* de B em A , definida por $A*B = (c_{ij})$ onde: $c_{ij} = (a_{ij}, b_{ij})$ para $1 \leq i \leq n$ e $1 \leq j \leq n$.

Definição 1.10: As matrizes A e B são ditas *ortogonais* se a concatenação $A * B$ possuir todos os elementos de $E \times E$. As matrizes $A_1, A_2, \ldots, A_k$ são *mutuamente ortogonais* se A_i for ortogonal a A_j para $i \neq j$.

Exemplo 1.11: As matrizes do exemplo 1.8 são mutuamente ortogonais. De modo geral, podemos caracterizar quadrados latinos em termos de ortogonalidade.

Proposição 1.12: Uma matriz A de ordem m é quadrado latino se e somemte se as matrizes:

$$\begin{bmatrix} 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \ldots & \vdots \\ m-1 & m-1 & \ldots & m-1 \end{bmatrix} \quad , \quad \begin{bmatrix} 0 & 1 & \ldots & m-1 \\ 0 & 1 & \ldots & m-1 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 1 & \ldots & m-1 \end{bmatrix} \quad e \quad A$$

são mutuamente ortogonais.

Prova: Conseqüência direta da definição de quadrado latino.

1.2 Alguns resultados combinatórios

Dado seu interesse particular para o nosso trabalho, mostraremos uma forma direta de construir certas classes de planejamentos, que serão usadas posteriormente na obtenção de limites inferiores para a função polarizada .

Neste capítulo, salvo menção contrária, denotaremos um vetor r-dimensional X por $(X_0, X_1, \ldots, X_i, \ldots, X_{r-1})$ onde X_i representa a i-ésima coordenada de X ($0 \leq i \leq r-1$) .O vetor X^t denota o transposto de X.

Lema 1.13: Se r é primo então:
(a) existe planejamento resolúvel $(r^2, r, 1)$;
(b) existe configuração transversal (r, r);
(c) existem $r-1$ quadrados latinos de ordem r mutuamente ortogonais.

Prova: Seja $\mathbb{Z}_r$ o anel dos inteiros módulo r, onde $+$ e $\cdot$ denotam as operações usuais de adição e produto, respectivamente. Contruiremos o planejamento desejado $P = (V, \beta)$. Sem perda de generalidade, podemos identificar V como constituído pelos elementos da soma direta $\mathbb{Z}_r \oplus \mathbb{Z}_r$. Assim, seus elementos têm a forma: $(a, b) = a \cdot r + b$, onde $0 \leq a, b \leq r-1$.

Tome $G_i = \{ (i, y) \in V \ : \ 0 \leq y \leq r-1\}$ para $0 \leq i \leq r-1$. Desse modo, $G = \{G_i, 0 \leq i \leq r-1\}$ particiona V em r blocos. Mais ainda, G é uma classe de paralelas na segunda coordenada.

Para $0 \leq a, b \leq r-1$, considere:
(i) $F(a,b) = (a, b+a, 2b+a, \cdots, (r-1)b+a)^t$

(ii) $B(a,b)$ o r-subconjunto de V formado pelos elementos de $(0, 1, \ldots, r-1)^t * F(a,b)^t$, isto é:

$$B(a,b) = \{(0,a), (1, b+a), \ldots, (r-1, (r-1)b+a) \}$$

Seja B o conjunto cujos elementos são os blocos $B(a,b)$. Finalmente, $\beta = B \cup G$ é o conjunto de blocos desejado.

Claramente temos $|V| = r^2$ e qualquer bloco tem tamanho r. Para (V, B) ser planejamento resolúvel, resta provar que qualquer 2-subconjunto de V está contido em um único bloco de β. Dividiremos esta tarefa em três partes.

Primeira parte: a intersecção de dois blocos não excede um elemento:
(1.1) $|G_i \cap G_j| = 0$ para $i \neq j$, pois G particiona V ;
(1.2) $|G_i \cap B(a,b)| = 1$ por construção de $B(a,b)$;
(1.3) a intersecção de dois blocos de B tem cardinalidade menor ou igual a um. De fato, digamos que $x \neq y$ e $\{x, y\} \subset B(a,b) \cap B(c,d)$. Como $\{x, y\} \subset B(a,b)$, temos $x = (n, nb+a)$ e $y = (m, mb+a)$, onde $n \neq m$ por (1.2). Por outro lado, $\{x, y\} \subset B(c,d)$ e assim:

$$nb + a = nb + c$$
$$mb + a = mb + c$$

Subtraindo membro a membro as duas igualdades . $(b-d)(n-m) = 0$. Como $\mathbb{Z}_r$ é corpo e $n - m \neq 0$, obtemos $d = b$. Claramente temos $a = c$ e, portanto, $B(a,b) = B(c,d)$.

Parte dois: qualquer 2-subconjunto $\{x, y\}$ de V aparece uma vez nos blocos de β. De fato, dado um x de V, ele está contido em $r+1$ blocos, pois há r classes de paralelas em B mais a classe G(parte três). Para cada um desses blocos, x se relaciona com $r-1$ pontos. Então x se relaciona com $(r-1)(r+1) = r^2-1$ pontos. Há (r^2-1) 2-subconjuntos de V que contém x e, nenhum desses pode aparecer mais de uma vez (primeira parte). Assim todos são distintos.

Parte três: Dado $0 \leq b \leq r-1$, a união $B(0,b) \cup B(1,b) \cup \ldots \cup B(r-1,b)$ forma uma classe de paralelas . Tome $(i,j) \in V$. Claramente existe um $0 \leq a \leq r-1$ tal que $ib + a = j$, ou seja, $(i,j) \in B(a,b)$. Por outro lado, (i,j) pertence apenas a um bloco da classe de paralelas.

Com estas três partes, conclui-se o item (a) do lema . A tripla (V, G, B) forma uma configuração transversal (r, r) pois:

(i) cada bloco de B possui um ponto de cada bloco de G.

(ii) cada 2-subconjunto $\{x, y\}$, x e y pertencentes a blocos distintos de G , está num único bloco de B.

Finalmente, os $r-1$ quadrados latinos podem ser construídos da seguinte forma. Dado $1 \leq i \leq r-1$, considere F_i a matriz cujas entradas são as i-ésimas projeções dos vetores $F(a,b)$:

$$F_i = (\ F(a,b)_i\ ) \quad \text{onde } 0 \leq a, b \leq r-1$$

Utilizando o fato de $\mathbb{Z}_r$ ser um corpo, prova-se que F_i é quadrado latino e que $\{F_1, F_2, \ldots, F_{r-1}\}$ contitui um conjunto de matrizes mutuamente ortogonais. □

-Matriz Geradora-

O leitor deve notar que as componentes de $(0, 1, \ldots, r-1)^t * F(a,b)^t$ foram definidas adicionando-se a nas segundas coordenadas das componentes de $(0, 1, \ldots, r-1)^t * F(0,b)^t$. Já vimos que $\cup_{a=0}^{r-1}\{\ B(a,b)\ \}$ é uma classe de paralelas. Dessa forma, para b fixado, $(0, 1, \ldots, r-1)^t * F(a,b)^t$

podem ser construídos a partir de $(0, 1, \ldots, r-1)^t * F(0, b)^t$. Assim, $B(0,0), B(0,1), \ldots, B(0, r-1)$ geram as famílias de paralelas de B.

Com este princípio, introduziremos um algoritmo de obtenção desses geradores e, em conseqüência , todos os blocos de B.

Definição 1.14: Fixe $0 \leq k \leq r-1$, denote por Ψ_k a *matriz geradora* definida por $\Psi_k = (ka + b)_{0 \leq a,b \leq r-1}$, isto é:

$$\Psi_k = \begin{bmatrix} 0 & 1 & 2 & \ldots & r-1 \\ k & (k+1) & k+2 & \ldots & k+r-1 \\ 2k & 2k+1 & 2(k+1) & \ldots & 2k+r-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (r-1)k & (r-1)k+1 & (r-1)k+2 & \ldots & (r+1)(k+1) \end{bmatrix}$$

A coluna j de Ψ_k coincide com o vetor $F(j, k)$; os elementos da diagonal principal de Ψ_k , com as componentes de $F(0, k+1)$. Este, por sua vez, aparece na primeira coluna ($j = 0$) de Ψ_k e gera o bloco $B(0, k+1)$. Analogamente, os elementos da diagonal principal de Ψ_{k-1} coincidem com os pontos de $F(0, k+2)$, gerando $B(0, k+2)$ e assim sucessivamente. Portanto, este procedimento recursivo produz $F(0,0)$, $F(0,1)$, $\ldots$, $F(0, r-1)$,os quais geram a família B .

Exemplo 1.15: Construção de planejamento resolúvel $(9, 3, 1)$. Considere $V = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ e a bijeção canônica entre V e $\{0, 1, \ldots, 8\}$. Pelo lema 1.13 , temos $F(b, 0)^t = \{b, b, b\}$ para $b = 0, 1, 2$. Assim

$$\Psi_0 = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix}$$

Concatenando o vetor $(0, 1, 2)^t$ com as colunas de Ψ_0 , obtemos três blocos de B :

$$B(0,0) = (0, 3, 6) \qquad B(1,0) = (1, 4, 7) \qquad B(2,0) = (2, 5, 8)$$

Das outras duas matrizes geradoras:

$$\Psi_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \qquad \Psi_2 = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

obtemos os blocos:

$$B(0,1) = (0,4,8) \qquad B(1,1) = (1,5,6) \qquad B(2,1) = (2,3,7)$$
$$B(0,2) = (0,5,7) \qquad B(1,2) = (1,3,8) \qquad B(2,2) = (2,4,6)$$

Tomando-se $G = \{(0,1,2),(3,4,5),(6,7,8)\}$, o planejamento $P = (\ \{0,1,\ldots,8\}, B \cup G\ )$ é resolúvel com parâmetros $(9,3,1)$.

Em 1.13(c) , vimos que $F_1, F_2, \ldots, F_{r-1}$ são mutuamente ortogonais. De um modo geral vale:

Lema 1.16: Para qualquer potência de primo $q = r^n$, existe um conjunto de $q-1$ quadrados latinos mutuamente ortogonais de ordem q .

Prova: Seja o corpo de Galois $GF(q)$ com q elementos . Para $k \in GF(q) \setminus \{0\}$, defina a matriz:

$$F_k = (F_k(b,a)) = (k.a + b) \qquad \{a,b\} \subset GF(q)$$

A qual é quadrado latino devido à estrutura de corpo em $GF(q)$. Falta mostrar que F_k e F_j são ortogonais para $k \neq j$. Suponha que $(F_k(b,a), F_j(b,a)) = (F_k(d,c), Fj(d,c))$. Assim como na demonstração do lema 1.13(c), encontramos $a = c$ da igualdade $(k-j).(a-c) = 0$, desde que $k \neq j$. Logo $b = d$, pois F_k é quadrado latino.

No lema 1.13(c), poderíamos construir os blocos de β partindo da existência de $(r-1)$ quadrados latinos mutuamente ortogonais de ordem r e vice-versa. Na realidade, os conceitos: quadrado latino, planejamento resolúvel, configuração transversal estão intimamente ralacionados pela:

Proposição 1.17: Para $m \geq 2$, as afirmações seguintes são equivalentes:
(a) existe planejamento resolúvel $(m^2, m, 1)$;
(b) existe configuração transversal (m, m);
(c) existe $m-1$ quadrados latinos de ordem m mutuamente ortogonais.
Prova: Ver [Si].

2 Formulação da Função Polarizada

No primeiro parágrafo da Introdução lembramos um resultado folclórico da Teoria de Ramsey :

> seis é a quantidade mínima de pessoas numa reunião para garantir a existência de um grupo de três pessoas que se conhecem mutuamente, ou de um grupo de três pessoas que são estranhas duas a duas (assumimos a simetria da relação "conhecer ").

Podemos generalizar este problema de várias maneiras, a saber:

(a) subistituir a relação binária "conhecer" por uma n-ária (não necessariamente simétrica);

(b) supor que a relação possa assumir r valores distintos e não apenas dois (conhecido ou desconhecido);

(c) exigir que o grupo tenha um valor arbitrário t de pessoas.

Afim de formular matematicamente estas possíveis generalizações do problema em questão , vamos adotar algumas notações e definições. Dados um conjunto X e um número natural n , denotamos por $|X|$ a sua cardinalidade, por X^n o produto cartesiano de X n vezes e $X^{(n)} = \{Y : Y \subset X \ , |Y| = n\}$. Salvo menção contrária, assumiremos a simbologia da teoria dos conjuntos conforme [Je] .

Definição da Função de Ramsey

Sejam a, t, n e r cardinais finitos. Uma *r-coloração* do conjunto S é simplesmente uma função $\chi : S \to r$. Para cada $s \in S$, $\chi(s)$ recebe o nome de cor de s (em relação a χ). Um subconjunto $T \subset S$ é *monocromático* ou *homogêneo* se a imagem de T, $\chi''(T)$, tem apenas um elemento.

A relação de partição $a \to (t)^n_r$ (lê-se *a flecha t, n, r*) significa: para qualquer r-coloração de $a^{(n)}$ existe um subconjunto $T \subset a$, $|T| = t$, $T^{(n)}$ homogêneo.

Obviamente quando $a \rightarrow (t)^n_r$ não vale (neste caso, indicado por $a \not\rightarrow (t)^n_r$ - lê-se *a não flecha* t, n, r) significa que há pelo menos uma r-coloração de a^n onde nenhuma das r cores contém um subconjunto $T^{(n)}$ homogêneo, com $|T| \geq t$.

Os índices inferior e superior não serão indicados em alguns casos. Nestes, assumiremos o valor como sendo 2. Por exemplo: $a \rightarrow (t)^3$ representa $a \rightarrow (t)^3_2$ e $a \not\rightarrow (t)_4$ significa $a \not\rightarrow (t)^2_4$. Conforme estas notações, a asserção a que nos referimos no parágrafo inicial resume-se a : $6 \rightarrow (3)$ e $5 \not\rightarrow (3)$.

F. Ramsey, em 1928, provou que para toda tripla (t, r, n) sempre existe um a suficientemente grande satisfazendo $a \rightarrow (t)^n_r$. Dessa forma, o problema relativo à generalização comentada da asserção acima pode ser interpretado simbolicamente por: dados r, t, n ; qual o menor a tal que $a \rightarrow (t)^n_r$? Logo, faz sentido definir :

$$R(t, r, n) = \min\{a \in I\!N : a \rightarrow (t)^n_r\}$$

Esta é a famosa *função de Ramsey*. Desde que $6 \rightarrow (3)$, $5 \not\rightarrow (3)$ e que a relação $a \rightarrow (t)^n_r$ é claramente monótona crescente em t , n e r , temos $R(3, 2, 2) = 6$. No entanto, conhecem-se poucos valores exatos dessa função, mesmo para parâmetros pequenos. Há mais de sete décadas esta função vem resistindo a todos os tipos de "ferramentas" matemáticas e investidas (mesmo em computadores) empregados na sua determinação.

Definição da função polarizada

A partir de 1971, variantes desse problema começaram a ser pesquisadas (ver [Fe]). O artigo [Ca3] , publicado em 1986, apresenta uma versão na qual considera a possibilidade da relação não ser necessariamente simétrica. Passamos à sua formulação.

> Sejam t, r, n naturais. A relação de partição $a \Rightarrow (t)^n_r$ (lê-se *a dupla flecha* t, n, r) significa: para toda r-coloração χ de a^n existe uma cor i e existem $H_j \subset a$, com $|H_j| = t, 1 \leq j \leq n$, tais que $\chi(H_1 \times H_2 \times \ldots \times H_n) = \{i\}$.

Neste caso, o conjunto $H_1 \times H_2 \times \ldots \times H_n$ recebe o nome de *t-monocromático* Se $a \rightrightarrows (t)^n_r$ não vale, escrevemos $a \not\rightrightarrows (t)^n_r$ (lê-se *a não dupla flecha* t, n, r) . Em alguns casos, omitiremos o índice inferior r (índice superior n) se $r = 2$ ($n = 2$).

No artigo [Ca3] é demonstrado o similar do teorema de Ramsey finito: dados t, r, n ; sempre existe um natural a suficientemente grande tal que $a \rightrightarrows (t)^n_r$. O menor a satisfazendo tal propriedade é definido como sendo o valor da função $\rho(t, r, n)$, ou seja,

$$\rho(t, r, n) = \min\{a \in \mathbb{N} : a \rightrightarrows (t)^n_r\}$$

Como retiramos a obrigatoriedade da simetria, esta nova função tem caráter vetorial. Por este motivo, ρ é dito função polorazida.

Já mencionamos que $R(3, 2, 2) = 6$; em compensação, a determinação exata de seu similar nesta versão continua em aberto, tendo até o momento a solução parcial : $10 \leq \rho(3, 2, 2) \leq 19$.

Este fato não é isolado. Há vários problemas em aberto nesta versão cujos similares na Teoria de Ramsey já foram solucionados.

Impondo a restrição $H_1 = H_2 = \ldots = H_n$, se $a \rightrightarrows (t)^n_r$ então $a \to (t)^n_r$ .Tal observação mostra que $a \to (t)^n_r$ reduz-se a um caso particular de $a \rightrightarrows (t)^n_r$, no entanto, por serem problemas NP-completos, apresentam a princípio a mesma dificuldade computacional . Das delimitações feitas para a função ρ neste trabalho conseguimos obter um único valor exato dos casos não trivias, a saber, $\rho(2, 2, 2) = 5$.

Vejamos os casos triviais. Dados t, r, n , o menor a tal que $a \rightrightarrows (t)^n_1$ é $a = t$ ($\rho(t, 1, n) = t$). Por outro lado, $\rho(1, r, n) = 1$ quando $t = 1$. Agora, para $n = 1$, o Princípio da Casa do Pombo diz que $\rho(t, r, 1) = r(t - 1) + 1$. Neste sentido, a função ρ pode ser encarada como uma das possíveis generalizações do princípio citado. Daqui em diante, vamos considerar os casos onde os parâmetros são todos superiores a 1. Claramente vale:

Proposição 2.1:(regras de monotonicidade) Se $a \leq a'$, $t \leq t'$, $r' \leq r$, $n' \leq n$ e $a \rightrightarrows (t)^n_r$ então $a' \rightrightarrows (t')^{n'}_{r'}$

3 Delimitações Inferiores

Para a determinação de um limite inferior da função ρ , digamos $a < \rho(t, r, n)$ ($a \neq (t)_r^n$), basta exibir uma r-coloração de a^n que não apresente um t-subconjunto monocromático.

Até o momento, não é de nosso conhecimento a publicação de nenhum trabalho referente ao assunto que nos propomos a enfocar nesta seção (a saber, obtenção de limites inferiores), salvo os poucos resultados devidos a Carnielli (ver [Ca3] e [Ca4]).

Tendo em vista os comentários acima, apresentaremos algumas novas classes de limites inferiores cujas colorações dependem essencialmente das estruturas de certos planejamentos e de quadrados latinos.

Teorema 3.1 Se r é primo então $r^2 < \rho(2, r, 2)$.

Prova: Exibiremos uma r-coloração χ de $V \times V$ tal que $|V| = r^2$ e cujas cores não contém um conjunto da forma: $\{x_1, x_2\} \times \{y_1, y_2\}$. Sem perda de generalidade, podemos identificar os pontos de V com os elementos de $\mathbb{Z}_r \times \mathbb{Z}_r$ e as cores, com $\{0, 1, \ldots, r-1\}$.

Dado um $x_i \in V$, adotaremos a tabela:

x_i	A_0	...	A_j	...	A_{r-1}

para indicar que as células $\{x_i\} \times A_j$ de $V \times V$ recebem a cor j , onde $0 \leq j \leq r-1$ e $A_0 \cup A_1 \cup \ldots \cup A_{r-1}$ particiona V .

Para um a de $\mathbb{Z}_r$ fixado, considere a tabela:

$(a,0)$	$B(0,a)$	...	$B(j,a)$	...	$B(r-1,a)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
(a,b)	$B(b,a)$	...	$B(b+j,a)$	...	$B(b+r-1,a)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$(a,r-1)$	$B(r-1,a)$	...	$B(r-1+j,a)$	...	$B(r-1+r-1,a)$

onde a família dos blocos $B(b,a)$, $0 \leq b \leq r-1$, consiste na classe de paralelas gerada pelo vetor $F(0,a)$ na demonstração do lema 1.13

Agora, variando a, obtemos a coloração χ com as propriedades:

(P1) para qualquer elemento v de $V \times V$ existe uma cor j tal que $\chi(v) = j$, pois $\cup_{b=0}^{r-1}\{B(b,a)\}$ particiona V pelo lema 1.13

(P2) não existe um 2-subconjunto homogêneo para χ . De fato, se tal ocorresse, existiria um 2-subconjunto de V aparecendo 2 vezes em blocos de B contidos nesta cor . Mas isto leva a um absurdo, desde que $B \subset \beta$ e (V, β) é planejamento.

A prova está completa.□

Comentário Assumindo as notações acima, podemos notar que, com a fixado, a eliminação da primeira coluna da tabela acima origina um quadrado latino dado pela matriz $(B(i+j,a))_{r\times r}$ .Variando a , obtemos r cópias de quadrados latinos isomorfos e a propriedade:

(P3) os blocos de uma cor são os mesmos r^2 blocos de B do Lema 1.13

As propriedades (P1) a (P3) evidenciam uma simetria muito especial na classe de colorações descrita.

Exemplo 3.2. $10 \leq \rho(2,3,2)$. A aplicação do teorema 3.1 quando $r = 3$ determina a coloração (empreganos a bijeção usual entre $\mathbb{Z}_3 \times \mathbb{Z}_3$ e $\{0,1,\ldots,8\}$ para facilitar a leitura):

cor 0	*cor* 2	*cor* 2
(0,0) (0,3) (0,6)	(0,1) (0,4) (0,7)	(0,2) (0,5) (0,8)
(1,1) (1,4) (1,7)	(1,2) (1,5) (1,8)	(1,0) (1,3) (1,6)
(2,2) (2,5) (2,8)	(2,0) (2,3) (2,6)	(2,1) (2,4) (2,7)
(3,0) (3,4) (3,8)	(3,1) (3,5) (3,6)	(3,2) (3,3) (3,7)
(4,1) (4,5) (4,6)	(4,2) (4,3) (4,7)	(4,0) (4,4) (4,8)
(5,2) (5,3) (5,7)	(5,0) (5,4) (5,8)	(5,1) (5,5) (5,6)
(6,0) (6,5) (6,7)	(6,1) (6,3) (6,8)	(6,2) (6,4) (6,6)
(7,1) (7,3) (7,8)	(7,2) (7,4) (7,6)	(7,0) (7,5) (7,7)
(8,2) (8,4) (8,6)	(8,0) (8,5) (8,7)	(8,1) (8,3) (8,8)

Nota: Esta construção não se aplica quando r é potência de primo. Vejamos o contra-exemplo $r = 4$. Seguindo a construção mencionada, a cor 0 conteria as células do tipo:

$$(0,0) \times B(0,0) \qquad e \qquad (2,0) \times B(0,2)$$

Como $F(0,0) = (0,0,0,0)$ e $F(0,2) = (0,1.2,2.2,2.3) = (0,2,0,2)$ (operações em $\mathbb{Z}_4$), teríamos $B(0,0) = (0.4,8,12)$ e $B(0.2) = (0,6,8,14)$. O conjunto $\{0,0\} \times \{0,8\}$ seria homogêneo.

Esta limitação acontece pelo fato de empregarmos a estrutura cíclica do grupo $(\mathbb{Z}_r, +)$ para r primo, o qual não é válido diretamente em $(GF_{(q)}, +)$ para q potência de primo.

No entanto, uma generalização do resultado acima é possível para r potência de primo (Teorema 3.5). Para aproveitar a nomenclatura veremos antes o resultado:

Teorema 3.3. Para r primo, $r(r+1) < \rho(2, r+1, 2)$.

Prova. Seja a coloração desejada $\acute{\chi} : \acute{V} \times \acute{V} \to \{0,1,...,r\}$, onde $\acute{V} = \mathbb{Z}_{r+1} \oplus \mathbb{Z}_r$. Considere $\chi : V \times V \to \{0,1,...,r-1\}$ do teorema 3.1 representada na forma de tabelas:

(a,b)	$B(b,a)$	...	$B(b+j,a)$	...	$B(b+r-1,a)$

Exibiremos $\acute{\chi}$ em etapas, algumas delas baseadas em certas alterações dos blocos de χ

(1) Fixemos $(a,b) \in V, 0 \leq a,b \leq r-1$.

(2) Construção do bloco $\acute{B}(b+j,a)$ a partir de $B(b+j,a)$. $0 \leq j \leq r-1$. Na cor j, substituímos o elemento de $B(b+j,a)$ cuja primeira coordenada é $(a+j)$ por $(r, a+j) \in \acute{V}$. Seja $\acute{B}(b+j,a)$ este novo bloco:

$$B'(b+j,a) = B(b+j,a) \cup \{(r,a+j)\} \setminus \{(\ a+j, (a+j)a+b+j\ )\}$$

Variando j , o conjunto dos elementos substituídos na tabela acima foram:

$$\left\{(a, a^2+b), (a+1, a^2+b+a+1), \ldots, (a+r-1, a^2+b+(r-1)(a+1))\right\}$$

Por outro lado, $B(b-a, a+1)$ contém os mesmos r pontos.

(3) Como $\acute{B}(b,a) \cup \acute{B}(b+1,a) \cup \ldots \cup \acute{B}(b+r-1,a) \cup B(b-a,a+1)$, forma uma partição de $\acute{V}$, colorimos as células com primeira coordenada igual a (a,b) conforme a nova tabela:

(a,b)	$B'(b,a)$	$\ldots$	$B'(b+j,a)$	$\ldots$	$B'(b+r-1,a)$	$B(b-a,a+1)$

(4) Variando (a,b) e repetindo as 3 etapas iniciais, obtemos a coloração de $r^3(r+1)$ células.

(5) Para os pontos da forma $(r,b), 0 \leq b \leq r-1$, considere as tabelas:

(r,b)	G_b	$\ldots$	G_{b*j}	$\ldots$	G_{b*r-1}	G_{b*r}

onde $G_i = \{i\} \times \mathbb{Z}_r$ e $*$ denota a adição em $\mathbb{Z}_{r-1}$.

A contrução de χ' manteve as propriedades:

(p1) $|G_k \cap G_j| = 0$ para $k \neq j$;

(p2) $|G_j \cap B(b,a)| \leq 1$ (lema 1.13)

(p3) $|B(b,a) \cap B(c,d)| \leq 1$ (lema 1.13)

Mais ainda, a nova coloração satisfaz:

(p4) $\left|\acute{B}(b,a) \cap \acute{B}(c,d)\right| \leq 1$. Suponha que $\{x,y\} \subset \acute{B}(b,a) \cap \acute{B}(c,d)$. Não podem acontecer os casos $\{x,y\} \subset V$ e $\{x,y\} \subset \{r\} \times \mathbb{Z}_r$ devido às propriedades (p3) e (p1), respectivamente. Resta o caso $x \in V$ e $y \in \{r\} \times \mathbb{Z}_r$. Por construção, y aparece em r blocos, digamos $\acute{B}_1, \acute{B}_2, \ldots, \acute{B}_r$. Mas $B_1 \cup B_2 \cup \ldots \cup B_r$ particiona V e contém o conjunto $(\acute{B}_1 \cup \acute{B}_2 \cup \ldots \cup \acute{B}_r) \setminus \{r\} \times \mathbb{Z}_r$. Portanto, nesses r blocos, não há dois distintos que contenha x.

As quatro propriedades provam que não existe uma cor i e um $Q = \{u,v\} \times \{x,y\}$ tal que $\acute{\chi}(Q) = \{i\}$.□

Exemplo 3.4: $13 \leq \rho(2,4,2)$. Identificando $\acute{V} = \mathbb{Z}_4 \oplus \mathbb{Z}_3$ com o conjunto $\{0,1,\ldots,11\}$, temos

$$G_0 = \{0,1,2\} \quad G_1 = \{3,4,5\} \quad G_2 = \{6,7,8\} \quad G_3 = \{9,10,11\}$$

A coloração $\acute{\chi} : \acute{V} \times \acute{V} \to \{0,1,2,3\}$ definida pela tabela abaixo não produz 2-quadrado monocromático

	cor 0	*cor* 1	*cor* 2	*cor* 3
0	9 3 6	1 10 7	2 5 11	0 4 8
1	9 4 7	2 10 8	0 3 11	1 5 6
2	9 5 8	0 10 6	1 4 11	2 3 7
3	0 10 8	1 5 11	9 3 7	2 4 6
4	1 10 6	2 3 11	9 4 8	0 5 7
5	2 10 7	0 4 11	9 5 6	1 3 8
6	0 5 11	9 3 8	2 10 6	1 4 7
7	1 3 11	9 4 6	0 10 7	2 5 8
8	2 4 11	9 5 7	1 10 4	0 3 6
9	0 1 2	3 4 5	6 7 8	9 10 11
10	3 4 5	6 7 8	9 10 11	0 1 2
11	6 7 8	9 10 11	0 1 2	3 4 5

Já observamos que a classe de colorações construída na prova do teorema 1.3 não funciona para r potência de primo. No entanto, podemos propor outra contrução para tal resultado fazendo uso do lema 1.16 .

Teorema 3.5 Para $q = p^n$potência de primo vale $q^2 < p(2, q, 2)$.

Prova: Considere $GF_{(q)}$ o grupo de Galois com q elementos. Pelo lema 1.16 , existem $q-1$ quadrados latinos de ordem q com entradas em $GF_{(q)}$. Através de uma bijeção entre $\mathbb{Z}_q$ e $GF_{(q)}$ transforme estas $q-1$ matrizes em quadrados latinos, digamos $A_1, A_2, \ldots, A_{q-1}$, cujas entradas estão em $\mathbb{Z}_q$.

A proposição 1.12 garante a ortogonalidade mútua entre estes novos quadrados latinos e a matriz:

$$A_0 = \begin{bmatrix} 0 & 1 & \ldots & q-1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \ldots & q-1 \end{bmatrix}$$

Considere a q-coloração $\chi : (\mathbb{Z}_q \oplus \mathbb{Z}_q)^2 \to \{0, 1, \cdots, q-1\}$ da seguinte forma. Para todo $(a, b) \in (\mathbb{Z}_q \oplus \mathbb{Z}_q)$ e para toda cor j, defina $\chi(\ (a, b), (c, d)\ ) = j$ se e somente se

$$(c, d) \in \{(0, A_0(a, b) + j),\ (1, A_1(a, b) + j), \ldots, (q-1, A_{q-1}(a, b) + j)\}$$

Da ortogonalidade mútua do conjunto $\{A_0, A_1, A_2, \ldots, A_{q-1}\}$ prova-se a inexistência de 2-subconjunto monocromático para a função χ. □

Teorema 3.6: Se $a < \rho(t, r, 2)$ então $\left[\frac{m-1}{t-1}\right] . a < \rho(m, r, 2)$ para $m \geq t$.

Prova: Sejam $l = \left[\frac{m-1}{t-1}\right]$, $V = \mathbb{Z}_l \oplus \mathbb{Z}_a$ e χ uma r-coloração desejada.

Por hipótese, para cada $i, 0 \leq i \leq l-1$, existe uma função $\chi_i : (\{i\} \times \mathbb{Z}_a)^2$ que não apresenta t-subconjunto monocromático. Fixemos uma cor dentre estas, digamos 0 .

Para cada $x \in \mathbb{Z}_a$, denote por:

i) $T_i(x)$ o subconjunto de $\{i\} \times \mathbb{Z}_a$ tal que $(i, x) \times T_i(x)$ é pintado de 0 com respeito a χ_i ,onde $0 \leq i \leq l-1$

ii) $A(x) = T_0(x) \cup T_1(x) \cup \ldots \cup T_{l-1}(x)$.

Agora, pintamos com a cor 0 as células de V^2 que pertencem à família $(i, x) \times A(x)$, $0 \leq i \leq l-1$. Tomando-se o mesmo procedimento para as outras cores, construímos a coloração χ.

Não existem subconjuntos $Q_1 \subset V, Q_2 \subset V$ com $|Q_1| \geq m$, $|Q_2| \geq m$ e $\chi(Q_1 \times Q_2) = \{0\}$. Suponha que $\{y_1, y_2, \ldots, y_m\} \subset Q_2$. Como V foi particionado em $\left[\frac{m-1}{t-1}\right]$ classes , existem t destes $y's$ contidos numa única classe considerada, digamos $\{y_1, y_2, \ldots, y_t\} \subset V_0$.

Por hipótese, $\{y_1, y_2, \ldots, y_t\}$ aparece no máximo $t-1$ vezes nos blocos do tipo $T_0(x)$. Assim, $\{y_1, y_2, \ldots, y_t\}$ aparece no máximo $(t-1)\left[\frac{m-1}{t-1}\right] < m$ vezes como subconjunto de blocos do tipo $A(x)$. Logo, $\{y_1, y_2, \ldots, y_t\}$ não chega a estar contido em m blocos de χ na cor 0 .□

Corolário 3.7 :Se $a < \rho(2, r, 2)$ então $(m-1)a < \rho(m, r, 2)$ para $m \geq 2$.

Prova: Basta tomar $t = 2$ no teorema acima.□

Teorema 3.8 [Ca3]: Se $m \geq 3$ ou $r \geq 3$ então $(m+1)r < \rho(m, r, 2)$.

Prova Denote por $\langle a/b \rangle$ a estrutura formada pela matriz $(m+1) \times (m+1)$ cuja diagonal principal recebe a cor a e as entradas restantes, cor b . Fixe um quadrado S descrito pela superposição de dois quadrados latinos $r \times r$, por exemplo:

$$S = \begin{bmatrix} \langle 0/1\rangle & \langle 1/2\rangle & \dots & \langle r-1/0\rangle \\ \langle 1/2\rangle & \langle 2/3\rangle & \cdots & \langle 0/1\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle r-1/0\rangle & \langle 0/1\rangle & \dots & \langle r-2/r-1\rangle \end{bmatrix}$$

Vamos mostrar que não existe quadrado $m \times m$ homogêneo contido na matriz $r(m+1) \times r(m+1)$ gerada por S. Fixe a cor 0. Para cada linha i, denote por L_i o conjunto de colunas tal que $\{i\} \times L_i$ tenha cor 0. Por construção, $|L_i| = m+1$ para todo i.

Mais ainda, $|L_i \cap L_j| \leq m-1$ para $i \neq j$. De fato; seja $|L_i \cap L_j| \geq m$, então obrigatoriamente estas m colunas em comum aparecem em estruturas do tipo $\langle a/0\rangle$. No entanto, como se vê diretamente da construção de S, não há duas estruturas distintas $\langle a/0\rangle$ e $\langle b/0\rangle$ numa mesma linha ou coluna de S, desde que a formação deste quadrado provém da concatenação de dois quadrados latinos. Forçosamente $i = j$. □

Nota: A restrição $m \geq 3$ ou $r \geq 3$ se explica porque, no caso $m = r = 2$, temos a matriz gerada por S:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Note que os pontos centrais formam um quadrado 2×2 de cor 0.

As idéias relativas à construção acima e argumentos de cardinalidade podem ser aplicados no resultado seguinte

Teorema 3.9 :$25 \leq \rho(3,3,2)$.

Prova: Conforme a prova acima, tome estruturas de tamanho 4×4 $\langle a/b\rangle$ formadas pelas cores 0, 1 e 2. Seja S o quadrado 6×6:

$$S = \begin{bmatrix} \langle 0/1\rangle & \langle 0/2\rangle & \langle 1/0\rangle & \langle 2/0\rangle & \langle 1/2\rangle & \langle 2/1\rangle \\ \langle 0/2\rangle & \langle 1/0\rangle & \langle 2/0\rangle & \langle 1/2\rangle & \langle 2/1\rangle & \langle 0/1\rangle \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \langle 2/1\rangle & \langle 0/1\rangle & \langle 0/2\rangle & \langle 1/0\rangle & \langle 2/0\rangle & \langle 1/2\rangle \end{bmatrix}$$

Para evitar confusão, trocaremos o substantivo "linha de S " por "bloco de S ". Considere a matriz 24×24 gerado por S . Fixe a cor 0 e assuma a mesma definição dada para L_i na demonstração anterior.

Falta provar a inexistência de 3-subconjunto monocromático. Sejam 3 linhas distintas L_i, L_j, L_k tal que $|L_i \cap L_j \cap L_k| \geq 3$, digamos que o 3-subconjunto de colunas $\{c_1, c_2, c_3\}$ está em $\{L_i, L_j, L_k\}$. Devido às simetrias das linhas, podemos supor $i = 1$. Assim:

$$\{c_1, c_2, c_3\} \subset \{1, 5, 10, 11, 12, 14, 15, 16\}$$

Claramente $\{1, 5\} \cap (L_1 \cap L_j \cap L_k) = \emptyset$.

Devido às simetrias da coloração, os 3-subconjunto formados pelas 6 colunas restantes podem ser reduzidos, sem perda de generalidade, em apenas dois casos:

$$\begin{array}{lll} c_1 = 10 & c_2 = 11 & c_3 = 12 \\ c_1 = 10 & c_2 = 11 & c_3 = 14 \end{array}$$

No primeiro caso, as colunas $\{10, 11, 12\}$ apareceriam em 3 estruturas $\langle a/0\rangle$. No entanto, só há 2 delas. Assim, $|\{1, j, k\}| < 3$, levando a uma contradição.

Analisemos a segunda possibilidade ($c_3 = 14$). Como $|L_i \cap L_j \cap L_k| \geq 3$, temos $|L_1 \cap L_j| \geq 3$ e $|L_1 \cap L_k| \geq 3$. Assim, estas duas linhas estão obrigatoriamente nos blocos 1, 2 ou 6 de S .

A 14^a componente de cada linha gerada pelo segundo bloco de S diferem de 0 ($S(2.4) = \langle 1/2\rangle$). Por outro lado, não aparece o vetor $(0, 0)$ nas coordenadas 10 e 11 das linhas geradas pelo sexto bloco de S ($S(6, 3) = \langle 0/2\rangle$).

Resta a possibilidade $\{j, k\}$ são linhas do 1^o bloco. Por simples inspeção concluímos $\{1, j, k\} \subset \{1, 4\}$, levando novamente a uma contradição, pois supomos L_1, L_j, L_k mutuamente distintas.□

O próximo corolário provém de relações entre resultados apresentados neste capítulo.

Corolário 3.11: Para r primo, q potência de primo, $m \geq 2$ e $a \geq 3$ valem:

1. $(m-1).q^2 < \rho(m, q, 2)$
2. $(m-1).(r+1).r < \rho(m, r+1, 2)$
3. $3.(m-1).a < \rho(m, a, 2)$

Prova: Os ítens (1) e (2) provém de aplicações diretas dos teoremas 3.3, 3.5 e 3.6. Pelo teorema 3.8, temos $3a \not\to (2)^2_a$ quando $m = 2$ e assim pelo corolário 3.7, $3(m-1)a \not\to (m)^2_a$.□

Até agora, todos os resultados desta seção apresentam provas construtivas. Este procedimento não é o único possível.

De fato, o *método probabilístico de Erdös* , o qual fornece provas existenciais de estruturas finitas com certas propriedades, foi utilizado na prova do seguinte limite inferior para a função de Ramsey (ver [GRS])

" Para todo $t \geq 3$, $R(t, 2, 2) > 2^{\frac{t}{2}}$ "

Baseado nesta demonstração, propomos resultado similar para a função polarizada. O símbolo K_{nn} denota um grafo bipartido completo de dimensão (n, n) . Desta forma, um t-subconjunto monocromático é isomorfo ($\sim$) a um K_{tt} monocromático.

Teorema 3.12 Se $\binom{n}{t}^2 r^{1-t^2} < 1$ então $\rho(t, r, 2) > n$.

Prova Vamos mostrar que existe uma função $K_{nn} \to \{0, 1, \ldots, r-1\}$ desprovida de t-subconjunto homogêneo. Considere Ω o espaço amostral formado por todas as r-colorações de K_{nn} e a probabilidade P definida por: $P[(a, b)] = \frac{1}{r}$ para toda aresta (a, b) em K_{nn} .

Dado S um subgrafo de K_{nn} isomorfo a K_{tt} , denotando por A_S o evento " S é monocromático", temos $P[A_s] = r^{1-t^2}$. Se $\bigvee_{S \sim K_{tt}} A_S$ representa o evento "algum t-subconjunto é homogêneo " , então

$$P\left[\bigvee_{S \sim K_{tt}} A_S\right] \leq \sum_{S \sim K_{tt}} P[A_S] \leq \binom{n}{t}^2 r^{1-t^2}$$

Por hipótese, alguma r-coloração de K_{nn} está no complementar do evento $\bigvee_{S \sim K_{tt}} A_S$.□

Exemplo 3.13

(a) Para $r = 2$, $t = 6$ e $n = 25$,

$$\binom{25}{6} = 177.100 < 185.363, \ldots = \sqrt{2^{25}}$$

Conforme 3.12, $\rho(6, 2, 2) > 25$, melhorando o limite $\rho(6, 2, 2) > 20$ (corolário 3.11)

(b) Mais ainda:

$\rho(t, 2, 2) > 39, 61, 94, 144$, respectivamente para $t = 7, 8, 9, 10$

os quais melhoram as estimativas determinadas pelo corolário 3.11 .

4 Delimitações superiores

Como vimos, basta exibir uma única r-coloração de a^n desprovida de qualquer t-subconjunto homogêneo para valer o limite inferior $a < \rho(t, r, n)$. Por outro lado, para valer a desigualdade $\rho(t, r, n) \leq a$ é necessário mostrar que todas as r-colorações de a^n contém um t-subconjunto monocromático.

Nesta seção veremos os poucos resultados referentes a tais limites. Iniciamos com dois resultados obtidos em [Ca3].

Lema 4.1 [Ca3] Para $n \geq 1$, $l > t$ e $\{a_i, 1 \leq i \leq n\}$ um conjunto de n inteiros , temos

$$\sum_{i=1}^{n} \binom{l + a_i}{t} \geq n \binom{l}{t} \qquad \text{se } \sum_{i=1}^{n} a_i = 0 \tag{1}$$

onde $\binom{x}{t}$ denota a função binomial sujeita à convenção $\binom{x}{t} = 0$ para $x < t$.

Prova : Por indução em n . A afirmação é verdadeira quando $n = 1$. Suponha que seja válida para $n \geq 1$. Se $a_{n+1} = 0$, (1) se verifica. Para $a_{n+1} \neq 0$, obtemos a desigualdade acima aplicando um número finito de vezes a relação:

$$\binom{l + a_j - 1}{t} + \binom{l + a_k + 1}{t} \leq \binom{l + a_j}{t} + \binom{l + a_k}{t} \tag{2}$$

se $a_j - 1 \geq a_k$.

Falta verificar (2) . Da identidade de Pascal: $\binom{x}{y-1} + \binom{x}{y} = \binom{x+1}{y}$, vem:

$$\binom{l + a_k}{t - 1} = \binom{l + a_k + 1}{t} - \binom{l + a_k}{t} \text{ e } \binom{l + a_j - 1}{t - 1} = \binom{l + a_j}{t} - \binom{l + a_j - 1}{t}$$

De $a_j - 1 \geq a_k$ obtemos $\binom{l+a_k}{t-1} \leq \binom{l+a_j-1}{t-1}$, provando a relação (2).□

Teorema 4.2 [Ca3] : Se $n^2 > r(k-1)$ para k onde

$$n\binom{\left[\frac{k}{n}\right]}{t} > (t-1)\binom{n}{t} \quad , \quad \left[\frac{k}{n}\right] \geq t$$

então $\rho(t, r, 2) \leq n$.

Prova: Se $n^2 > r(k-1)$ então, dado uma r-coloração de n^2 , sempre existe uma cor com pelo menos k células. Tome um subconjunto S formado por $n\left[\frac{k}{n}\right] \leq k$ pares ordenados da cor mencionada e considere a partição de S : $(a, b) \sim (c, d)$ se e somente se $a = c$.

Há no máximo n classes, cada uma contendo $\left[\frac{k}{n}\right] + a_i$ células (a_i pode ser negativo), sujeito à restrição :

$$\sum_{i=1}^{n}\left(\left[\frac{k}{n}\right] + a_i\right) = n\left[\frac{k}{n}\right]$$

De cada classe podemos extrair $\binom{\left[\frac{k}{n}\right]+a_i}{t}$ t-subconjuntos de n . Tomando-se $l = \left[\frac{k}{n}\right]$, o lema acima fornece:

$$\sum_{i=1}^{n}\binom{l+a_i}{t} \geq n.\binom{l}{t}$$

Da hipótese e do Princípio da Casa do Pombo garante-se a existência de um t-subconjunto homogêneo em S.□

Exemplos 4.3 De acordo com o teorema 4.2, as melhores delimitações encontradas nos exemplos abaixo são:

$$\rho(2,2,2) \leq 6 \quad \rho(2,3,2) \leq 12 \quad \rho(3,2,2) \leq 20$$

Corolário 4.4 Para qualquer $r \geq 2$, $\rho(2, r, 2) \leq r(r+1)$.

Prova Aplicação direta do teorema. Dado $r \geq 2$, tome $n = r(r+1)$ e $y = \left[\frac{k}{n}\right]$

$$\frac{n.y.(y-1)}{2} > \frac{n.(n-1)}{2}.1 \Leftrightarrow y.(y-1) > r.(r+1) - 1$$

Se $y = r + 1$, a desigualdade acima vale. Tome o menor k tal que $y = \left[\frac{k}{n}\right]$, ou seja , $k = r.(r+1)^2$. Como $r^2.(r+1)^2 > (r.(r+1)^2 - 1).r$, temos $n^2 > r.(k-1)$, satisfazendo às condições do teorema.

Nos próximos resultados desta seção utilizaremos a nomenclatura

$$\| x \|_t = \sum_{i=1}^{n} \binom{x_i}{t}$$

onde t é um número natural e x um vetor n-dimensional , $x = (x_1, x_2, \ldots, x_n)$. Para facilitar a leitura, os índices da somatória serão omitidos quando não houver perigo de confusão.

Teorama 4.5 Seja $k \geq 2$ e m um número natural, vale :

$$\min\{ \| x\|_t : \| x\|_1 = m\} = v\binom{\left[\frac{m}{n}\right]}{t} + (n-v)\binom{\left[\frac{m}{n}\right]}{t} \qquad (3)$$

onde $v = m - n\left[\frac{m}{n}\right]$.

Prova: Usaremos as notações e desigualdades do lema 4.1. Definindo $l = \left[\frac{m}{n}\right]$, $a_i = x_i - l$ para $1 \leq i \leq n$ e $a = (a_1, a_2, \ldots, a_n)$, obtemos $\sum a_i = v$ devido à condição restritiva $\| x\|_1 = m$. Vamos analisar dois casos. A igualdade (3) se verifica para $\frac{m}{n}$ natural ;basta aplicar lema 4.1,pois $\sum a_i = v = 0$. Caso contrário, se $\frac{m}{n}$ não é natural, temos $0 < \frac{m}{n} - \left[\frac{m}{n}\right] < 1$ e assim $0 < \sum a_i = v < n - 1$. A igualdade abaixo vale:

$$\min\{ \| (l + a_1, l + a_2, \ldots, l + a_n)\|_t : \| a \|_1 = v\} = v\binom{\left[\frac{m}{n}\right]}{t} + (n-v)\binom{\left[\frac{m}{n}\right]}{t}$$

De fato, a melhor solução desse problema de mínimo se verifica quando há v a_is com valor 1 e $(n-v)$ com valor 0 ; pois se $a_j - a_k \geq 2$, podemos aplicar a desigualdade (2) . Como $\sum a_i = v < n - 1$, as soluções possíveis $(a_1, a_2, \ldots, a_n)$ têm v valores iguais a 1 e os $(n-v)$ valores restantes iguais a 0 . Mas:

$$\min\{ \| (l + a_1, l + a_2, \ldots, l + a_n)\|_t : \| a \|_1 = v\} = \min\{ \| x\|_t : \| x\|_1 = m\}$$

e isto completa a prova.□

Comentário A solução da classe de problemas de programação inteira estabelecida pelo teorema acima propicia determinação de novos limites superiores . Mais ainda, até o final deste capítulo, veremos aplicações deste resultado. Entre estas, cotas superiores de ρ e da função relativa ao problema de Zarankiewicz (seção 5) melhoram as propostas obtidas por vários pesquisadores. Desta forma, embora de demonstração simples, o teorema 4.5 tem se revelado eficaz ; configurando-se como o principal resultado desta seção .

Teorema 4.6: Se $\min\{ \| x\|_t : \| x\|_1 \geq \left\rceil \frac{n^2}{r} \right\lceil \} > (t-1).\binom{n}{t}$ então $\rho(t,r,2) \leq n$.

Prova: Claramente, para $m \leq u$ temos:

$$\min\{ \| x\|_t : \| x\|_1 = m\} \leq \min\{ \| x\|_t : \| x\|_1 = u\}$$

Em uma r-coloração de n^2 há n^2 células distribuídas em r cores. Por hipótese, existe uma cor, digamos azul, com pelo menos $\left\rceil \frac{n^2}{r} \right\lceil$ células. Considere x_i como sendo o número de células pintadas de azul na linha i , para $1 \leq i \leq n$. Da observação inicial e hipótese, concluímos que existe um subconjunto C de colunas, com $|C| \geq t$, aparecendo num subconjunto L das linhas t vezes. Assim, $L \times C$ forma um conjunto homogêneo.□

Corolário 4.7: Para qualquer $r \geq 2$, $\rho(2,r,2) \leq r(r+1)-1$.

Prova: Aplicação direta de 4.6 . Dado r , tomamos $n = r(r+1)-1$ e $m = \left\rceil \frac{n^2}{r} \right\lceil$, ou seja, $m = r^3 + 2r^2 - r - 1$. Como

$$r(r(r+1)-1) < r.(r+1)^2 - 2(r+1) + 1 = m < (r+1)(r(r+1)-1)$$

temos $\left\rceil \frac{m}{n} \right\lceil = r+1$ e $\left\lceil \frac{m}{n} \right\rceil = r$. Por 4.5 , há $(r+1)(r(r+1)-1) - m = r$ componentes x_i de valor r e r^2-1 de valor $r+1$, ou seja:

$$\min\{ \| x\|_t : \| x\|_1 = m\} = r.\frac{r.(r-1)}{2} + (r^2-1).\frac{r.(r+1)}{2} > \binom{n}{2}$$

satisfazendo às condições de 4.6 .□

Exemplos 4.8: Conforme 4.6 , as delimitações são:

$$\rho(2,2,2) \leq 5 \qquad \rho(2,3,2) \leq 11 \qquad \rho(3,2,2) \leq 19$$

as quais fornecem melhores estimativas do que às encontradas via 4.2 , mesmo para o último caso, quando $t = 3$.

Nota Estes exemplos não são fatos isolados; da comparação entre esses teoremas, podemos notar que o último fornece estimativas melhores para quaisquer valores de t e r. De fato, dados t e r, sejam n e k satisfazendo às condições de 4.2:

$$k < \frac{n^2}{r} + 1 \Leftrightarrow k \leq \frac{n^2}{r} \leq \left]\frac{n^2}{r}\right[$$

Da hipótese e desde que $n\left[\frac{k}{n}\right] \leq \left]\frac{n^2}{r}\right[$, valem as desigualdades:

$$(t-1).\binom{n}{t} < \min\{\ \|\ x\|_t :\ \|\ x\|_1 = n.\left[\frac{k}{n}\right]\} \leq \min\{\ \|\ x\|_t :\ \|\ x\|_1 = \left]\frac{n^2}{r}\right[\}$$

Em outras palavras; dados t e r, se n satisfaz o teorema 4.2 então o mesmo n também satisfaz às condições do teorema 4.6. Portanto, este último fornece um menor ou igual limite superior.

O resultado 4.5 também é útil na determinação do número máximo de células de uma cor sem que esta apresente um conjunto monocromático de certa ordem. Para ilustrar esta declaração, levantamos a conjectura seguinte:

Conjectura 4.9: $\rho(2,3,2) = 10$.
Evidências: Já sabemos que $9 < \rho(2,3,2) \leq 11$. Claramente, se $m \geq 36$

$$\min\{\ \|\ x\|_2 :\ \|\ x\|_1 = 36\} > \binom{10}{2} = 45 \Rightarrow \min\{\ \|\ x\|_2 :\ \|\ x\|_1 = m\} > 45$$

Vamos mostrar a primeira desigualdade do problema de programação linear inteira descrito acima. Por 4.5, a solução mínima $x = (x_1, x_2, \ldots, x_n)$ tem 6 coordenadas com valor 4 e 4 coordenadas de valor 3, assim

$$\min\{\ \|\ x\|_2 :\ \|\ x\|_1 = 36\} = 6.\binom{4}{2} + 4\binom{3}{2} = 48 > 45$$

formando um 2-conjunto monocromático, ou seja, se $10 < \rho(2,3,2)$ então nenhuma cor pode ter 36 células. São 100 células distribuidas em 3 cores,

digamos, azul, verde e amarela. Restam , sem perda de generalidade, apenas as configurações seguintes:

$$(35, 35, 30) \quad (35, 34, 31) \quad (35, 33, 32) \quad (34, 34, 32) \quad (34, 34, 33)$$

onde as entradas dos vetores representam o número de células da coloração respectivamente nas cores azul, verde e amarela.

Afirmamos que nenhuma cor pode ter 35 células caso aconteça $10 < \rho(2, 3, 2)$. Seja a cor azul com 35 células. Por 4.5, a solução mínima $x = (x_1, x_2, \ldots, x_n)$ tem 5 coordenadas de valor 4 e 5 de valor 3 para o problema $\min\{ \| x\|_2 : \| x\|_1 = 35\}$, cujo valor é 45.

Para não formar 2-conjunto monocromático, todos os 2-subconjuntos $\{i, j\}$ $0 \leq i \neq j \leq 10$ devem aparecer um única vez. Como há 5 blocos de tamanho 4 e 5 blocos de tamanho 3, então deverá aparecer um elemento, digamos o "1", em pelo menos dois blocos de tamanho 4. Temos:

(i) num bloco de tamanho 4, o elemento "1" se relaciona com os outros 3 elementos, formando 3 2-subconjuntos do tipo $\{i, j\}$;

(ii) num bloco de tamanho 3, o elemento "1" se relaciona com os outros 2 elementos, formando 2 2-subconjuntos do tipo $\{i, j\}$.

Como todos os $\{1, j\}$ (são ao todo 9) devem ocorrer uma única vez, nos deparamos com a equação diofantina $3.a + 2.b = 9$ cujas possíveis soluções são:

$$a = 3\ b = 0 \quad ou \quad a = 1\ b = 3$$

O elemento "1" aparece em pelo menos dois blocos de tamanho 4 ($a > 1$). Assim, este elemento está em 3 blocos de tamanho 4 ($a = 3$) e em nenhum bloco de tamanho 3 ($b = 0$) . Ou seja, 3 dos blocos têm a configuração: $(1, \_, \_, \_)$, onde os espaços vazios são preenchidos com outros elementos.

Para a formação do quarto bloco de tamanho 4, precisaremos repetir um 2-subconjunto contido em um dos 3 blocos iniciais já descritos. É inevitável a formação do 2-conjunto monocromático na cor com 35 células.

Continuam os casos: $(34, 34, 32)$ $(34, 33, 33)$. Se $10 < \rho(2, 3, 2)$, então obrigatoriamente a 3-coloração de $\{0, 1, \ldots, 9\}^2$ que não possui conjunto homogêneo apresenta uma das duas configurações restantes.

Testamos diversas colorações dessas configurações restantes do seguinte modo: Criamos 34 células que não apresentam conjunto monocromático cujos blocos são:

$\{0\,1\,2\,3\}\{0\,4\,5\,6\}\{1\,4\,7\,8\}\{2\,5\,8\,9\}\{0\,7\,9\}\{1\,6\,9\}\{3\,5\,7\}\{3\,4\,9\}\{2\,6\,7\}\{3\,6\,8\}$

(eliminamos as vírgulas). Em seguida, geramos colorações das células restantes através do pacote "Mathematica", ver [Wo]. Foram feitas centenas de tentativas e em todas, encontradas conjunto homogêneo.

Esses testes corroboram a nossa conjectura.

Tabelas de limites: função polarizada

Apresentamos os limites de $\rho(t,\ r,\ n)$ para os casos iniciais de t e r , com $n = 2$ ($I \leq \rho(t,\ r,\ 2) \leq S$. A coluna da esquerda de cada tabela indica limite inferior (I) bem como sua justificativa (expoente de I) dada através do apêndice abaixo. Cotas superiores (coluna da direita: S) foram obtidos via 4.5 , 4.6 e 4.7 .

$\rho(2,\ r,\ 2)$		
I	r	S
5^A	2	5
10^A	3	11
17^A	4	19
26^A	5	29
31^B	6	41
50^A	7	55
65^A	8	71
82^A	9	89
91^B	10	109

$\rho(3,\ r,\ 2)$		
I	r	S
10^C	2	19
25^E	3	61
33^{D_i}	4	137
51^{D_i}	5	262
$61^{D_{ii}}$	6	447
98^{D_i}	7	704
128^{D_i}	8	1045
162^{D_i}	9	1482
162^F	10	2027

$\rho(4,\ r,\ 2)$		
I	r	S
13^{D_i}	2	55
28^{D_i}	3	255
65^{D_i}	4	786
76^{D_i}	5	1899

Apêndice: resumo de limites

Se q é potência de primo, r primo, m e a naturais :

(A) $q^2 < \rho(2,\ q,\ 2)$. (teorema 3.5)

(B) $r(r+1) < \rho(2,\ r+1,\ 2)$. (teorema 3.3)

(C) se $r \geq 3$ ou $m \geq 3$, então $r.(m+1) < \rho(m,\ r,\ 2)$. (de 3.8)

(D)
$$\begin{cases} (i) & q^2(m-1) < \rho(m,\ q,\ 2) \\ (ii) & r(r+1)(m-1) < \rho(m,\ r+1,\ 2) \quad \text{(por 3.11)} \\ (iii) & 3.a.(m-1) < \rho(m,\ a,\ 2) \end{cases}$$

(E) $24 < \rho(3,\ 3,\ 2)$ (por 3.9)

(F) regras de monotonicidade (2.1)

5 O problema de Zarankiewicz

Nesta seção, pretendemos estabelecer a conexão entre dois problemas aparentemente independentes, a saber, a função polarizada e o problema de Zarankiewicz.

Através desta conexão, é possível "traduzir" delimitações entre as funções ρ e K (relativa ao problema de Zarankiewicz).

Partindo de resultados deste capítulo (seções 3 e 4), tal tradução de valores fornece boas estimativas para K , chegando inclusive a apresentar limites superiores ótimos em alguns casos. Mais ainda, outros casos melhoram as estimativas obtidas por alguns pesquisadores (ver [GZ] e [Zn]).

Motivados pela conexão entre K e ρ , propomos uma generalização do problema de Zarankiewicz.

5.1 Introdução

Zarankiewicz, em 1951, propôs o problema seguinte.

> Seja A_n uma matriz quadrada de ordem n , cujas entradas recebem exclusivamente as cores 0 e 1 . O problema de Zarankiewicz consiste em determinar o menor número de $1's$ em A_n de modo que assegure a existência de uma submatriz de ordem t formada apenas pela cor 1 , onde $2 \leq t < n$. Tal número será denotado por $K_t(n)$.

Convém notar que $K_t(n)$ independe de permutação das cores 0 e 1 , isto é, a cor da submatriz homogênea não interfere na determinação de $K_t(n)$.

Guy e Znám mencionam, na introdução do artigo [GZ], resultados referentes à delimitações superiores de $K_t(n)$, alguns deles obtidos por outros pesquisadores via conexão com a Teoria dos Grafos. Citamos alguns:

- $K_t(n) \leq t.n + \left[(t-1)^{\frac{1}{t}}.n^{(\,2-\frac{1}{t})}\right]$ (1)

- $K_t(n) \leq 1 + \left[\frac{n.(t-1)}{2} + (t-1)^{\frac{1}{t}}.n^{(\,2-\frac{1}{t})}\right]$ (2)

- $K_3(n) \leq 1 + n + \left[n.(2.n^2 - \frac{11.n}{2} + \frac{9}{2})^{\frac{1}{3}}\right]$ (3)

- O principal resultado de [GZ], cuja prova utiliza argumentos de Análise Real, afirma: se A_n possui mais de $n.u$ 1's e

$$n.\binom{u}{t} \geq (t-1).\binom{n}{t} \text{então } K_t(n) \leq 1+\lfloor n.u \rfloor \tag{4}$$

O artigo [Zn] mostra :

- $K_t(n) \leq 1 + \left\lfloor \frac{n.(t-1)}{2} + (t-1)^{\frac{1}{t}}.n.\left(n - \frac{3}{8}(t-1)^{\left(1-\frac{1}{t}\right)} \right) \right\rfloor$ (5)

- $$K_t(n) \leq 1 + \left\lfloor \frac{n.(t-1)}{e} + (t-1)^{\frac{1}{t}}.n^{\left(2-\frac{1}{t}\right)} \right\rfloor$$
  onde $e = (2.f-1)/(f-1)$, $(t-1).f^t = n$ (6)

5.2 Conexão entre ρ e K

Dado $t \geq 2$, considere a função: $g_t(n) = K_t(n) - \left\rceil \frac{n^2}{2} \right[$, onde $\rceil x \lfloor$ denota o menor inteiro não inferior a x. De acordo com a desigualdade (1),

$$\lim_{n \to \infty} g_t(n) = -\infty \qquad (\forall t \geq 2)$$

Assim, a seguinte função de mínimo está bem definida:

$$\min \left\{ a \in I\!N : K_t(a) - \left\rceil \frac{a^2}{2} \right[\leq 0 \right\}$$

O próximo resultado vai ao encontro dessa questão, cuja resposta relaciona-se com a função ρ . Antes disso, convém observar que uma partição de A_n em r cores sempre pode ser reduzida a uma partição com 2 cores, e vice-versa. Desse modo, $K_t(n)$ não depende da quantidade de cores e da cor da submatriz de ordem t.

Lema 5.1: Dados $t \geq 2$ e $r \geq 2$,

$$\text{se } K_t(a) \leq \left\rceil \frac{a^2}{r} \right[\text{ então } a \rightrightarrows (t)_r$$

Prova: Dada uma r-coloração de a^2, sempre existe uma cor com pelo menos $\left\rceil \frac{a^2}{r} \right[$ células. Esta cor apresenta t-subconjunto homogêneo pois assumimos que $K_t(a) \leq \left\rceil \frac{a^2}{r} \right[$. □

Teorema 5.2: Para $t \geq 2$ e $r \geq 2$,

$$\rho(t, r, 2) \leq \min \left\{ a \in I\!N : K_t(a) \leq \left] \frac{a^2}{r} \right[\right\}$$

Prova: Consequência direta do lema anterior. □

Através dos resultados da seção 4 e do teorema 5.2 obtém-se diretamente

Corolário 5.3 Seja q potência de primo, r primo e a qualquer, então:

(a) $K_2(y) > \left] \frac{y^2}{q} \right[$ para $y \leq q^2$

(b) $K_2(y) > \left] \frac{y^2}{r+1} \right[$ para $y \leq (r.(r+1))^2$

(c) $K_3(y) > \left] \frac{y^2}{2} \right[$ para $y \leq 24$

Nota A matriz 5×5 abaixo, com 12 elementos 1 's , não forma submatriz de ordem 2 nesta cor

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

Mais ainda, não é difícil ver que $K_2(5) = 13$ (ver próximo resultado). Os fatos $5 \rightrightarrows (2)_2$ e $\left] \frac{5^2}{2} \right[= 13$ sugerem a validada da recíproca de 5.1. Por outro lado, um argumento adicional usado na corroboração da conjectura $\rho(2, 3, 2) = 10$ (seção 4) é $K_2(10) = 35$. Assim, a recíproca de 5.1 resultaria falsa se $10 \rightrightarrows (2)_3$.

Teorema 5.4: Se $\min\{\|x\|_t : \|x\|_1 = m\} > (t-1).\binom{n}{t}$ então $K_t(n) \leq m$.
Prova Análoga à demonstração do teorema 4.6 .□

Este resultado, em conjunto com 4.5 , permite determinar novos limites para a função K. Vejamos alguns exemplos.

Exemplo 5.5: $K_4(8) \leq 53$ e $K_4(9) \leq 65$. Faremos apenas a prova do primeiro limite. Tome $m = 53$, por 4.5

$$\min\{\|x\|_4 : \|x\|_1 = 53\} = 5.\binom{7}{4} + 3.\binom{6}{4} = 220$$

Mas $220 > 3.\binom{8}{4} = 210$, satisfazendo às condições do corolário 5.??. Estas cotas melhoram em uma unidade os limites obtidos em [Zn]($K_4(8) \leq 54$ e $K_4(9) \leq 66$).

Também obtemos $K_4(6) \leq 32$ e $K_4(7) \leq 43$, as quais são cotas superiores ótimas, desde que $K_4(6) > 31$ e $K_4(7) > 42$ (ver [Zn]).

Exemplo 5.6 De acordo com 4.5 e 5.4 , temos $K_3(19) \leq 181$. Por outro lado, as estimativas determinadas pelas desigualdades (1) a (6) foram, respectivamente:

$$K_3(19) \leq 227, 190, 182, 182, 185, 184$$

O resultado por nós obtido melhora em uma unidade a cota superior de $K_3(19)$.

5.3 Generalização do problema de Zarankiewicz

Em vista da conexão entre K e ρ , propomos a generalização do problema de Zarankiewicz formulada logo abaixo.

O problema de Zarankiewicz multidimensional e multicolorido:

considere $(\mathbb{Z}_n)^d$ particionada em r cores: $C_1, C_2, \ldots, C_r$. Qual o menor número de células necessárias , $K_t(n,d)$, para garantir a existência de um produto cartesiano $H_1 \times H_2 \times \ldots \times H_d$ ($|H_j| \geq t$) homogêneo nas cores com $|C_j| \geq K_t(n,d)$?

Quando $r = 2$ e $d = 2$, esta nova questão se reduz ao conhecido problema de Zarankiewicz. Claramente $K_t(n,2) = K_t(n)$.

Nestas condições, para todo $t \geq 2$, $r \geq 2$ e $d \geq 2$ valem:

Lema 5.7

$$\text{se } K_t(a,d) \leq \left\lceil \frac{a^d}{r} \right\rceil \text{ então } a \rightrightarrows (t)^d_r$$

Teorema 5.8:

$$\rho(t,r,d) = \min\left\{a \in \mathbb{N} : K_t(a,d) \leq \left\rfloor \frac{a^d}{r} \right\rfloor\right\}$$

As provas são análogas às já vistas. Dessa forma, este generalização mantém a conexão entre K e ρ.

Destacamos duas questões em aberto.

Problema Resultados (exemplos 5.5 e 5.6) sugerem que as cotas determinadas para K via teoremas 5.4 e 4.5 são sempre melhores ou iguais do que as encontradas em alguma das desigualdades (1) a (6). Tal sugestão é correta?

Problema Como estender os teoremas 5.4 e 4.5 para dimensões d superiores a dois ?

Capítulo II

O Problema das Hipertorres

6 Códigos Latinos

6.1 Resultados Básicos

Dados naturais positivos q e n , denotamos por V_q^n o espaço formado por todas os vetores (*palavras*) de tamanho n cujas componentes (*letras*) estão no anel dos inteiros módulo q , $\mathbb{Z}_q$ (*alfabeto* $q-$*nário*).

A *distância de Hamming* $d(x,y)$ entre duas palavras de V_q^n estabelece o número de coordenadas nas quais elas diferem.

Um *código* C consiste simplesmente num subconjunto de V_q^n . Seus elementos recebem o nome de *palavras-código* . Dado C , associamos a este código a distância:

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

Definição 6.1: Seja L um código em V_q^n com q^m palavras-código . Dizemos que L é *d-código latino* se as distâncias de Hamming entre os pontos de L não são inferiores a $r+1$ ($d \geq r+1$) , onde $r = n - m$.

Exemplo 6.2 Seja N formado pelas 8 palavra :

$$\begin{array}{cccc} (0,0,0,0) & (0,0,1,1) & (0,1,0,1) & (0,1,1,0) \\ (1,0,0,1) & (1,0,1,0) & (1,1,0,0) & (1,1,1,1) \end{array}$$

Por simples inspeção, verifica-se que N é 2-código latino em V_2^4.

Exemplo 6.3 Seja L em V_3^4 constituída pelas palavras:

$(0,0,0,0)$	$(1,0,1,2)$	$(2,2,1,0)$
$(0,1,1.1)$	$(1,1,2,0)$	$(2,0,2,1)$
$(0,2,2.2)$	$(1,2,0,1)$	$(2,1,0,2)$

Neste caso, L forma um 3-código latino em V_3^4 .

Na literatura, os códigos latinos recebem vários nomes; por exemplo, também são chamados de *códigos com distância de separação máxima* , ou simplesmente, códigos MDS . A motivação dessa nomenclatura se deve ao fato:

um código MDS de tamanho q^m em V_q^n e $r = n - m$ satisfaz $d \leq r + 1$

O exemplo 6.2 ilustra um caso onde d atinge a distância máxima. Neste exemplo, escolhidas quaisquer $m = 2$ coordenadas, obtemos os 9 vetores de V_3^2 como projeções das palavras-código de L . Em geral, esta propriedade de simetria vale para todo código MDS devido :

Proposição 6.4 [Sn] Seja L um código MDS de tamanho q^m em V_q^n e $d = r + 1$. Então m coordenadas das palavras-código podem ser consideradas como posições de "informações" e as r restantes, como posições de "checagem" (redundantes). Ou seja, com m posições de uma palavra-código é possível recuperar as r remanescentes.

Prova: Há q^m vetores num alfabeto $q-$nário em m posições fixadas. Como $d = r + 1$, duas palavras-código x , y não podem coincidir em todas estas m coordenadas. Caso contrário, $d(x, y) \leq n - m = r$, contrariando a hipótese $d = r + 1$. Assim cada uma das q^m associações possíveis ocorre exatamente numa única palavra-código.

Proposição 6.5 [Sn] Um código q-nário L de tamaho q^2 e $d = r + 1$ equivale a um conjunto de r quadrados latinos mutuamente ortogonais de ordem q .

Prova: Seja $\{L_3, L_4, \ldots, L_{r+2}\}$ um conjunto de r quadrados latinos mutuamente ortogonais de ordem q , onde as entradas estão em $\mathbb{Z}_q$. Construa o código L com q^2 palavras-código

$$L = \{ \ (i, j, L_3(i, j), L_4(i, j), \ldots, L_{r+2}(i, j)) \qquad i, j \in \mathbb{Z}_q \}$$

Dados x e y distintos em L , eles diferem em pelo menos $r-1$ das últimas r coordenadas, devido à ortogonalidade mútua dos quadrados latinos. Mais ainda, se x e y coincidem em uma das duas posições iniciais, então diferem nas r restantes, pois L_k é quadrados latinos . Das observações feitas, $d(x,y) \geq r+1$ para todo $x \neq y$ em L .

Reciprocamente, suponha a existência de um código q-nário L com $|L| = q^2$ Pela proposição 6.4 , todos os vetores $(i,j) \in \mathbb{Z}_q^2$ aparecem exatamente uma única vez nas duas primeiras coordenadas das palavras-códigos. Assim, podemos encarar x em L como função das coordenadas mencionadas: $x = x(i,j)$, onde

$$x(i,j) = (i, j, x_3(i,j), x_4(i,j), \ldots, x_{r+2}(i,j))$$

Para cada k , $3 \leq k \leq r+2$,definimos o quadrado latino : $L_k(i,j) = (x(i,j))_k$ onde $0 \leq i,j \leq q-1$. Variando (i,j) , as projeções dos vetores $x(i,j)$ nas coordenadas k e l contém todos os elementos de $\mathbb{Z}_q^2$. Como há q^2 entradas na concatenação $L_k * L_l$, obrigatoriamente cada par ordenado de $\mathbb{Z}_q^2$ aparece um única vez em $L_k * L_l$. Assim, L_k e L_l são quadrados latinos ortogonais, onde $3 \leq k \neq l \leq r+2$ □.

Exemplo 6.6: Sejam os dois quadrados latinos ortogonais :

$$L_3 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \qquad L_4 = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}$$

Pela proposição acima, definindo $L = \{(i, j, L_3(i,j), L_4(i,j)), 0 \leq i,\ j \leq 2\}$, obtemos o código do exemplo 6.3.

Analogamente, de um código MDS com $m \geq 3$, podemos contruir um conjunto de r "hipercubos" latinos m-dimensionais de ordem q. Estes "hipercubos" terão relação de ortogonalidade como consequência do fato: duas palavras-código não coincidem em mais de $m-1$ coordenadas. A recíproca também se verifica .

É um fato conhecido a não existência de um conjunto com mais de $q-1$ quadrados latinos ("hipercubos") mutuamente ortogonais de ordem q . Assim, pela proposição 6.5 , num código MDS com $m \geq 2$, forçosamente temos $r \leq q-1$ (ou $d \leq q$).

6.2 Códigos Lineares

Até o fim desta seção, q representa um número primo ou potência de primo. Portanto, o alfabeto V_q^n , de todas as n-uplas cujas coordenadas pertencem ao corpo finito $GF_{(q)}$, forma um espaço vetorial. Neste contexto, um *código linear* V é simplesmente um subespaço vetorial de V_q^n.

Exemplo 6.7 : O conjunto constituído pelos 8 vetores :

$$(0,0,0,0,0)\ (1,0,0,1,1)\ (0,1,0,1,0)\ (1,1,0,0,1)$$
$$(0,0,1,0,1)\ (1,0,1,1,0)\ (0,1,1,1,1)\ (1,1,1,0,0)$$

forma um subespaço vetorial N e ,portanto, um código linear.

Considere os vetores de uma base de um código linear V como linhas da matriz associada G . Portanto, um vetor pertence ao código V se e somente se ele é combinação linear das linhas de G .O posto desta matriz se iguala à dimensão de V .

Seja $\overline{V}$ o espaco dual de V em V_q^n e H sua matriz associada.(*matriz checagem* de V) Assim, $v \in V$ se e somente se ele é ortogonal a todas as linhas de H, $vH^t = 0$. Esta igualdade acontece para todo v em V ; em particular, para os vetores da base de G

$$GH^t = 0$$

Exemplo 6.8 O espaço obtido pela dualidade do código em 6.7 é constituído por quatro palavras :

$$(0,0,0,0,0), (1,1,0,1,0), (1,0,1,0,1), (0,1,1,1,1)$$

Os primeiros dois vetores não nulos são lineramente independentes. Neste caso,

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Claramente o núcleo de H coincide com N .

Proposição 6.9 [BM] : Seja V um código linear formado pelo núcleo de uma matriz H. Para cada palavra código v tal que $d(v,0) = s$,existe uma dependência linear de s colunas de H . Reciprocamente, para cada relação

de dependência linear envolvendo s colunas de H, existe uma palavra-código v com $d(v,0) = s$.

Prova: Seja $v = (a_1, a_2, \ldots, a_n)$ um vetor de V_q^n ; v é palavra-código se e somente se $vH^t = 0$, ou , denotando a i-ésima coluna de H por h_i ,

$$a_1h_1 + a_2h_2 + \ldots, a_nh_n = 0$$

O número de colunas de H que aparecem com coeficientes não nulos coincide com o número de componentes não nulas de v . Analogamente, os coeficientes de uma relação de dependência linear sobre as colunas de H são componentes de uma palavra-código.□

Logo, um código linear q-nário com matriz checagem H , tem distância d se e somente se:

(a) todo subconjunto de $d-1$ colunas de H é linearmente independente,

(b) algum subconjunto de d colunas de H é linearmente dependente .

A distância de Hamming é invariante sobre : operações não singulares de permutação de colunas, multiplicação de linhas por constantes não nulas. Consideramos dois *códigos equivalentes* quando um pode ser transformado no outro através de operações descritas neste parágrafo. Em particular, um código linear pode ser tranformado em um equivalente cuja matriz checagem tem a forma : $H = (A; I)$ ou $H = (A; -I)$, onde I denota a matriz identidade $r \times r$.

Desde que todo conjunto de $r+1$ colunas de H é linearmente dependente, temos $d \leq r+1$ e:

Corolário 6.10 [Sn]: Seja V um código linear em V_q^n , com matriz checagem H e m posições de informação. As equivalências valem:

(1) $d = r+1$,

(2) todo conjunto de r colunas de H é linearmente independente,

(3) toda submatriz quadrada de ordem j em A tem determinante não nulo, onde $1 \leq j \leq \min\{r, m\}$.

Prova: ver [Sn]

Dado um código linear MDS em V_q^n com matriz checagem H . Inicialmente tranformamos a matriz checagem na forma $H = (A; I)$. Denotamos

por $\overline{H}$ a matriz $\overline{H} = (A^t; I)$ a qual é contituída pela junção da matriz identidade I_m com a transposta de A . Do corolário 6.10 , $\overline{H}$ é um código linear (chamado *código dual* de V) com $\overline{m} = r$, $\overline{r} = m$ e distância $\overline{d} = m + 1$.

6.3 Construção de algumas classes de códigos latinos

Teorema 6.11:[Su]

(a) Para todo n , q ($q \geq 2$) existe 2-código latino em V_q^n ;

(b) Se q é potência de 2 existe um q-código latino em V_q^{q-2}

Se q é primo ou potência de primo existem:

(c) $(n-1)$- código latino em V_q^n para todo $2 \leq n \leq q+1$;

(d) 3-código latino em V_q^n , para todo $4 \leq n \leq q+1$.

Prova : (a) Dados $r = 1$ e um m qualquer, podemos formar um código MDS em V_q^{m+1} de tamanho q^m e $d = 2$. Basta definir as palavras-código como sendo todas as $(m+1)$-uplas com coordenadas em Z_q cujas somas das entradas é nula módulo q

$$L = \left\{(a_1, a_2, \ldots, a_{m+1}) \in V_q^{m+1} : a_1 + a_2 + \ldots + a_{m+1} \equiv 0 \ (mod)\ q\right\}$$

(b) Seja α uma raíz primitiva de $GF_{(q)}$; definimos a matriz checagem do código desejado por $H = (A; I_{q-1})$onde $A = (\ \alpha^{ij}\ )$ para $j = 0, 1, 2$ e $0 \leq i \leq q-2$

As componentes de A diferem do zero em $GF_{(q)}$. Não é difícil ver que as determinantes das submatrizes 2×2 em A nunca se anulam. Por último, qualquer determinante de uma submatriz 3×3 em A não coincide com zero, pois sua expressão tem a forma:

$$(\alpha^i - \alpha^j)(\alpha^j - \alpha^k)(\alpha^k - \alpha^i) \neq 0$$

para $\{i, j, k\} = \{0, 1, 2\}$. Assim ,a condição (3) do corolário 6.10 é satisfeita.

(c) Considere α uma raíz primitiva de $GF_{(q)}$. Para $r = q-1$, tome a matriz checagem $H = (A; I_{q-1})$ onde $A = (\ \alpha^{ij}\ )$ para $j = 0, 1$ e $0 \leq i \leq q-2$.

O item (3) do corolário 6.10 se verifica . Para $n < q-1$, a eliminação de j linhas, digamos $l_1, l_2, \ldots, l_j$ e as respectivas colunas $c_1, c_2, \ldots, c_j$ de I produz uma matriz checagem de um código linear com $m = 2$ e $n = q-1-j$.

(d) Basta tomar os códigos duais dos construídos no item (c).□

7 Formulação do Problema das Hipertorres

7.1 Introdução

Conforme a Introdução deste trabalho, havíamos comentado que 8 é o número mínimo de torres necessárias para satisfazer a seguinte propriedade : qualquer posição do tabuleiro de xadrez pode ser atingida movendo-se uma única vez uma das torres .

Podemos generalizar esta situação pelo menos de duas formas, a saber: considerando tabuleiro com k^n posições no espaço n-dimensional e possibilitando que cada torre realize até R movimentos.

Em termos pictóricos, é este problema que nos propomos a estudar neste capítulo. Passamos a descrição formal do mesmo. Antes relembraremos algumas definições da seção anterior.

Denotamos por V_k^n o conjunto de todos as palavras $x = (x_1, x_2, \ldots, x_n)$ com n letras , onde x_i assume um dos valores $0, 1, \ldots, k-1$, tomados sobre o anel dos inteiros módulo k , $\mathbb{Z}_k$.

Definimos a distância de Hamming, $d(x, y)$, entre dois vetores x, y em V_k^n como sendo o número de letras nos quais os dois diferem. Com esta distância, (V_k^n, d) torna-se um espaço métrico.

Dado R , $0 \leq R \leq n$, o *domínio R-dimensional* de x em V_k^n, denotado por $B(x, R)$, é definido como o conjunto de todos as palavras y em V_k^n cuja distância de Hamming não excede R do dado ponto inicial x,ou seja, $B(x, R) = \{y \in V_k^n : d(x, y) \leq R\}$. Claramente $B(x, 0) = \{x\}$ e $B(x, n) = V_k^n$.

Se V_k^n pode ser dado como uma união de domínios R-dimensional de vetores em H , então o subconjunto H é chamado uma *R-cobertura* de V_k^n , ou uma cobertura $(n, k, n-R)$; ou melhor, H forma uma R-cobertura se e somente se

$$V_k^n = \bigcup_{x \in H} B(x, R).$$

Elementos de H recebem o nome de *hipertorres* e este conjunto, *domínio de hipertorres*. Desde que a união dos domínios de todas as palavras cobrem V_k^n , podemos definir a função $\gamma(n,k,n-R)$ como a mínima cardinalidade das coberturas $(n,k,n-R)$, isto é:

$$\gamma(n,k,n-R) = \min\{|H| : H \text{ é cobertura } (n,k,n-R)\}.$$

Quando $R = 1$, frequentemente utilizaremos $\sigma(n,k)$ para representar $\gamma(n,k,n-1)$.

O problema da cobertura por hipertorres consiste em se determinar os valores exatos da função γ .

A motivação da nomenclatuta foi inspirada no caso $n = 2, k = 8$ e $R = 1$, que pode ser interpretada como o problema descrito no parágrafo inicial . Para fixar conceitos, vejamos algumas situações simples.

Exemplo 7.1 Inicialmente vamos verificar que $\sigma(2,8) = 8$. Tome H em V_8^2 composto pelas 8 palavras do tipo $(0,i)$, $0 \leq i \leq 7$. Claramente H é 1-cobertura de V_8^2 ($\sigma(2,8) \leq 8$) . Dado 7 palavras, digamos (x_i, y_i) , considere a palavra (a,b) , onde a (b) difere de todas as letras x_i (y_i) . Assim, $d((a,b),(x_i,y_i)) = 2$ para $1 \leq i \leq 7$ e a igualdade segue .

Exemplo 7.2 Para $n = 3$, $k = 2$, $R = 1$; $H = \{(000),(111)\}$ é 1-cobertura de V_2^3 . ($\sigma(3,2) \leq 2$) . Por outro lado, como as letras assumem valores 0 ou 1 , qualquer vetor em V_2^3 cobre apenas 4 palavras ($2 \leq \sigma(3,2)$). Logo, $\sigma(3,2) = 2$.

Das condições acima, não é difícil ver que:

$$H = \{(0000),(0001),(1110),(1111)\}$$

é 1-cobertura de V_2^4 . Porém 3 palavras não são suficientes, pois cada uma delas cobre exatamente 5 vetores , ficando pelo menos uma palavra descoberta.

Embora a formulação deste problema necessite de uma linguaguem matemática simples, o leitor não deve se enganar quanto a complexidade envolvida na determinação de seus valores exatos.

7.2 Campeonato de futebol com n jogos

A função $\sigma(n,3)$ tem uma aplicação interessante. Num cartão da Loteria Esportiva, em cada jogo de futebol há três possibilidades: coluna "1" , "2" ou a do "meio ". Assim, o valor de $\sigma(13,3)$ pode ser interpretado como o número mínimo de apostas que garanta pelo menos 12 acertos num dos cartões , contemplando o apostador. Pesquisas já demonstraram que $\sigma(n,3) = 3^{10}$.

Num torneio com 5 jogos de futebol, há 3^5 possibilidades distintas de resultados destes jogos. Kamps e van Lint [KvL] provaram que $\sigma(5,3) = 27$: 27 previsões de um modo "inteligente" garantem o acerto de 4 resultados numa das apostas . A demonstração, elementar mas nada trivial, faz uso de 11 páginas no periódico "Journal of Combinatorial Theory".

Curiosamente os casos $\sigma(n,3)$, para $n = 6,7,8,\ldots$ continuam em abertos, resistindo a todos as tentativas de resolução. A computação dos exatos valores da função σ constitui um problema combinatório dificílimo; basta dizer que a cobertura das hipertorres já foi classificada como um problema NP-completo.

Aplicações do caso geral de γ são menos óbvias, exceto no caso $\gamma(n,3,s)$, o qual pode ser visto como a maneira mais eficiente de assegurar s previsões corretas num torneio de futebol com n jogos.

7.3 Evolução do problema

O problema precursor da cobertura das torres foi proposto por Taussky e Todd, em 1948, cuja formulação segue.

> Seja G um grupo abeliano com n geradores $g_1, g_2, \ldots, g_n$, todos de ordem k. Originalmente, o problema consistia em determinar $\sigma(n,k)$, definido como a mínima cardinalidade de um subconjunto H de G com a propriedade que todo elemento $g \in G$ pode ser escrito na forma $g = hg_i^{\alpha_i}$, onde $h \in H$ e $g_i^{\alpha_i}$ uma potência de um gerador.

Em 1960, eles reformularam o mesmo problema em termos puramente combinatórios. Este novo enfoque tornou-se predominante ao longo dos anos.

Os primeiros trabalhos publicados referentes à cobertura das torres trataram exclusivamente a função σ ($R = 1$). No início da década de 70, apenas poucas classes infinitas de valores exatos (ou mesmo desigualdades) eram conhecidos.

Teorema 7.1 (Resultados prévios): O artigo [Ca1] ,1985, apresenta um resumo dos principais resultados :

(a) $\sigma(2,k) = k$ e $\sigma(3,k) = \left\rfloor \frac{k^2-1}{2} \right\lfloor$ para todo k [St]

(b) $\sigma(n,k) = k^{n-r}$ para k potência de primo e $1 + n(k-1) = k^r$

(c) $\sigma(k+1, kp) = p^k k^{k-1}$ se k é primo

(d) $\sigma(n,k) \geq \frac{k^{n-1}}{(n-1)}$

(e) $\gamma(n,k,2) \geq \frac{k^2}{(n-1)}$

(f) $\sigma(n,2) = 4, 7, 12, 32$ para $n = 4, 5, 6$ e 8 respectivamente.[St]

(g) $\sigma(4,4) = 24$ e $\sigma(5,3) = 27$ [KvL] .

A partir da década de 80, passou-se a estudar a função γ em sua forma mais geral ($R \geq 1$) (ver [Ca1],[Ca2]).

Da forma como foi definida, as componentes do espaço "hipercúbicos" são fixas ($\mathbb{Z}_k \times \mathbb{Z}_k \times \ldots \times \mathbb{Z}_k$). Mais recentemente, a cobertura das hipertorres foi generalizado considerando-se componentes mistas na sua constituição dos espaços ($\mathbb{Z}_{k_1}^{n_1} \times \mathbb{Z}_{k_2}^{n_2} \times \ldots \times \mathbb{Z}_{k_l}^{n_l}$)(ver [Os]).

No entanto, abordaremos apenas tais cobertura em espaços "hipercúbicos".

8 Resultados Gerais

Inicialmente, abordaremos alguns resultados triviais da cobertura das hipertorres.

Em seguida, descreveremos *métodos construtivos* , os quais produzem "novas"coberturas através de certas combinações de códigos previamente conhecidos.

Utilizando resultados das seções anteriores (6 e 7), aplicações destes métodos fornecem boas estimativas superiores para γ , tornando possível inclusive a deteminação de valores exatos de certas classes infinitas de parâmetros.

Todos os resultados desta seção encontram-se em [Ca1] .

8.1 Resultados elementares

Até o fim desta seção, denotaremos $s = n - R$ em $\gamma(n, k, n - R)$. Não há nada a fazer quando $k = 1$. Os casos $R = 0$ e $R = n$ fornecem os valores trivias : $\gamma(n, k, n) = k^n$ e $\gamma(n, k, 0) = 1$, respectivamente. Para $R = n - 1$, não é dificil ver que $\gamma(n, k, 1) = k$ (proposição 8.13) .

Proposição 8.1 Para quaisquer n e k , valem :

(a) $\gamma(n, k, n) = k^n$

(b) $\gamma(n, k, 0) = 1$

(c) $\gamma(n, k, 1) = k$

(d) $\gamma(n, k, s) \leq k^s$.

Portanto, estaremos interessados na determinação de $\gamma(n, k, s)$ onde $n \geq 3$, $k \geq 2$ e $2 \leq s \leq n - 1$ $(1 \leq R \leq n - 2)$.

Considere H e H' códigos em V_k^n e V_k^m , respectivamente. Definimos a *soma direta* de 2 vetores $x = (x_1, x_2, \ldots, x_n) \in H$ e $y = (y_1, y_2, \ldots, y_m) \in H'$ como sendo $x \bullet y = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) \in V_k^{n+m}$. Analogamente, definimos a soma direta de 2 códigos por $H \bullet H' = \{x \bullet y \in V_k^{n+m} : x \in V_k^n, y \in V_k^m\}$.

Proposição 8.2 (regras de monotonicidade): Para $0 \leq s \leq n$, valem as desigualdades:

(a) $\gamma(n+1,k,s) \leq \gamma(n,k,s)$

(b) $\gamma(n,k,s) \leq \gamma(n,k,s+1)$

(c) $\gamma(n,k,s) \leq \gamma(n,k+1,s)$.

Prova: (a) De H uma cobertura minimal (n,k,s) , $H \bullet \{(0)\}$ produz uma cobertura $(n+1,k,s)$;

(b) direto , pois $B(x,n-s-1) \subset B(x,n-s)$;

(c) Para $x = (x_1, x_2, \ldots, x_n)$ em V_{k+1}^n , definimos

$$\overline{x_i} = \begin{cases} x_i & \text{se } x_i \in \{0,1,\ldots,k-1\} \\ k-1 & \text{se } x_i = k \end{cases} \qquad 1 \leq i \leq n$$

De uma cobertura $(n,k+1,s)$ H , podemos produzir a cobertura (n,k,s) : $\{\overline{x} \in V_k^n : x \in H\}$.□

Um domínio R-dimensional em V_k^n tem cardinalidade $v = \sum_{i=1}^{R} \binom{n}{i}(k-1)^i$. Assim obtemos o limite trivial :

Proposição 8.3 Dados n , k e R , se $v = \sum_{i=1}^{R} \binom{n}{i}(k-1)^i$ então

$$\gamma(n,k,n-R) \geq \left\lceil \frac{k^n}{v} \right\rceil$$

8.2 Métodos Construtivos

Proposição 8.4 Se $0 < m \leq n$, $0 < q \leq s$, $s - q < n - m$ e $q \leq m$ então :

(a) $\gamma(n,k,s) \leq \gamma(n-m,k,s-q).\gamma(m,k,q)$;

(b) $\gamma(n+r,k,s+r) \leq \gamma(n,k,s).k^r$ para todo $r \geq 1$.

Prova : (a) Tome H uma cobertura $(n-m,k,s-q)$ e H' uma cobertura (m,k,q) . Afirmamos que $H \bullet H'$ é uma cobertura (n,k,s) . De fato, dado x em V_k^n , podemos representá-lo na forma $x = x_1 \bullet x_2$, com $x_1 \in V_k^{n-m}$ e $x_2 \in V_k^m$. Por hipóteste, existem $y_1 \in H$ e $y_2 \in H'$ tais que

$d(x_1, y_1) \leq (n-m)-(s-q)$ e $d(x_2, y_2) \leq m-q$. Pela propriedade triangular, $d(x_1 \bullet y_1, x_2 \bullet y_2) \leq n - s$. A parte (b) é conseqüência direta de (a), pois $\gamma(r, k, r) = k^r$.□

Exemplo 8.5 De $\sigma(13, 3) = 3^{10}$ (teorema 7.1(g)), obtemos $\sigma(14, 3) \leq 3^{11}$. De $\sigma(5, 3) = 27$ (teorema 7.1(c)) ganhamos $\gamma(15, 3, 12) \leq \sigma(5, 3)^3 = 3^9$.

Teorema 8.6 : Para todo n , k , r , p e q satisfazendo $0 \leq p \leq r$ e $0 \leq q < n$, acontece:

$$\gamma(\ nr, k, (n-q)(r-p)\ ) \leq \gamma(\ n, \gamma(r, k, r-p), n-q\ )$$

Prova: Dado

$x = (x_1, x_2, \ldots, x_r, x_{r+1}, x_{r+2}, \ldots, x_{2r}, \ldots, x_{(n-1)r+1}, x_{(n-1)r-2}, \ldots, x_{nr}) \in V_k^{nr}$

podemos representá-lo como um vetor de tamanho n formado pelos símbolos $y_i = (x_{ir-1}, x_{ir-2}, \ldots, x_{(i-1)r})$ em V_k^n , $0 \leq i \leq n-1$. Considere H_1 uma cobertura minimal $(r, k, r-p)$ e $a = \gamma(r, k, r-p) = |H_1|$. Para todo y_i existe $z_i \in H_1$ com $y_i \in B(z_i, p)$, ou seja, y_i e z_i diferem em p coordenadas no máximo. Seja H_2 um q-cobertura minimal de V_a^n ($|H_2| = \gamma(n, k, n-q)$) , onde os símbolos estão em H_1 , isto é , H_2 forma uma q-cobertura de $(H_1)^n$. Dado $z = (z_1, z_2, \ldots, z_n)$, existe um $w = (w_1, w_2, \ldots, w_n)$ em H_2 tal que z e w diferem em q coordenadas no máximo. Logo, o primeiro vetor $(y_1, y_2, \ldots, y_n)$ e w coincidem em pelo menos $nr - ((n-q)p + qr) = (n-q)(r-p)$ posições e a desigualdade segue.□

Exemplo 8.7 : Vamos ilustrar o caso $n = 4$, $r = 3$, $k = 2$ e $q = p = 1$. Sabemos que $\gamma(3, 2, 2) = \sigma(3, 2) = 2$, basta tomar a cobertura minimal $H_1 = \{(0, 0, 0), (1, 1, 1)\}$ (exemplo 7.2) . Seguindo os passos do teorema acima, considere

$$V_2^4 = (H_1)^4 = \left\{(\overline{0}, \overline{0}, \overline{0}, \overline{0}), (\overline{0}, \overline{0}, \overline{0}, \overline{1}), \ldots (\overline{1}, \overline{1}, \overline{1}, \overline{0}), (\overline{1}, \overline{1}, \overline{1}, \overline{1})\right\}$$

onde $\overline{0} = (0, 0, 0)$ e $\overline{1} = (1, 1, 1)$.

O código $H_2 = \left\{(\overline{0}, \overline{0}, \overline{0}, \overline{0}), (\overline{0}, \overline{1}, \overline{1}, \overline{1})(\overline{1}, \overline{0}, \overline{0}, \overline{0}), (\overline{1}, \overline{1}, \overline{1}, \overline{1})\right\}$ forma 1-cobertura minimal de $(H_1)^4$ (ver 7.2).

Por exemplo, seja o vetor $x = (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$. Tomando-se $z_0 = z_2 = z_3 = \overline{0}$ e $z_1 = \overline{1}$, vem $d(y_i, z_i) = 0, 0, 1.1$ respectivamente para $i = 0, 1, 2, 3$. Como $z = (\overline{0}, \overline{1}, \overline{0}, \overline{0}) \in (H_1)^4$, tome $w = (\overline{0}, \overline{0}, \overline{0}, \overline{0}) \in H_2$ $(d(z, w) = 1)$. Destes comentários, concluimos : $d(y_i, w_i) \leq 0, 3, 1, 1,$

respectivamente para $i = 0, 1, 2, 3$. Logo, $d(y, w) \leq 5$ (veja ilustração abaixo)

$$\begin{array}{cccc} y_0 = 000 & y_1 = 111 & y_2 = 010 & y_3 = 001 \\ z_0 = 000 & z_1 = 111 & z_2 = 000 & z_3 = 000 \\ w_0 = 000 & w_1 = 000 & w_2 = 000 & w_3 = 000 \end{array}$$

Por simples inspeção, $d(y_i, w_i) = 0, 3, 1, 1$ para $i = 0, 1, 2, 3$, respectivamente.

Para o vetor $x = (101, 010, 001, 110)$, considerando os mesmos H_1 e H_2 acima , tome $z_0 = z_3 = (111)$ e $z_1 = z_2 = (000)$. Defina $w = (\overline{0}, \overline{0}, \overline{0}, \overline{1}) \in H_2$. Neste exemplo, $d(x, w) = 3 + 1 + 1 + 1 = 6 = p(n - q) + qr$.

Quando $p = 0$ e $q = 1$ no teorema acima, obtemos $\gamma(nr, k, (n-1)r) \leq \gamma(n, \gamma(r, k, r), n - 1) = \gamma(n, k^r, n - 1) = \sigma(n, k^r)$. O caso $q = 0$ e $p \leq r$ diz que $\gamma(nr, k, n(r - p)) \leq \gamma(r, k, r - p)^n$ (caso particular da proposição 8.4).

Exemplo 8.8 Tome $r = 3$, $k = 3$ e $p = 1$, $\gamma(3, 3, 2) = 5$

(a) para $n = 3$ e $q = 2$, o teorema acima fornece $\gamma(9, 3, 2) \leq \gamma(3, 5, 1) = 5$ (resultado 8.1) , melhorando o limite trivial .

(b) para $n = 3$ e $q = 1$, $\gamma(9, 3, 4) \leq \gamma(3, 5, 2) = \left\rfloor \frac{5^2+1}{2} \right\lceil = 13$ (ver teorema 7.1)

O próximo teorema possibilita a construção de limites superiores partindo de códigos latinos conhecidos (ver seção 6) .

Teorema 8.9 : Se existe um $(R + 1)$-códico latino em V_k^n então a desigualdade abaixo vale para todo $r \geq 1$

$$\gamma(n, kr, n - R) \leq k^{n-R}\gamma(n, r, n - R)$$

Prova : Recordemos o resultado 6.4 : num $(R + 1)$-código latino G em V_k^n , uma escolha de $n - R$ coordenadas fornece todos os vetores de V_k^{n-R} como projeções das palavras-códigos nestas coordenadas consideradas.

Seja $x = (a_1, a_2, \ldots, a_n)$ em V_{kr}^n ; podemos representar a_i , $1 \leq i \leq n$, na forma $a_i = rb_i + c_i$, onde $0 \leq b_i \leq k - 1$ e $0 \leq c_i \leq r - 1$. Da nomenclatura $x_1 = (b_1, b_2, \ldots, b_n)$ e $x_2 = (c_1, c_2, \ldots, c_n)$, vem $x = r \cdot x_1 + x_2$ (onde $\cdot$ e $+$ denotam as operações produto escalar e adição vetorial , respectivamente) .

Se H é uma cobertura minimal $(n, r, n-R)$ e G um $(R+1)$-código latino em V_k^n ,afirmamos que o conjunto $r.G + H = \{r.z_1 + z_2 : z_1 \in G, z_2 \in H\}$ é cobertura $(n, kr, n-R)$. De fato, qualquer x em V_{kr}^n pode ser decomposto em $x = r \cdot x_1 + x_2$, $x_1 \in V_k^n$ e $x_2 \in V_r^n$. Por hipótese, existe $y_2 \in H$ que coincide com x_2 em $(n-R)$ coordenadas pelo menos, e que existe uma palavra-código y_1 coincidindo com x_1 nestas mesmas posições, como observamos no início da prova. Logo, o vetor x pertence ao domínio R-dimensional de uma palavra em $r.G + H$.□

Exemplo 8.10 Seja G o 3-código latino descrito no exemplo 6.2 . O código $H = \{(0000)\}, (1111)\}$ constitui uma cobertura minimal $(4, 2, 2)$. Dessa forma, $2.G + H$ possui os elementos:

0000	2204	4204	1111	3305	5305
0222	2420	4042	1333	3530	5053
0444	2042	4420	1555	3053	5530

As três primeiras tabelas são geradas por $(0000) \in H$ e as restantes, por $(1111) \in H$. Pelo teorema 8.8 , $2.G + H$ descreve uma 2-coberura de V_6^4 .

8.3 Classes Particulares

O teorema 6.11 em conjunto com o teorema acima permite-nos obter diretamente o seguinte:

Corolário 8.11 As desigualdades valem :

(a) $\sigma(n, kr) \leq \sigma(n, r).k^{n-1}$ para todo n , k , r

(b) $\gamma(2^n + 2, 2^n r, 3) \leq 2^{2n}\gamma(2^n + 2, r, 3)$ para todo n , k , r

Se k é primo ou potência de primo, então :

(c) $\gamma(n, rk, 2) \leq k^2\gamma(n, r, 2)$ para todo $2 \leq n \leq k + 1$

(d) $\gamma(n, rk, n-2) \leq k^{n-2}\gamma(n, r, 2)$ para todo $4 \leq n \leq k + 1$.

Corolário 8.12 Se k é primo ou potência de primo então$\sigma(k+1, rk) = r^k k^{k-1}$ para todo $r \geq 1$ e $k \geq 1$.

Prova: Conforme o resultado 7.1 (ítens c e d) , temos $\sigma(k+1, k) = k^{k-1}$ e $\sigma(k+1, kr) \geq r^k k^{k-1}$. Mas $\sigma(k+1, kr) \leq r^k k^{k-1}$ por 8.11(a) .

O Princípio da Casa do Pombo valida o resultado abaixo, o qual generaliza a proposição 8.1(c). Dessa forma, mais uma classe infinita de valores da função γ passa a ser conhecida.

Proposição 8.13 : Se $0 < s \leq n$ e $s \leq \left\rfloor \frac{n}{k} \right[$ então $\gamma(n, k, s) = k$.

Prova : Tome y em V_k^n , para cada $0 \leq i \leq k-1$ definimos a função $f_i(y)$ como sendo o número de letras i em y . Dado x em V_k^n , afirmamos que existe um j , $0 \leq j \leq k-1$, tal que $f_j(x) \geq s$. Se a asserção não vale, temos

$$\sum_{i=0}^{k-1} f_i(x) \leq k(s-1) \leq k\left(\left\rfloor \frac{n}{k} \right[- 1\right) < n$$

e isto é impossível , pois a soma do membro à esquerda sempre coincide com n . Portanto, as k palavra-código $(00\ldots0), (11\ldots1), \ldots (k-1\ k-1\ldots k-1)$ formam uma cobertura (n, k, s) . Por outro lado, uma cobertura (n, k, s) tem pelo menos k vetores. De fato, consideremos um conjunto com m palavras $(a_1^i, a_2^i, \ldots, a_n^i)$,$1 \leq i \leq m < k$. Os vetores formados pelas letras b_i não pertencentes à coluna i deixam de ser cobertos pelos m vetores mencionados. Logo, $\gamma(n, k, s) = k$.

Corolário 8.14 Se k é primo ou potência de primo e $2 \leq n \leq k+1$ então $\gamma(n, k(n-1), 2) = k^2(n-1)$

Prova : Conforme o corolário 8.11(c) e 7.1(e) , $\gamma(n, k(n-1), 2) = k^2\gamma(n, n-1, 2)$. Mas $\gamma(n, n-1, 2) = n-1$ pela proposição acima .

Exemplo 8.15 De 8.12, obtemos $\gamma(7, 3, 2) = 3$ e $\gamma(8, 3, 3) = 3$. De acordo com resultado acima, tais limites produzem:

(a) $\gamma(9, 3, 4) \leq \gamma(7, 3, 2).\ \gamma(2, 3, 2) = 3.3^2 = 27$

(b) $\gamma(9, 3, 4) \leq \gamma(8, 3, 3).\ \gamma(1, 3, 1) = 3.3$, melhorando o limite encontrado em 8.8 .

Tabelas

As tabelas apresentadas encontram-se nos trabalhos : [Ca1] ($k = 2$) e [Os] ($k = 3, 4, 5$) .

$\gamma(n,\ 2,\ n-R)$					
n	$R=1$	$R=2$	$R=3$	$R=4$	$R=5$
2	2				
3	2	2			
4	4	2	2		
5	7	2	2	2	
6	12	4	2	2	2
7	16	??	2	2	2

$\gamma(n,\ 3,\ n-R)$					
n	$R=1$	$R=2$	$R=3$	$R=4$	$R=5$
2	3				
3	5	3			
4	9	3	3		
5	27	6-8	3	3	
6	63-73	12-17	6	3	3
7	147-186	26-34	7-12	3	3

$\gamma(n,\ 4,\ n-R)$					
n	$R=1$	$R=2$	$R=3$	$R=4$	$R=5$
2	4				
3	8	4			
4	24	7	4		
5	64	12-16	4	4	
6	228-256	28-64	8-16	4	4
7	748-1024	80-192	16-32	7-12	4

$\gamma(n,\ 5,\ n-R)$					
n	$R=1$	$R=2$	$R=3$	$R=4$	$R=5$
2	5				
3	13	5			
4	45-51	9-11	5		
5	157-184	20-35	8-10	5	
6	625	65-125	11-25	5	5

9 O Método de Cobertura por Matrizes

Em [KvL], Kamps e van Lint provaram que $\sigma(5,3) = 27$ e $\sigma(9,3) \leq 2.3^6$. Baseados neste artigo, Lam e Blokhuis (ver [BL]) sistematizaram um método de determinação de cotas superiores de σ ,conhecido como *método de cobertura por matrizes*. Por sua vez, Carnielli [Ca2] estendeu este método para o caso multidimensional ($R \geq 1$) , obtendo algumas classes de delimitações e relações de parâmetros da função γ .

Nesta seção abordaremos tal método. Baseado nos artigos [BL],[Ca2],[Za], conseguimos obter resultados novos e algumas generalizações de teoremas em [BL] e [Ca2] .

9.1 Descrição do Método

Inicialmente, vamos estabelecer algumas notações: I_r denota a matriz identidade de ordem r . Sejam B e C matrizes $r \times n$ e $r \times m$, respectivamente. Definimos a *justaposição* de C em B , denotada por $(B;C)$, como sendo a matriz $r \times (n+m)$ cujas primeiras n colunas provêm de B e as m restantes, de C. Em particular, para $x \in V_k^n$ e $y \in V_k^m$, o vetor $(x;y)$ representa a justaposição de y em x .

Definição 9.1: Seja M uma matriz $r \times (n-r)$ com entradas em $\mathbb{Z}_k$, $k \geq 2$, $r \leq n$. Tome $0 \leq R \leq n$ e $A = (I;M)$. Uma coleção S em V_k^r é chamada de *R-cobertura de V_k^r usando A* se cada vetor de V_k^r pode ser coberto por S com "ajuda " de R colunas de A , ou melhor:

$$V_k^r = \left\{ s + \sum_{j=1}^{R} \alpha_j a_j : \qquad s \in S,\ \alpha_j \in \mathbb{Z}_k,\ a_j \text{ coluna de } A \right\}$$

A R-cobertura de V_k^r definida na seção 7 corresponde ao caso $r = n$; ou seja, corresponde à R-cobertura de V_k^r usando apenas os vetores canônicos de I_r . Para ver isto, considere S uma R-cobertura de V_k^r . Dado $x \in V_k^r$, existe um s em S tal que $d(x,s) \leq R$, digamos que x e s diferem nas coordenadas $i_1, i_2, \ldots, i_l$, com $0 \leq l \leq R$. Logo

$$x - s = \alpha_{i_1} e_{i_1} + \alpha_{i_2} e_{i_2} + \ldots + \alpha_{i_l} e_{i_l}$$

onde e_i representa i-ésimo vetor canônico de V_k^r (e_i em I_r) e $\alpha_i \in \mathbb{Z}_k$. Logo, S é R-cobertura usando I_r .

Exemplo 9.2 O conjunto $S = \{s_i = (i, i, i, i, i), 0 \leq i \leq 4\}$ é 3-cobertura de V_5^5 usando a matriz :

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{bmatrix}$$

De fato, denote $v = (0, 1, 2, 3, 4)$ e considere y um vetor arbitrário de V_5^5 . Não há nada a fazer se y apresenta pelo menos 2 coordenadas com o mesmo valor, pois $d(y, s_i) \leq 3$ para algum i . Caso contrário, resta a situação onde todos os valores das coordenadas são distintos; assim , basta verificar que existem $\alpha \in \{1, 2, 3, 4\}$ e $s_i \in S$ tais que $d(y - \alpha.v, s_i) \leq 2$. Pelo configuração de S , podemos supor que $y = (0, a, b, c, d)$.

Fixe inicialmente $a = 1$. Se $a \neq 1$ então $b \neq 2$, $c \neq 3$ e $d \neq 4$. Logo, por simples inspeção, restam os casos $y = (0, 1, 4, 2, 3)$ e $y = (0, 1, 3, 4, 2)$, os quais respectivamente fornecem $d(y - 2.v, s_0) \leq 2$ e $d(y - 3.v, s_0) \leq 2$. Para $a \neq 1$ a verificação é análoga.

Em seguida, apresentamos o teorema principal desta seção.

Teorema 9.3 [Ca2] Seja $1 \leq R \leq n$, $1 \leq r \leq n$ e S é uma R-cobertura de V_k^r usando $A = (M; I_r)$. Nestas condições,

$$\gamma(n, k, n - R) \leq |S| . k^{n-r}$$

Prova : Considere z em V_k^n escrito na forma $(x; y)$, com $x \in V_k^r$ e $y \in V_k^{n-r}$. Como S é R-cobertura de V_k^r usando A e $A(x; y) = (I : M)(x; y) = x + My \in V_k^r$, existem $s \in S$ e $i_1, i_2, \ldots, i_R$ tais que :

$$x + My = s + \sum_{j=1}^{R} \alpha_{i_j} a_{i_j}$$

Reordene ,se necessário, os índeces de tal modo que: a_{i_j} são vetores canônicos de V_k^r para $1 \leq j \leq q$ e a_{i_j} são colunas de M para $q < j \leq R$. Denotando: $x^* = x - \sum_{j=1}^{q} \alpha_{i_j} e_{i_j}$ e $y^* = y - \sum_{j \geq q+1}^{R} \alpha_{i_j} e_{i_j}$, temos $x^* = x - My^*$ pois

$$s - My^* = x - \sum_{j=1}^{R} \alpha_{i_j} a_{i_j} + \sum_{j \geq q+1}^{R} \alpha_{i_j} a_{i_j} = x - \sum_{j=1}^{q} \alpha_{i_j} e_{i_j} = x^*$$

Assim $d(y, y^*) \leq R - q$, $d(x, s - My^*) \leq q$ e

$$d\left((x;y),(s - My^*;y^*)\right) \leq R)$$

Desde que y^* é um vetor arbitrário de V_k^{n-r} , a coleção de todos os $|S|.k^{n-r}$ vetores do tipo $(s - My^*; y^*)$ forma R-cobertura de V_k^n .□

Quando $R = 1$, o teorema fornece:

$$\text{se } S \text{ forma 1-cobertura de } V_k^r \text{ então } \sigma(n,k) \leq |S|.k^{n-r}$$

(principal resultado de [BL]) . Neste sentido, o teorema 9.3 pode ser visto como a generalização multidimencional do método descrito neste artigo, como havíamos comentado no início da seção .

9.2 Aplicações do Método

via códigos latinos

Em alguns casos, códigos latinos permitem a construção sistemática de certas classes de coberturas usando matrizes apropriadas, como mostram os resultados desta subseção:

Lema 9.4 [Ca2] Seja $k \geq 2$, $r \geq 1$, $n \geq d$. Se existe um $(d+1)$-código latino L em V_k^n então existe código satisfazendo: S é uma $(d+1)$-cobertura de $V_{k^r}^n$ usando uma matriz A de dimensões $n \times (n + k^{n-d} - 1)$, com $|S| = \gamma(n, r, n-d)$.

Prova Para cada $x \in V_{k^r}^n$, podemos escrevê-lo na forma $x = x_1 + r.x_2$, com $x_1 \in V_r^n$ e $x_2 \in V_k^n$. Seja S uma d-cobertura minimal de V_r^n e $A = (M; I)$ a matriz $n \times (n + k^{n-d} - 1)$ onde M é constituída pelas palavras-códigos não nulas de L .

Para cada $x = x_1 + r.x_2$, existe y_1 em S que coincide com x_1 em pelo menos $n - d$ coordenadas. É possível escolher $y_2 \in L$ que coincide com x_2 nestas mesmas $n - d$ posições. (ver proposição 6.4). Logo , x e $y_1 + r.y_2$ diferem em d coordenadas no máximo. Note que se $y_2 \neq (0, 0, \ldots, 0) \in L$ então y_2 é uma coluna de A . Caso contrário ($y_2 = (0, 0, \ldots, 0)$) então y_2 e x_2 se igualam em $n - d$ coordenadas, obtendo $d(x, y) \leq d$. Em qualquer caso: $x = y_1 + r.y_2 + \sum_{i=1}^{d} \alpha_i e_i$. Portanto, S é uma $(d + 1)$-cobertura de V_{kr}^n usando A .□

Exemplo 9.5 Vamos ilustar o caso $n = 4$, $k = 3$, $d = 2$. Já vimos que $S = \{(0000), (1000), (0111), (1111)\}$ forma 2-cobertura minimal de V_3^4 . Pelo teorema acima, S também é uma 3-cobertura de V_6^4 usando a matriz

$$A = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Note que a união das primeiras oito colunas com o vetor nulo forma 3-código latino de V_6^4 descrito em 6.3 .

Teorema 9.6 [Ca2] Se $k \geq 2$, $r \geq 1$, $n \geq d$, $q = k^{n-d} - 1$ e existe um $(d + 1)$-código latino em V_k^n , então

$$\gamma(n+q, kr, n+q-(d+1)) \leq \gamma(n, r, n-d).(kr)^q \qquad (1)$$

Prova : Consequência direta de 9.3 e 9.4.□

A obtenção de desigualdades do tipo (1) fica dependendo da existência de códigos latinos . Contudo, 6.11 fornece algumas classes de tais códigos e por 9.6 :

Corolário 9.7:[Ca2]

(a) para todo $r, n \geq 2, k \geq 2$ e $a = k^{n-d} - 1$

$$\gamma(n + a, kr, n + a - 2) \leq \sigma(n, r).(kr)^a$$

(b) para todo r, n, k primo ou potência de primo com $2 \leq n \leq k + 1$ e $b = k^2 - 1$

$$\gamma(n + b, kr, n + b) \leq \gamma(n, r, 2).(kr)^b$$

(c) para todo n, r , k primo ou potência de primo com $4 \leq n \leq k+1$ e $c = k^{n-2} - 1$

$$\gamma(n+c, kr, n+c-3) \leq \gamma(n, r, n-2).(kr)^c$$

Exemplos 9.8
(a) Para $n = 4$, $k = 3$ e $r = 3$, de 9.7(a) temos $\gamma(30, 9, 28) \leq 3^{54}$
(b) Para $n = 4$, $k = 3$ e $r = 2$, obtemos $\gamma(12, 6, 9) \leq 2.6^8$ de 9.7(b)
(c) Para $n = 4$, $k = 5$ e $r = 3$, $\gamma(28, 15, 25) \leq 3.15^{24}$ por 9.7(c)

via relações indutivas

Teorema 9.9: Seja $n = t^s \gamma(r-s, k, (r-s)-(R-1)) + (r-s)$ para $k \geq 2$, $2 \leq t \leq k$, $s \leq r$ e $r - s \geq R - 1$. Nestas condições vale

$$\gamma(n, k, n-R) \leq (k-t+1)^s . k^{n-r}$$

Prova: Tome $S = \{0\} \times V_{k-t+1}^s \subset V_k^r$ e a matiz:

$$A = \left[\begin{array}{c|c} * & \\ \gamma(r-s, k, (r-s)-(R-1)) & I_{(r-s)} \\ * & \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \cdots\ \cdots \\ u & 0 \end{array}\right]$$

onde a submatriz $\left[\begin{array}{ccc|c} * & \gamma(r-s, k, (r-s)-(R-1)) & * & u \end{array}\right]^T$ representa todas as colunas do tipo $(v; u)$ com : v pertence a uma $(R-1)$-cobertura minimal de V_k^{r-s} a qual contém o vetor nulo e u pertence a V_k^s . A matriz A tem dimensões $r \times n$ e contém os vetores de I_r . Falta provar que S é uma cobertura de V_k^n usando A .

Dado um vetor em V_k^r , ele pode ser representado por $(x; y)$ com $x \in V_k^{r-s}$ e $y \in V_k^s$. Tome $z \in V_{k-t+1}^s$ e $j \in V_t^s$ tais que $z + j = y$. Assim , $(x; y) = (0; z) + (x; j)$. Por construção de A, existe uma coluna da forma $(v; j)$ com $d(x, v) \leq R-1$, digamos

$$(x; j) = (v; j) + \sum_{i=1}^{R-1} \alpha_i . e_{l_i}$$

onde $0 \leq \alpha_i \leq k-1$ e e_{l_i} denota o $_{l_i}$-ésimo vetor canônico de V_k^r . Logo

$$(x;y) = (0;z) + 1.(v;j) + \sum_{i=1}^{R-1} \alpha_i.e_{l_i}$$

Como $(0;z) \in S$, $I_r \subset A$ e $(v;j) \in A$, temos que S é cobertura de V_k^r usando A . Pelo teorema 9.3, a relação indutiva segue.□

Observações:

(1) Em particular, para $s = 1$ e $R = 2$ obtemos

$$\gamma(n,k,n-2) \leq (k-t+1).k^{n-r} \text{ se } n = t\sigma(r-1,k) + (r-1)$$

que corresponde ao teorema 3.7 de [Ca2]. Neste sentido, 9.9 generaliza tal resultado.

(2) Nas hipóteses de 9.9, para $m \geq n$ vale:

$$\gamma(m,k,m-R) \leq \gamma(n,k,n-R).k^{m-n} \leq (k-t+1)^s.k^{m-r}$$

Neste contexto, para $s = 1$, $R = 2$, $n = t\sigma(r-1,k)+(r-1)$ a relação acima valida

$$\gamma(m,k,m-2) \leq (k-t+1).k^{m-r} \text{ se } m = 1+t[1+k+\sigma(3,k)+\ldots+\sigma(r-1,k)]$$

Mas esta desigualdade é a tese do teorema 3.6 de [Ca2] , o qual pode ser obtido via teorema 3.7 de [Ca2], como foi verificado acima.

(3) Quando $t = k$ no enunciado de 9.9, temos

$$\gamma(n,k,n-R) \leq k^{t^s.\gamma(r-s,k,r-s-(R-1))-s} = \frac{1}{k^{r-R}} \text{ do limite trivial } k^{n-R}$$

Exemplos 9.10

(a) Para $n = 2.\sigma(3,4)+3 = 19$, temos $\gamma(19,4,17) \leq 3.4^{15}$.

(b) Para $n = 3.\gamma(4,3,3)+4$vale $\gamma(31,3,29) \leq 3^{26}$.

O teorema acima estabelece uma classe de limites para $\gamma(n,k,n-R)$ quando n é uma "combinação linear" de valores de γ cujos parâmetros apresentam o raio constante, a saber $R-1$. Contudo, podemos obter certas delimitações para γ com n dependendo de valores de γ cujos raios dos parâmetros não excedam R .

Teorema 9.11: Seja $r = \sum_{i=1}^{s} a_i$ e $n = r - 1 + \prod_{i=1}^{s} \gamma(a_i, k, a_i - R_i)$ para $k \geq 2$, $a_i \geq R_i$, $s \geq 2$ e $n \geq 1 + \sum_{i=1}^{s} R_i$. Então :

$$\gamma\left(n, k, n - \left(1 + \sum_{i=1}^{s} R_i\right)\right) \leq k^{n-r}$$

Prova: Defina $S = \{0\} \times V_k^r$ e $A = (B; C)$ com

$$B = \begin{bmatrix} \gamma(a_1, k, a_1 - R_1) \\ \gamma(a_2, k, a_2 - R_2) \\ \\ \vdots \\ \\ \gamma(a_s, k, a_s - Rs) \end{bmatrix} \qquad C = \begin{bmatrix} I_{r-1} \\ - - - \\ 0 \end{bmatrix}$$

onde a submatriz B é constituída pelas colunas do tipo $(v_1; v_2; \ldots; v_s)$ com: (a) v_i pertence a uma R_i-cobertura minimal de $V_k^{a_i}$ a qual contém o vetor nulo $0 \in V_k^{a_i}$, para $1 \leq i \leq s - 1$; (b) v_s pertence a uma R_s-cobertura minimal de $V_k^{a_s}$ a qual contém o vetor $(0, 0, \ldots, 1) \in V_k^{a_s}$.

Assim, I_r está na matriz A de dimensões $r \times n$. Falta verificar que S é uma $(1 + \sum_{i=1}^{s} R_i)$-cobertura de V_k^r usando A . Considere $(x_1; x_2; \ldots; x_s) \in V_k^r$, onde $x_i \in V_k^{a_i}$. Por construção de A , existe uma coluna da forma $(y_1; y_2; \ldots; y_s)$ tal que $d(x_i, y_i) \leq R_i$ para todo $1 \leq i \leq s$.

A aplição do teorema principal completa a prova, pois $(x_1; x_2; \ldots; x_s)$ e $(y_1; y_2; \ldots; y_s)$ diferem em $(\sum_{i=1}^{s} R_i)$ coordenadas no máximo.□

Observação : O limite por nós encontrado equivale a

$$\frac{1}{k^{\sum_{i=1}^{s}(a_i - R_i) - 1}} \text{ do limite trivial } k^{n - \left(1 + \sum_{i=1}^{s} R_i\right)}$$

Exemplos 9.12:

(a) Se $n = (5 + 4 - 1) + \gamma(5, 3, 2).\gamma(4, 3, 2) = 17$ então $\gamma(17, 3, 11) \leq 3^6$.

(b) Para $n = (4 + 2 - 1) + \sigma(4, 2) + \sigma(2, 2) = 13$, temos $\gamma(13, 2, 10) \leq 2^7$.

(c) Se $n = (3.3 - 1) + \sigma(3, 2)^3 = 16$ então $\gamma(16, 2, 12) \leq 2^7$. Mas este resultado melhora $\gamma(16, 2, 12) \leq 2^6$ desde que $\gamma(9, 2, 5) = 2$.

Teorema 9.13: Seja p primo ou potência de primo, $n = R + \prod_{i=R}^{r-1} \gamma(i, p, i-R)$ para $r \geq R+1$. Então:

$$\gamma(n, p, n-R) \leq [1 + (p-1).(r-R)].p^{n-r}$$

Prova: Tome

$H = \left\{(0, \alpha e_j) \in V_p^{r-R+1} : \alpha \in GF_{(p)}\ , e_j \in I_{r-R}\right\}$ e $S = H \times \{0\} \subset V_p^r$

Claramente $|S| = 1 + (p-1).(r-R)$. Considere

$$A = \begin{bmatrix} 0 & 0 & \dots & 1 & 0_R \\ 0 & 0 & \dots & \gamma(r-1, p, r-1-R) & 0_R \\ 0 & \vdots & & * & \\ \vdots & 0 & \dots & & \vdots \\ 0 & 1 & \dots & & \\ 1 & \gamma(R-1, p, 1) & \dots & & 0_R \\ \gamma(R, p, 0) & * & \dots & \vdots & -- \\ & \vdots & & & \\ \vdots & \vdots & & & I_R \\ & * & \dots & * & \end{bmatrix}$$

onde $[0 \dots 01\ \gamma(i, p, i-R) * \dots *]^T$ representa a submatriz $\gamma(i, p, i-R) \times r$ composta pelas colunas $(0, 0, \dots 0, 1, v)^T$, sendo v uma palavra-código de uma R-cobertura minimal de V_k^i contendo o vetor nulo (para $R \leq i \leq r-1$). A submatriz $[O_R \dots O_R; I_R]^T$ denota os vetores $(0; e_j) \in V_p^r$ com $e_j \in I_R$

Desde que $\gamma(R, p, 0) = 1$ e $\gamma(R+1, p, 1) = p$, I_r está em $A_{r \times n}$. Do teorema 9.3, basta verificar que S é uma cobertura de V_p^r usando A .

Seja $w = (0, 0, \dots, 0, a_1, a_2, \dots, a_i)$ um vetor arbitrário de V_p^r , onde as primeiras $r-1$ coordenadas são nulas, $0 \leq i \leq r$. Se $i = 0$ então $w = 0 \in S$; em geral , se $i \leq R$

$$w = 0 + a_1.e_{r-i+1} + a_2.e_{r-i+2} + \dots + a_i.e_r$$

Como $0 \in S$ e e_j está em A , $w \in B(0, R)$.

Se $i \geq R+1$ existe $\beta \in GF_{(p)}$ tal que $a_1.\beta = 1$, pois $a_1 \neq 0$. Assim, $\beta w = (0, 0, \dots, 0, 1, \beta a_2, \dots, \beta a_i)$ e, por construção de A , existe uma coluna v em $[0, \dots, 0, 1, \gamma(i-1, p, i-1-R) * \dots *]^T$ tal que $d(\beta w, v) = s \leq R$, ou melhor,

$$\beta w = v + \alpha_1.e_{l_1} + \alpha_2.e_{l_2} + \ldots + \alpha_s.e_{l_s} \quad , \alpha_i \in GF_{(p)} \ , \ e_{l_i} \in I_r, 1 \leq i \leq s$$

Vamos considerar dois casos possíveis. Se $s < R$, obrigatoriamente w é uma combinação linear de $s+1 \leq R$ colunas de A . Para $s = R$, podemos supor sem perda de generalidade que e_{l_1} tem as últimas $R-1$ coordenadas iguais a zero, pois há R vetores unitários distintos. Logo

$$w = \beta^{-1}\alpha_1.e_{l_1} + \beta^{-1}v + \beta^{-1}\alpha_2.e_{l_2} + \ldots + \beta^{-1}\alpha_R.e_{l_R}$$

O vetor $\beta^{-1}\alpha_1.e_{l_1}$ pertence a S pois $2 \leq l_1 \leq r-R+1$. Portanto, S é uma R-cobertura de V_p^r usando A .□

Observação : Em particular, o caso $R = 1$ coincide com o teorema 3.9 de [Ca2].

Exemplos 9.14:

(a) Para $p = 3$, $R = 1$ e $r = 6$ vale $\sigma(46,3) \leq 11.3^{40}$ pois $n = 1 + (1+3+5+9+27)$ (ver tabela seção 8)

(b) Se $p = 2$, $R = 2$ e $r = 7$,temos $n = 2 + (1+2+2+2+4)$ (ver tabela seção 8) e $\gamma(13,2,11) \leq 6.2^6$. Este resultado melhora $\gamma(13,2,11) \leq 2^9$ obtido através de $\gamma(5,2,3) = 2$.

(c) Se $p = 2$, $R = 3$ e $r = 9$, $n = 3+(1+2+2+2+2+4) = 16$ e $\gamma(16,2,13) \leq 7.2^7$ que equivale a $\frac{7}{8}$ do limite $\gamma(16,2,13) \leq \sigma(4,2)^3.2^4 = 2^{10}$.

outras aplicações

Teorema 9.15: Para $1 \leq R \leq n$ e p primo ou potência de primo, vale

$$\gamma\left(p(n-R+1)+R, p, p(n-R+1)\right) \leq \gamma\left(n, p, n-R\right) p^{(p-1).(n-R+1)}$$

Prova: Considere S o subconjunto de V_p^{n+1} composto pelos vetores $(z;0)$, onde z é uma palavra-código de uma R-cobertura mínimal de V_p^n contendo o vetor nulo. Seja a matriz

$$A = \begin{bmatrix} 1.I_{n-R+1} & 1.I_{n-R+1} & 2.I_{n-R+1} & (p-1).I_{n-R+1} & 0 \\ & & & & 0 \\ 0_{R-1} & 0_{R-1} & 0_{R-1} & 0_{R-1} & \\ & & & & I_R \\ 00\ldots0 & 11\ldots1 & 11\ldots1 & 11\ldots1 & \end{bmatrix}$$

A notação 0_{R-1} indica a matriz ~~quadrada~~ nula de ordem $R-1$. Claramente $|S| = \gamma(n, p, n-R)$ e I_{n+1} está na matriz $A_{(n+1)\times p(n-R-1)+R}$.

Considere $w = (x;t) \in V_p^{n+1}$, com $x \in V_p^n$ e $t \in GF_{(q)}$. Existe um z em S satisfazendo $d((x;o),(z;0)) = s \leq R$, digamos

$(x;0) = (z;0) + \alpha_1.e_{l_1} + \alpha_2.e_{l_2} + \ldots + \alpha_s.e_{l_s} \quad \alpha_i \in GF_{(p)}$, $e_{l_i} \in I_r, 1 \leq i \leq s$

A continuação da prova é análoga à demonstração anterior. Claramente w está em $B((z;0),R)$ se $t = 0$. Para $t \neq 0$ vamos analisar dois casos. Se $s < R$,temos $w \in B((z;0),R)$ pois

$$w = (z;0) + t.e_{n+1} + \alpha_1.e_{l_1} + \alpha_2.e_{l_2} + \ldots + \alpha_s.e_{l_s}$$

Por último, $s = R$. Como há R vetores canônicos (todos distintos de e_{n+1}), existe um deles, digamos e_{l_1} , tal que $1 \leq l_1 \leq n-R+1$. Logo

$$w = (z;0) + t.\left(e_{n+1} + t^{-1}\alpha_1.e_{l_1}\right) + \alpha_2.e_{l_2} + \ldots + \alpha_R.e_{l_R}$$

Por construção , $e_{n+1} + t^{-1}\alpha_1.e_{l_1} \in A$, satisfazendo às condições de 9.3 .□

Observações:

(1) A cota superior encontrada equivale a $\frac{\gamma(n,p,n-R)}{p^{n-R+1}}$ do limite trivial $p^{p(n-R+1)}$. Quanto menor $\gamma(n,p,n-R)$ e maior $^{n-R+1}$, melhor a cota em relação ao limite trivial.

(2) Em particular, o caso p primo e $R = 1$ coincide com o teorema 4.1 de [BL].

(3) Em [Os], página 16, consta o resultado seguinte.Se p é primo ou potência de primo então

$$\gamma(pn+1,p,pn-R+1)) \leq \gamma(n,p,n-R)p^{n.(p-1)}$$

Ora, da proposição 8.4 e de 9.15 , temos

$$\gamma(pn+1,p,pn-R+1)) \leq \gamma(n,p,n-R)p^{n.(p-1)}$$

Logo, o teorema acima implica o resultado apresentado em [Os] .

Corolário 9.16 [BL]: Para p primo ou potência de primo e R arbitrário, vale

$$\sigma(p+1,p,p) \leq p^{p-1}$$

Prova : Basta tomar $n = R = 1$ em 9.15

Esta classe de desigualdades produz as melhores delimitações possíveis, como havíamos comentado anteriormente.

Exemplos:9.17

(a) Se $n = 4$, $R = 1$ e $p = 3$ então $\sigma(13,3) \leq 9.3^8 = 3^{10}$, sendo este limite ótimo (ver seção 7).

(b) Se $n = 3$, $R = 1$ e $p = 3$ obtemos $\sigma(10,3) \leq 5.3^6$, cujo limite coincide com a tabela em [Os].

(c) De $\gamma(5,2,3) = 2$ temos $\gamma(10,2,8) \leq 2^5$, melhorando o limite $\gamma(10,2,8) \leq 2^6$ obtido através de $\gamma(5,2,5) = 2$.

(d) Como $\gamma(8,2,5) = 4$, vale $\gamma(13,2,10) \leq 2^6$.

(e) De 9.16 : $\sigma(4,3) \leq 3^2$, $\sigma(5,4) \leq 4^3$, $\sigma(6,5) \leq 5^4$, ... estas estimativas são ótimas.

Seja M uma R-cobertura de V_k^r e $\overline{M}$ um subconjunto de M satisfazendo a propriedede: todo m em M pode ser expresso como $m = \alpha.\overline{m}$, onde $0 \leq \alpha \leq k-1$ e $\overline{m} \in \overline{M}$.

Lema 9.18 Considere M e $\overline{M}$ nas condições mencionadas , com $\left|\overline{M}\right| = v$. Se $n = r + v$ então

$$\gamma\left(n,k,n-R\right) \leq \left[1+(r-R+1).(k-1)\right]k^v$$

Prova: Tome S o subconjunto de V_k^r constituído pelos vetores do tipo $z = \alpha.e_j$, onde $0 \leq \alpha \leq k-1$ e e_j o j-ésimo vetor unitário de V_k^r com $1 \leq j \leq r-R+1$. Claramente $|S| = [1+(r-R+1).(k-1)]$. Defina $A = (\overline{M}; I_r)$.

Dado x em V_k^r , existe $m \in M$ com $d(x,m) = s \leq R$. Como $m = \alpha.\overline{m}$ e $\overline{m} \in \overline{M}$, temos :

$$x = \alpha.\overline{m} + \alpha_1.e_{l_1} + \alpha_2.e_{l_2} + \ldots + \alpha_s.e_{l_s}.$$

Não há nada a fazer se $s < R$. Quando $s = R$, pelo Princípio da Casa do Pombo, existe um vetor canônico, digamos e_{l_1} , satisfazendo $1 \leq e_{l_1} \leq r-R+1$. Como $\alpha_1.e_{l_1} \in S$ e $\overline{m} \in A$, concluímos que S é uma R-cobertura de V_k^r usando A e a tese segue pelo teorema 9.3 .

Observação :

(1) Este lema pode fornecer melhores estimativas para $\gamma\left(n,k,n-R\right)$ se

$$\left[1+(r-R+1).(k-1)\right] \leq \gamma\left(r,k,r-R\right)$$

Como a maioria dos valores γ é desconhecida, a cota proveniente deste lema melhora o limite trivial quando $\left[1+(r-R+1).(k-1)\right] \leq k^{r-R}$, ou equivalentemente,

$$(r-R+1) \leq k^{(r-R-1)} + k^{(r-R-2)} + \ldots 1$$

mas esta desigualdade acontece desde que $(r-R+1) \leq r-2$.

Teorema 9.19 Para $a = \gamma(r, k, r-R)$ acontece :

$$\gamma(a+r-1, k, a+r-1-R) \leq [1+(r-R+1).(k-1)]\, k^{a-1}$$

Prova: Conside M uma R-cobertura minimal de V_k^r contendo o vetor nulo. Aplique 9.18 para $\overline{M} = M - \{0\}$.

Exemplos 9.20

(a) Sabemos que $\sigma(4,4) = 24$ (seção 7) . Definindo $r = k = 4$ e $a = 23$, o teorema 9.19 fornece $\sigma(27,4) \leq (1+4.3).4^{23} = 13.4^{23}$.

(b) Como $\sigma(6,3) \leq 73$, significa que existe 1-cobertura de V_3^6 com 73 palavras , sendo uma delas o vetor nulo . Para esta situação , $\sigma(78,3) \leq 13.3^{72}$, melhorando o limite $\sigma(78,3) \leq 3^{75}$ desde que $\sigma(13,3) = 3^{10}$.

(c) De $\sigma(6,2) = 12$, vem $\sigma(17,2) \leq 7.2^{11}$ que equivale a $\frac{7}{8}$ do limite $\sigma(17,2) \leq 2^{14}$, pois $\sigma(8,2) = 2^5$ (ver seção 7) . Mais ainda , o caso $\sigma(7,2) = 16$ produz $\sigma(22,2) = 2^{18}$, melhorando $\sigma(22,2) \leq 7.2^{16}$ obtido anteriormente.

A diminuição da cardinalidade de $\overline{M}$ necessita de uma propriedade particular: múltiplos de "poucas" palavras-código geram toda a cobertura M . Tal situação ocorre nas seguintes situações:

Corolário 9.21 Seja $R \geq 1$ e p primo . Suponha ainda que exista um subgrupo M no grupo aditivo V_p^r tal que M também é uma R-cobertura de V_p^r com $|M| = p^b$. Se $v = \frac{p^b-1}{p-1}$ e $n = r+v$ então:

$$\gamma(n, k, n-R) \leq [1+(r-R+1).(k-1)]\, p^v$$

Prova: Como p é primo, todo elemento não nulo de V_p^r tem ordem p . Desse modo, M pode ser particionado em classes laterais disjuntas (desconsiderando o elemento nulo do grupo) . Defina $\overline{M}$ como sendo a união de representantes (geradores) de cada classe lateral. Logo, $\left|\overline{M}\right| = v = \frac{p^b-1}{p-1}$ e

seus múltiplos geram o subgrupo M . O lema 9.18 completa a prova.□

Corolário 9.22 [Ca2] Nas condições do corolário acima, para $R = 1$ e $1 + (p-1)r$ potência de p, vale:

$$\sigma(n,p) \leq [1 + (p-1)r]\, p^v$$

Prova: Basta aplicar 9.91 e o resultado devido a Zaremba [Za] , o qual passamos a descrever.

> Considere $(V_p^r, +)$ grupo aditivo, onde p é primo. Seja $S = \{ ie_j : 0 \leq i \leq p-1, e_j \in I_r\}$. Se $1+(p-1)r$ é primo ou potência de primo, então existe um subgrupo $M < V_p^r$ tal que $M + S = V_p^r$ e $|M| = \frac{p^r}{1+(p-1)r}$□.

Observações:

(1) O caso $r = p+1$ e $|M| = p^{p-1}$ deste corolário coincide com o teorema 3.4 de [Ca2] .

(2) A cota obtida por 9.22 equivale a $\frac{1}{p^{r-1}-s}$ do limite trivial .

Teorema 9.23 [Ca2] Para todo n, $k \geq 2$, se $k(n-2-R) < n-2$ então

$$\gamma(n,k,n-R) \leq (k-1).k$$

Prova: Tome S em V_k^{n+1} formado pelas palavras $(a,a,\ldots,a)$, onde $a \neq k-1$. Defina a matriz $(n-1) \times n$ abaixo :

$$A = \begin{bmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 1 \end{bmatrix}$$

Por 9.3, basta provar que S é R-cobertura de V_k^{n-1} usando A . Se x em V_k^{n-1} tem $n-1-R$ letras iguais então não há nada a fazer . Caso contrário, x obrigatoriamente deve apresentar $n-R$ letras do tipo $k-1$. Neste caso:

$$x = (0,0,\ldots,0) + (k-1)(1,1,\ldots,1) + \sum_{i=1}^{R-1} \alpha_{t_i} e_{t_i}$$

e a tese segue por 9.3 .□

Exemplos 9.24
(a) $\gamma(8,4,3) \leq 12$
(b) $\gamma(9,3,4) \leq 6$, melhorando o limite $\gamma(9,3,4) \leq 9$ em 8.15 .

Tabela

Ilustramos na seguinte tabela alguns limites obtidos nesta seção. As letras correspondem aos exemplos originários de tais delimitações: A= 9.12 , B= 9.14 , C =9.17 , D =9.20 , E =9.24 . O símbolo • indica que o resultado coincide com [Os] e $\star$ que o limite é ótimo.

$\gamma(16,2,12) \leq 2^7$ A	$\gamma(16,2,13) \leq 7.2^7$ B
$\gamma(17,2,16) \leq 7.2^{11}$ D	$\gamma(13,2,10) \leq 2^6$ C
$\gamma(22,2,21) \leq 2^{18}$ D	$\gamma(10,2,8) \leq 2^5$ C
$\gamma(17,3,11) \leq 3^6$ A	$\gamma(46,3,45) \leq 11.3^{40} B$
$\gamma(13,3,12) \leq 3^{10}$ C$\star$	$\gamma(10,3,9) \leq 5.3^6$ C •
$\gamma(78,3,75) \leq 13.3^{72}$ D	$\gamma(9,3,4) \leq 6$ E
$\gamma(4,3,3) \leq 9$ C$\star$	$\gamma(5,4,4) \leq 4^3 \star$ C
$\gamma(27,4,26) \leq 13.4^{23}$ D	$\gamma(8,4,3) \leq 12$ E

10 Abordagem Computacional

10.1 Grafos

Um[1] *grafo* G consiste em um par ordenado (V, E) onde:

(i) V é um conjunto não vazio cujos elementos são chamados *nós* ou *vértices* de G ;

(ii) E uma relação"binária"($E \subset V^{(2)} = \{Y \subset V : |Y| = 2$) cujos componentes recebem o nome de *arestas* de G .

Uma aresta do tipo (x, x) é chamado *laço*. Dois vértices , x e y , são *adjacentes* se eles estão ligados por uma aresta , $(x, y) \in E$.

Para cada nó x em $G = (V, E)$, denote por V_x os nós adjacentes a x: $V_x = \{y \in V : (x, y) \in E \}$ e $E_x = \{(x, y) \in E : \{x, y\} \cap V \neq \emptyset\}$. Por último, defina o subgrafo $G_x = \{V \setminus V_x, E \setminus E_x\}$.

Dado seu interesse particular, apresentaremos um problema clássico em Teoria dos Grafos intimamente relacionados com a cobertura por hipertorres (ver [PS]).

Conjunto Dominante

Um *conjunto dominante* H em um grafo G é uma coleção de vértices que "dominam " todos os outros nós , ou melhor, para todo vértice x em G ,ou x está em H , ou existe um vértice y em H adjacente a x .

Um conjunto dominante minimal é um conjunto dominante tal que nenhum vértice possa ser removido sem destruir a propriedade de dominância . O menor número de vértices $ND(G)$ de um conjunto dominante minimal é denominado *número dominador*.

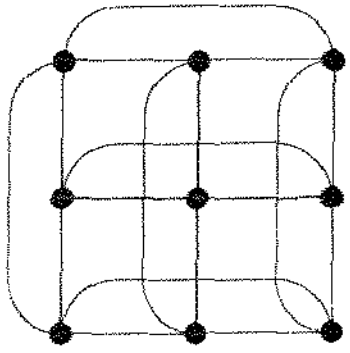
[1]Tópico obtido com a colaboração do prof. Cid C. Souza ,DCC-Unicamp

Formulação da cobertura por hipertorres via grafos

Dados naturais n , k e R , considere o grafo $Q_k^n(R) = (V, E)$ onde $V = V_k^n$ e $E \subset V^{(2)}$ tal que

$$(x, y) \in E \Leftrightarrow 1 \leq d(x, y) \leq R$$

Exemplo 10.1 O caso $n = 2$, $k = 3$ e $R = 1$ está associado ao grafo $Q_3^2(1)$ abaixo:



Propriedades de $Q_k^n(R)$

Para que um grafo sem laços $G = (V, E)$ possa estar associado à um problema de cobertura por hipertorres , ele deve apresentar as características seguintes:

(a) $|V| = k^n$;

(b) G é regular, o grau corresponde a $\sum_{i=1}^{R} \binom{n}{i} \cdot (k-1)^i$:

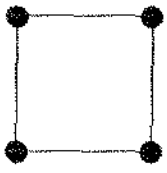
(c) para todo nó x em G , G_x é isomorfo (isomorfismo de grafos: $\cong$) a $Q_{k-1}^n(R)$, devido ao resultado:

Proposição 10.2 : Para todo nó x em $Q_k^n(R)$, vale :

$$Q_k^n(R)_x \cong Q_{k-1}^n(R)$$

Prova: A tese se verifiva para $x = (k-1, k-1, \ldots, k-1)$ pela própria definição de $Q_k^n(R)_x$. Os outros casos podem ser reduzidos ao anterior através de representação do grupo V_k^n por translação, desde que $d(u, v) = d(\phi(u), (\phi(v))$ para toda translação ϕ em V_k^n $\square$.

Exemplo 10.3: Para todo x no exemplo anterior, temos a representação de $Q_3^2(1)_x$:



Apresentamos a cobertura por hipertorres em termos da Teoria dos Grafos, cuja formulação segue. Dado o grafo $Q_k^n(R)$, uma R-cobertura minimal H de V_k^n pode ser interpretada como um subconjunto de vértices H em $Q_k^n(R)$ de cardinalidade mínima, satisfazendo à propriedade: para todo nó x em $Q_k^n(R)$, ou x está em H ou x é adjacente a um nó em $Q_k^n(R)$. Ora, esta situação corresponde à determinação do conjunto dominante minimal H em $Q_k^n(R)$. Portanto, estabelecemos a relação formal :

Proposição 10.4: Para todo n , k e R , temos

$$\gamma\left(n,k,n-R\right) = ND\left(Q_k^n(R)\right)$$

Comentários 10.5 Algumas propriedades mencionas de $Q_k^n(R)$ nos levam a conclusão de que estas classes de grafos apresentam estruturas muito particulares: grande simetria , alta regularidade, propriedade de decomposição (proposição 10.2) . Isto sugere que o tamanho grupo de automorfismos de $Q_k^n(R)$ é relativamente alto.

Desse modo, a cobertura por hipertorres pode ser reduzida a uma classe muito particular do problema conjunto dominante.

10.2 Programação Linear Inteira

Na[2] primeira parte desta seção, estabelelecemos a relação entre o problema do conjunto dominante e a cobertura por hipertorres. Também é possível formular este problema em termos de Programação Linear Inteira.

Considere H um conjunto dominante minimal de $Q_k^n(R) = (V, E)$. Para

[2]Tópico obtido com a colaboração do prof. Cid C. Souza ,DCC-Unicamp

cada nó u em V , associe a função característica

$$x_u = \begin{cases} 1 & se \quad u \in H \\ 0 & se \quad u \notin H \end{cases}$$

Desse modo, a asserção H é um conjunto dominante pode ser expressa por :

$$x_u + \sum_{v \in V_u} x_v \geq 1 \qquad \forall u \in V$$

Neste contexto, a minimalidade de H é representada pelo mínimo da função objetiva $\sum_{u \in V} x_u$.

Proposição 10.6: Dado $Q_k^n(R) = (V, E)$, vale a igualdade:

$$\gamma\,(n, k, n-R) = \min \left\{ \sum_{u \in V} x_u : \qquad x_u + \sum_{v \in V_u} x_v \geq 1 \qquad \forall u \in V \right\}$$

Prova: Consequência imediata dos comentários acima e de 10.4.

A determinação do valor exato de $\gamma(n, k, n-R)$ envolve duas etapas, a saber : construir uma R-cobertura em V_k^n de tamanho $\gamma(n, k, n-R)$; segunda etapa, mostar a não existência de um conjunto com menos de $\gamma(n, k, n-R)$ vetores satisfazendo a propriedade de cobertura .

A interpretação da cobertura por hipertorres via Programação Linear possibilitou a obtenção de boas cotas superiores e inferiores de $\gamma(n, k, n-R)$ (algumas exatas) , para valores pequenos dos parâmetors n, k e R .

No entanto, tal método revela-se pouco eficiente basicamente por dois motivos. Primeiro, em geral apresenta distância relativamente grande entre as duas cotas de $\gamma(n, k, n-R)$. Segundo, por se tratar de um problema NP-completo, a busca de limites via Programação Linear torna-se rapidamente infactível na medida que forem aumentando os valores dos parâmetros.

Contudo, cotas superiores já foram obtidas graças a um método chamado "Simulated Annealing" que passamos a comentar .

10.3 Algoritmo "Simulated Annealing"

No início da década de 80, alguns pesquisadores desenvolveram um algoritmo probabilístico conhecido por "Simulated Annealing" (ver [AK]). Esta técnica consiste basicamente da versão aleatória do método de iterações melhoradas , utilizado em problemas de otimização combinatória.

Inicialmente,"Simulated Anealing" foi empregado na determinação de cotas para o problema do campeonato de futebol com n jogos (ver seção 7) , possibilitando o limite $\sigma(6,3) \leq 74$.

Laarhoven e outros [LAL], em 1989, obtiveram os resultados:

(a) $\sigma(6,3) \leq 73$, melhorando em uma unidade o limite já mencionado. No entanto, a cobertura com 72 torres revelou-se infrutífera, apesar de ter sido feita centenas de milhares de iterações. Os autores constataram que, do ponto de vista computacional, há evidências que $\sigma(6,3) = 73$;

(b) Após 100 horas de execução em um computador VAX 11/785 , encontraram uma cobertura que implica $\sigma(7,3) \leq 186$.

Tais resultados ilustram a grande dificuldade na determinação de boas cotas superiores para códigos de tamanho relativamente grande, mesmo usando algoritmos não determinísticos.

No entanto, o uso simultâneo de "Simulated Annealing" e do método de cobertura por matrizes tem se revelado eficaz para parâmetros poucos maiores dos do método anterior, inclusive para $\sigma(n,3)$ onde $n = 8, 9, 11, 12$ e para $\gamma(n,k,n-R)$ com $R \geq 2$.

Uma aplicação de "Simulated Annealing "

A principal consequência do método cobertura por matrizes diz que: se S é uma R-cobertura de V_k^r usando a matriz $A_{r\times n}$ então $\gamma(n,k,n-R) \leq |S|.k^{n-r}$.

Este método pode ser reduzido ao problema de otimização combinatória descrito abaixo.

Dados n , k e R , inicialmente fixamos r e $t = |S|$. Em seguida, produza configurações $W = (S,A)$ onde

$$\Omega = \{W = (S,A) : \ S \subset V_k^r, \ |S| = t, \ A_{r\times n}\}$$

Considere a função *custo* c de W como sendo o número de palavras fora da cobertura W (ver definição 9.1) , ou melhor:

$$c(W) = \left| \left\{ V_k^r \setminus \left\{ s + \sum_{j=1}^{R} \alpha_j a_j \ : \ s \in S,\ \alpha_j \in Z_k,\ a_j \in A \right\} \right\} \right|$$

Assim, o problema equivale à determinação de $W^* \in \Omega$ que minimiza a função custo c . Se , por sorte, for encontrado um código $W = (S, A)$ satisfazendo $c(W) = 0$ então S é uma R-cobertura de V_k^r usando A e pelo teorema 9.3, temos $\gamma(n, k, n - R) \leq t.k^{n-r}$. Nesta situação, t é decrescido em 1 unidade e o problema novo é executado.

O algoritmo "Simulated Annealing" foi utilizado no problema de mínimo relativo ao método das matrizes por vários pesquisadores, apresentando boas cotas superiores para vários parâmetros . No artigo [LAL] consta o limite $\sigma(8, 3) \leq 486$ (encontrado em pouco mais de 10 minutos num computador VAX 11/785) . Por sua vez, [Ko] apresenta $\sigma(9, 3) \leq 53.3$[3] .

Através deste procedimento, [Os] fornece os limites $\sigma(11, 3) \leq 9477$ e $\sigma(12, 3) \leq 27702$, bem como vários coberturas com raio $R \geq 2$.

10.4 Busca Tabu

A[3] Busca Tabu é um procedimento adaptativo que vem sendo empregado na resolução aproximada de um vasto universo de problemas de otimização combinatória (ver [Gl-1], [Gl-2]).

Tal algoritmo explora o espaço de soluções a partir de uma solução inicial que é modificada sucessivamente. Assim, a sequência de soluções visitadas descreve um caminho no espaço de soluções. O Tabu consiste em um mecanismo que tem como objetivo principal evitar que o caminho descrito pela busca possua ciclos, o qual reduziria a abrangência da busca no espaço de soluções. Para a escolha da solução a ser visitada é necessário que se defina a vizinhança da nesma. O critério de seleção da próxima solução corrente, embora guloso, considera apenas as soluções dentro da vizinhança que podem ser alcançadas através de movimentos que não são tabu, daí o nome Busca Tabu.

[3]Esta descrição da Busca Tabu é devido ao prof. Marcus V.S.P. Aragão , DCC-Unicamp

A aplicação da Busca Tabu na determinação do menor conjunto dominante de um grafo utiliza como espaço de soluções todos os subconjuntos do conjunto de vértices V. Abaixo descreveremos o mecanismo para a obtenção de conjuntos dominantes dentro deste espaço. Neste problema, a vizinhança de uma solução corrente é definida como os subconjuntos de V obtidos pela exclusão ou inclusão de um outro vértice do grafo. Descarta-se aqui a possibilidade de se considerar apenas o espaço de conjuntos dominantes devido à severas restrições impostas sobre o caminho de busca em um espaço assim definido.

Falta comentar como o tabu é utilizado e como as soluções que não são conjuntos dominantes são descartadas. O primeiro é implementado pela proibição de entrada , ou saída (caso esteja dentro), de um vértice da solução corrente. Um tabu é imposto sobre a troca de um vértice quando o seu movimento na iteração anterior degradou uma função que avalia a qualidade do subconjunto de vértices corrente. Esta função poderia ser simplesmente a cardinalidade deste subconjunto, pois procura-se o menor subconjunto dominante, entretanto, é preciso que esta condição (dominância) se verefique. Para tal, contabiliza-se durante todo o procedimento o número de vértices do subconjunto corrente que dominam cada um dos vértices de V. Desse modo, uma função para medir a qualidade de um subconjunto pode ser obtida através do produto de uma "penalidade " (um número positivo) pelo número de vértices de V não atingidos pela cobertura da solução corrente adicionado a cardinalidade deste último. Um valor "grande "desta penalidade garante que o caminho descrito pela Busca Tabu irá convergir para um subconjunto dominante.

A Busca Tabu procede repetindo diversas vezes um número fixado de iterações. Para cada repetição, tanto a solução corrente como o valor da penalidade são modificados, de tal forma que este valor descreve uma função dente de serra compreendida entre zero e um número suficientemente grande. Ao final de um ciclo de repetições entre os valores das penalidades, sem que seja encontrado um conjunto dominante de valor inferior ao do menor conjunto dominante obtido até o ciclo anterior, o procedimento termina.

Uma aplicação da Busca Tabu

Um trabalho relativo à aplicação da Busca Tabu no problema das hipertorres está sendo desenvolvido pelos professores do DCC-UNICAMP : Cid

C. Souza e Marcus V.S.P. Aragão e pelos orientador e autor desta tese.

Embora em fase inicial de pesquisa, tal trabalho já apresenta resultados animadores. De uma bateria de simulações executadas para vários parâmetros da função γ, obteve-se boas cotas superiores em tempo relativamente pequeno (menos de um minuto em alguns casos).

Citamos o limite $\gamma(5,3,2) \leq 8$, dado pelas palavras-código:

01101	10022
02212	21200
02220	21202
10010	22112

A tabela abaixo ilustra alguns dos limites mais significativos. O número em colchetes indica a cota conforme [Os] e o símbolo •, que o limite coincide com o valor apresentado nesta referência.

$\gamma(6,3,1)$	≤ 73 •	
$\gamma(5,3,2)$	≤ 8 •	
$\gamma(6,3,2)$	≤ 17 •	
$\gamma(7,3,1)$	≤ 189	[186]
$\gamma(5,4,2)$	≤ 16 •	
$\gamma(4,5,1)$	≤ 52	[51]
$\gamma(4,5,2)$	≤ 11 •	

Capítulo III

Partições Polarizadas Infinitas

11 Alguns Tópicos de Teoria dos Conjuntos

Assumimos como pré-requisito alguma familiaridade com a Teoria dos Conjuntos de Zermelo-Fraenkel (ZF) , principalmente os tópicos referentes aos números: cardinais (manipulação aritmética) e ordinais . A título de revisão, comentaremos brevemente (embora seja necessária uma extensa lista de definições) alguns tópicos que serão utilizados no decorrer do capítulo.

Dado uma função $f : X \to Y$ e $A \subset X$; $f \restriction A$ representa a restrição de f em A , e $f"A$ a imagem de $f \restriction A$. Indicamos por $|X|$ a cardinalidade de X e ω o conjunto dos números naturais. Em geral, as notações seguem as mesmas de Jech [Je].

Uma ordem linear $(P, \leq)$ tal que todo subconjunto não vazio de P tem menor elemento recebe o nome de boa ordem. Um conjunto X é transitivo se : $\forall y(y \in X \Rightarrow y \subset X)$.

Definição 11.1 Todo conjunto transitivo e bem ordenado pela relação de pertinência é denominado *número ordinal* (ou simplesmente *ordinal*).

Para cada ordinal α , $\alpha + 1 = \alpha \cup \{\alpha\}$. Se existe um ordinal β tal que $\beta + 1 = \alpha$, então α é ordinal sucessor ; caso contrário, α é ordinal limite.

Definição 11.2 Um ordinal κ é *número cardinal* (*cardinal*) se não existe uma bijeção $f : \lambda \to \kappa$ para algum $\lambda \in \kappa$.

Para cada cardinal, λ^+ denota o menor cardinal maior que λ . Um cardinal $\kappa \neq 0$ é sucessor se existe um cardinal λ com $\lambda^+ = \kappa$; caso contrário, κ é cardinal limite. Todo cardinal infinito pertence à classe dos ordinais limites.

Proposição 11.3 (Lei de absorção dos cardinais infinitos) Se κ e λ são cardinais, com pelo menos um infinito, então :

$$\kappa + \lambda = \kappa.\lambda = \max\{\kappa, \lambda\}$$

Prova : ver [Je] .

Axioma da Escolha

O *Axioma da Escolha* (AC) afirma:

> " toda família de conjuntos não nulos Ω possui *função escolha*, isto é, existe c em Ω tal que $c(X) \in X$ para todo $X \in \Omega$."

Denotamos por ZFC a teoria ZF munida do AC (este axioma é indepeudente de ZF). Há várias asserções equivalentes do AC, dentre elas, citamos:
(a) Lema de Zorn ,
(b) Todo conjunto possui uma boa ordem .

Um versão mais fraca do AC , conhecida como forma enumerável do axioma da escolha (AC_ω) , postula :

> " toda família enumerável de conjuntos não vazios possui função escolha, particularmente, a união enumerável de conjuntos enumeráveis é enumerável ".

Cardinais Inacessíveis

Considere α um ordinal limite; a *cofinalidade* de α (notação : $cof(\alpha)$) denota o menor cardinal β tal que existe uma função $f : \beta \to \alpha$ cuja imagem $f"\beta$ não é limitada em α , ou equivalentemente,

$$cof(\alpha) = \beta \Leftrightarrow \beta = \min\left\{\lambda \leq \alpha : \quad \alpha = \bigcup_{i \in I} C_i : |I| = \lambda \ , \ \forall i \in I \ (|C_i| < \alpha)\right\}$$

onde λ é cardinal. Um cardinal infinito *regular* satisfaz a propriedade $cof(\alpha) = \alpha$. São exemplos de cardinais regulares : $\omega = \aleph_0$, cardinais sucessores , $cof(\alpha)$ se α é ordinal limite. Como $cof(\aleph_\omega) = \omega$, $\aleph_\omega$ não é regular.

Um cardinal κ é *limite forte* se : $2^\lambda < \kappa$ para todo $\lambda < \kappa$. Claramente ω é limite forte, mas $\aleph_1$ não o é .

Definição 11.4: Um cardinal κ com as características : $\kappa > \omega$, κ limite forte e regular recebe o nome de *cardinal inacessível* .

Sabe-se que demonstrar a existência de um cardinal inacessível no âmbito de ZFC não é possível, supondo a consistência desta teoria.

Hipótese do Contínuo Generalizada

No início deste século, Cantor já havia demonstrado o resultado abaixo, o qual ficou conhecido como:

Teorema de Cantor: Para todo cardinal κ , vale $\kappa < 2^\kappa$ ($\kappa^+ \leq 2^\kappa$) .
Prova : ver [Je].

A asserção (também independente de ZF) proposta por Cantor segue.

A *Hipótese do Contínuo Generalizada* (GCH) :

" $\forall$ κ cardinal infinito $\nexists$ cardinal λ tal que $\kappa < \lambda < 2^\kappa$."

Em vista do teorema de Cantor , GCH pode ser reformulada como :

$$\kappa^+ = 2^\kappa \text{ para todo cardinal infinito } \kappa .$$

Sabe-se que ZF$\vdash$ GCH$\rightarrow$AC , fato demonstrado por Sierpinski em 1927 (ver [Je]).

Axioma da Determinação

Denote por $P(\omega^\omega)$ o conjunto formado por todos os subconjuntos de $\omega^\omega = \{f : f : \omega \to \omega\}$. Considere dois jogadores, digamos A e B , disputando a partida $X \subset P(\omega^\omega) : X \to G_X$ tal que o resultado deste jogo, G_X , é definido por uma sequência em ω^ω

$$a_1, b_1, a_2, b_2, \ldots, a_i, b_i, \ldots$$

sujeito à regra: o segundo jogador B escolhe um natural b_i logo após o jogador A ter escolhido um natural a_i , para $i \in \omega$ (cada jogador conhece os movimentos prévios na elaboração da sequência).

A norma estabelece que A vence o jogo X se G_X está em X ; caso contrário, B o vence. Uma *estratégia vencedora* do jogo X consiste em um plano de jogo , segundo o qual, o competidor que escolher os números baseado neste plano sempre vence a partida X . O jogo X é *determinado* se um dos participantes possui uma estratégia vencedora.

O *Axioma da Determinação* (AD) postula:

" todos os jogos são determinados."

Convém observar um fato interessante : embora AD contradiga o AC , ele implica a sua versão mais fraca, ACω.

12 Teoria de Ramsey Infinita

O Princípio da Casa do Pombo afirma:

> "qualquer partição de um número finito de bolas x ($x \geq 2$) em $x-1$ classes apresenta uma delas com pelo menos 2 bolas (ou simplesmente $x \longrightarrow (2)^2_{x-1}$, conforme seção 2)."

A versão infinitária deste princípio diz:

> "se os elementos de um cardinal regular κ forem distribuídos numa quantidade de classes inferior a este cardinal , então há uma destas com κ elementos."

Análogo ao caso finito, visto na seção 2, a versão transfinita de tal princípio pode ser generalizada como segue.

Definição 12.1 Sejam κ , λ , n e δ cardinais não nulos , finitos ou infinitos. A relação de partição

$$\kappa \longrightarrow (\lambda)^n_\delta$$

significa: para toda coloração $F : \kappa^{(n)} \longrightarrow \delta$ existem uma cor $\xi \in \delta$ e um subconjunto $H \subset \kappa$, $|H| = \lambda$, tal que $F``(H^{(n)}) = \{\xi\}$ (H é monocromático ou homogêneo sobre F) , onde $X^{(n)} = \{Y \subset X : |Y| = n\}$. Escrevemos $\kappa \not\longrightarrow (\lambda)^n_\delta$ quando $\kappa \longrightarrow (\lambda)^n_\delta$ não se verifica.

Desconsideramos os casos triviais: $n = 1$, $\delta = 1$ e $\kappa < \lambda$. O enunciado do segundo parágrafo expresso em termos desta notação fica:

$$\kappa \longrightarrow (\kappa)^1_\delta \text{ para } \kappa \text{ cardinal regular e } \delta < \kappa \ .$$

A área pertinente ao estudo destas partições denomina-se Teoria de Ramsey, a qual, em termos intuitivos, consiste na determinação de alguma "ordem" (subestrutura regular) em ambientes de "grande desordem " (estrutura caótico) .

Para fixar conceitos, tomemos a função $F : \omega^{(2)} \longrightarrow 2$:

$$F(\{a,b\}) = \begin{cases} 0 & \text{se } a+b \text{ é par} \\ 1 & \text{se } a+b \text{ é ímpar} \end{cases}$$

Claramente, a classe dos números pares forma um subconjunto homogêneo de grandeza infinita . Mais ainda, a afirmação: " toda 2-coloração de $\omega^{(2)}$ apresenta subconjunto monocromático infinito" particulariza o resultado clássico devido à Ramsey , 1930 .

Teorema 12.2 (Teorema de Ramsey) Para naturais n e r , vale $\omega \rightarrow (\omega)^n_r$.
Prova: ver [DP] ou [Dr].

Sierpinski, em 1933, obteve certa classe de contra-exemplos para relações do tipo $\kappa \rightarrow (\kappa)^2_2$, mais especificamente:

Teorema 12.3: Para todo cardinal κ , $2^\kappa \not\rightarrow (\kappa^+)^2_2$.
Prova: ver [DP] ou [Je].

Cuja consequência imediata obtém-se : $\aleph_1 \not\rightarrow (\aleph_1)^2_2$, $\aleph_2 \not\rightarrow (\aleph_2)^2_2$ .... A questão da existência de um cardinal $\kappa > \omega$ em ZFC satisfazendo $\kappa \rightarrow (\kappa)^2_2$ foi solucionada pelo:

Teorema 12.4 Se $\kappa > \omega$ e $\kappa \rightarrow (\kappa)^2_2$ então κ é inacessível.
Prova: ver [DP] .

Destes fatos, conclui-se que ω é o único cardinal com a propriedade $\kappa \rightarrow (\kappa)^2_2$ no âmbito de ZFC, pois este não suporta a existência de um cardinal inacessível, conforme havíamos comentado na seção anterior.

Na década de 50, os eminentes matemáticos P.Erdös, R.Rado e A.Hajnal iniciaram o desenvolvimento de uma teoria que aborda várias generalizações e problemas variantes das partições mencionadas. Ao longo dos anos, a contribuição de muitos matemáticos nesta linha de pesquisa gerou uma extensa gama de resultados. Apresentamos mais duas contribuições importantes, pertinentes aos Fundamentos da Teoria dos Conjuntos, as quais vão ao encontro de nosso objetivo:

Teorema 12.5 Se n e r são naturais e $\kappa \geq \omega$ então $\kappa \rightarrow (\kappa)^2_2$ equivale a $\kappa \rightarrow (\kappa)^n_r$.
Prova: ver [CP2]

Teorema 12.6: A relação $\omega \longrightarrow (\omega)^n_r$ independe de ZF, pois algum uso do AC é necessário para validá-la:

$$ZF \nvdash (\omega \rightarrow (\omega)^n_r), \quad ZF \nvdash (\omega \not\rightarrow (\omega)^n_r) \text{ e } \quad ZF \vdash AC \Rightarrow (\omega \rightarrow (\omega)^n_r)$$

Prova: ver [CP2].

Contrastando a situação com expoente n finito, citamos o fato curioso:

Teorema 12.7 Embora a partição $\omega \longrightarrow (\omega)^\omega_2$ seja consistente com ZF, ela contraria o axioma da escolha.

$$ZF \vdash AC \Rightarrow (\omega \not\rightarrow (\omega)^\omega_r) \qquad (1)$$

Prova: ver [CP2] (apresentaremos uma prova alternativa de (1) na seção 14) .

Nos últimos anos, a área de pesquisa relacionada à Teoria de Ramsey tem se expandido em várias direções. Conexões e aplicações foram estabelecidas com as áreas de Geometria, Topologia. Teoria dos Números, Teoria dos Grafos , Fundamentos da Teoria dos Conjuntos.

Recentemente, conforme [NR] , surgiram novas publicações associando esta teoria às áreas de Análise Funcional, Teoria dos Ultrafiltros, Lógica-Matemática e Computabilidade.

13 Partições em Domínios de Dimensão Finita

Erdös, Rado e Hajnal foram os precursores da Teoria das Partições Polarizadas; tal fato se deve a um trabalho publicado em 1956, o qual apresenta partições de produtos cartesianos de dimensão dois, tendo este caso recebido atenção especial na maioria da literatura publicada nesta área.

Apresentamos aqui alguns resultados relativos às partições polarizadas em produtos cartesianos de dimensão finita encontrados em [CD1] ou [CD2].

Conforme seção anterior, a relação $\kappa \rightarrow (\lambda)^{\eta}_{\tau}$ pode ser vista como uma generalização da versão infinita do Princípio da Casa do Pombo. No entanto, esta generalização não é a única possível; de fato, exibiremos outra relação , conhecida como partição polarizada, que também estende tal princípio.

Definição 13.1 Considere $\lambda_1, \lambda_2, \ldots, \lambda_n, \alpha_1, \alpha_2, \ldots, \alpha_n$. δ e η cardinais, finitos ou infinitos. A *partição polarizada*

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_\eta \end{pmatrix} \rightarrow \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_\eta \end{pmatrix}_{\delta} \tag{1}$$

significa: para toda $F : \lambda_1 \times \lambda_2 \times \ldots \times \lambda_\eta \rightarrow \delta$, existem conjuntos $H_i \subset \lambda_i$, com $|H_i| = \alpha_i$ para $1 \leq i \leq \eta$ e existe uma cor $\xi \in \delta$ tal que $F"(H_1 \times H_2 \times \ldots \times H_\eta) = \{\xi\}$.

O caráter vetorial dos domínios destas colorações caracterizam as partições polarizadas como uma variante ordenada da clássica teoria de Ramsey (seções 2 ou 12). Quando $\lambda_i = \lambda$ e $\alpha_i = \alpha$ para todo $1 \leq i \leq \eta$, denotamos a relação (1) simplesmente por

$$\lambda \Rightarrow (\alpha)^{\eta}_{\delta} \tag{2}$$

Indicamos por $\not\rightarrow$ e $\not\Rightarrow$ nas situações onde (1) e (2) não se verificam, respectivamente . A classe particular formada pelo cardinais finitos α , η e δ gera a função ρ (capítulo I).

Assim como na versão finitária, é de interesse a determinação do menor cardinal transfinito λ que satisfaz $\lambda \rightrightarrows (\alpha)^{\eta}_{\delta}$.

Até o fim desta seção abordaremos exclusivamente partições polarizadas cujo domínio tem dimensão finita ($\eta \in \omega$).

Resultados Principais

Proposição 13.2: (regras de monotonicidade) Se $m \leq n$, $\delta' \leq \delta$, $\lambda_i \leq \lambda'_i$ e $\alpha'_i \leq \alpha_i$ para todo $1 \leq i \leq n$, temos

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}_{\delta} \Rightarrow \begin{pmatrix} \lambda'_1 \\ \lambda'_2 \\ \vdots \\ \lambda'_m \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha'_1 \\ \alpha'_2 \\ \vdots \\ \alpha'_m \end{pmatrix}_{\delta'}$$

Prova: Consequência imediata da definição 13.1 .

O próximo resultado apresenta consequências interessantes, permitindo o início das comparações entre as versões infinitas da teoria de Ramsey e das relações polarizadas.

Proposição 13.3 : Para todo cardinal κ , $\kappa \not\rightrightarrows (\kappa)^2_2$.

Prova : Considere a 2-coloração F em κ^2 :

$$F(\alpha, \beta) = \begin{cases} 0 \text{ se } \alpha < \beta \\ 1 \text{ se } \beta \leq \alpha \end{cases}$$

Suponha, sem perda de generalidade, que existam $H_1 \subset \kappa$ e $H_2 \subset \kappa$ com $F"(H_1 \times H_2) = \{0\}$. Fixe $\beta \in H_2$. As condições: β é ordinal ($\beta \in \kappa$), $|H_1| \leq \beta$ e κ cardinal implicam $|H_1| < \kappa$. Logo, não há formação de conjunto monocromático de tamanho $\kappa \times \kappa$. □

Observação 13.4 Em particular , a relação similar ao teorema de Ramsey não se verifica; ou seja

$$\omega \not\rightrightarrows (\omega)^n_r$$

revelando uma diferença importante entre as duas teorias. O mesmo acontece para o teorema 12.4. Contudo, enfraquecendo as exigências relativas à homogeneidade, o teorema de Ramsey pode ser utilizado para mostrar:

Proposição 13.5: Para quaisquer naturais a e r , $\binom{\omega}{\omega} \to \binom{\omega}{a}_r$.

Prova: Dado $F : \omega^2 \to 2$, tome a restrição $F \restriction \{(a,b) : a > b\}$. O teorema de Ramsey afirma a existência de um conjunto infinito H em ω monocromático. Defina H_1 como sendo os primeiros a elementos de H e $H_2 = H \setminus H_1$. Assim, $H_1 \times H_2$ forma conjunto homogêneo em F .□

Proposição 13.6: Considere a classe de funções recursivas de ω em ω :

$f_2(n) = 2.n-1 \quad f_{r+1}(n+1) = \max\{n + f_r(n+1),\ f_{r+1}(n)\} \quad f_{r+1}(1) = 1$

Nestas condições , para todo natural r :

$$\begin{pmatrix} \omega \\ f_r(n) \end{pmatrix} \to \begin{pmatrix} \omega \\ n \end{pmatrix}_r \qquad \forall n \in \omega$$

Prova : A demonstração segue por indução dupla nas variávies r e n (ver detalhes em [CP1]) .

Das regras de monotonicidade e da proposição 13.6 , claramente obtemos a proposição 13.5.

Observação 13.7 Convém notar que as duas partições concordam nas relações:

$$ZFC \vdash (\forall \kappa > \omega)\ \kappa \not\to (\kappa)^n_r \qquad e \qquad (\forall \kappa > \omega)\ \kappa \not\to (\kappa)^n_r$$

sugerindo a validade do resultado similar ao teorema 12.3 , a saber:

$$(\forall \kappa) \qquad 2^\kappa \not\to (\kappa^+)^2_2 \tag{3}$$

De um lado, a existência de cardinal satisfazendo $2^\kappa \to (\kappa^+)^2_2$ implica a negação da hipótese do contínuo, a qual é independente de ZF. Restam duas possibilidades:

(a) ou (3) é demonstrável em ZF,

(b) ou (3) é independente de ZF .

Em contrapartida, a solução desta questão pareca ser difícil, entrando na lista dos problemas em aberto. Propomos a questão : seriam (3) e a hipótese do contínuo generalizada equivalentes ?

$$\lambda \rightrightarrows (\alpha)^n_2 \text{ então } \alpha < \lambda \qquad (4)$$

O próximo teorema exemplifica relações do tipo (4) .

Lema 13.8 : Se λ_1 , λ_2 , ... λ_n são cardinais infinitos tais que $cof(\ \lambda_{i+1}) > 2^{\lambda_i}$ para todo $1 \leq i \leq n-1$, e se $\delta < cof(\ \lambda_1)$ então :

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \rightarrow \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}_\delta$$

Prova : Tome o caso $n = 2$. Dado $F : \lambda_1 \times \lambda_2 \rightarrow \delta$, considere a relação de equivalência $\sim$ em λ_2 .

$$\alpha \sim \beta \Leftrightarrow \ F(\xi, \alpha) = F(\xi, \beta) \ \ (\forall \xi < \lambda_1)$$

O número de classes de equivalência não supera 2^{λ_1} , pois

$$|\{f : \ f : \lambda_1 \rightarrow \delta\}| = \delta^{\lambda_1} \leq (2^\delta)^{\lambda_1} \leq 2^{\delta \cdot \lambda_1} = 2^{\lambda_1}$$

pela lei de absorção dos cardinais transfinitos. Assim, como λ_2 foi particionado numa quantidade de conjuntos menor que $cof(\lambda_2)$, há uma classe $H_2 \subset \lambda_2$ de tamanho λ_2 .

Defina a função auxiliar $G : \lambda_1 \rightarrow \delta$:

$$G(\xi) = F(\xi, \beta) \qquad \forall \beta \in H_2$$

Analogamente , deve existir H_1 homogêneo para G com $|H_1| = \lambda_1$, pois $cof(\lambda_1) > \delta$. Logo, $H_1 \times H_2$ é monocromático em F . A demonstração continua por indução na variável n, a passagem $n = k$ para $n = k+1$ segue em analogia ao caso $n = 2$.□

O caso mais simples deste resultado é:

$$\begin{pmatrix} \omega \\ (2^\omega)^+ \end{pmatrix} \rightarrow \begin{pmatrix} \omega \\ (2^\omega)^+ \end{pmatrix}_r \qquad \forall r \in \omega$$

Teorema 13.9: Se $n \in \omega$, κ inacessível e $\alpha, \delta < \kappa$ então $\kappa \rightrightarrows (\alpha)^n_\delta$

Prova : Dados $\alpha, \delta < \kappa$, tome $\lambda = \max\{\alpha, \delta\}$ e $\lambda_1 = \max\{\omega, \lambda^+\}$. Assim, λ_1 é cardinal regular infinito pertencente a κ , pois $\lambda < \lambda^+ \leq 2^\lambda < \kappa$.

Definindo $\lambda_{i+1} = \left(2^{\lambda_i}\right)^+$ para $1 \leq i \leq n-1$, a prova segue da aplicação do lema anterior e das regras de monotonicidade.

Nota: O teorema continua válido apenas considerando κ limite forte.

Como consequência imediata, 12.4 e 13.9 estabelecem outra conexão entre as duas teorias, a saber:

Corolário 13.10 : Se $\kappa > \omega$ e $\kappa \rightarrow (\kappa)^2_2$ então $\kappa \rightrightarrows (\alpha)^n_\delta$ para $\alpha, \delta < \kappa$

Teorema 13.11 : Para todo cardinal infinito κ e n natural:

$$\kappa^{+\,(n-1)} \not\rightrightarrows (2)^n_\kappa$$

Prova: Fixe inicialmente $n = 2$. Variando α , $\alpha < \kappa^+$, considere uma classe de funções injetoras $\{e_\alpha : \alpha \rightarrow \kappa \ , \ \alpha < \kappa^+\}$. Defina $F : \kappa^+ \times \kappa^+ \rightarrow \kappa$ por:

$$F(\alpha, \beta) = \begin{cases} 0 & se\ \alpha = \beta \\ e_{\max\{\alpha,\beta\}}(\min\{\alpha, \beta\}) + 1 & se\ \alpha \neq \beta \end{cases}$$

Não é difícil ver que não há formação de conjunto homogêneo do tipo $(2, 2)$, ou seja, não existe $H_1 \times H_2$ monocromático com $|H_i| = 2$, $i = 1, 2$.

Por hipótese indutiva, suponha a existência de uma $G : (\kappa^{+\,(n-1)})^n \rightarrow \kappa$ que não apresenta sequência homogênea do tipo $(2, 2, \ldots, 2)$ de tamanho n. Análogo ao caso $n = 2$, fixe uma função injetora $e_\alpha : \alpha \rightarrow \kappa^{+\,(n-1)}$ para cada $\alpha < \kappa^{+\,n}$. Defina $F : (\kappa^{+\,n})^{n-1} \rightarrow \kappa$ como segue. Para cada $(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})$ do domínio tome $\alpha_i = \max\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$.

$$F((\alpha_1, \alpha_2, \ldots, \alpha_{n+1})) = \left\{ \begin{array}{ll} 0 & se\ \exists\ j \neq i \text{ tal que } \alpha_i = \alpha_j \\ G\left(e_{\alpha_i}(\alpha_1), \ldots e_{\alpha_i}(\alpha_{i-1}), e_{\alpha_i}(\alpha_{i+1}), \ldots e_{\alpha_i}(\alpha_n)\right) + 1 & \text{c.c.} \end{array} \right\}$$

Seja $H_1 \times H_2 \times \ldots \times H_{n+1}$ uma sequência homogênea para F com $|H_i| = 2$, $i = 1, 2, \ldots n+1$. A cor difere de 0 pois é sempre possível encontrar uma sequência $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ em $H_1 \times H_2 \times \ldots \times H_{n+1}$ que apresente um único elemento maximal ($|H_i| > 1$). Para outras cores, tome $\alpha = \max\{H_1, H_2, \ldots, H_{n+1}\}$, digamos $\alpha \in H_i$. Por definição de F , $\prod_{j \neq i} e_\alpha{}''(H_j)$ é sequência homogênea para G , contrariando a hipótese indutiva.□

Proposição 13.12 : Para cada $n \in \omega$ e κ infinito:

$$\binom{\kappa^{++}}{\kappa^{+}} \to \binom{\kappa^{++}}{n}_{\kappa}$$

Prova : Tome $F : \kappa^{++} \times \kappa^{+} \to \kappa$. Para cada $\mu < \kappa^{++}$, $F \mid \{\mu\} \times \kappa^{+}$ determina uma partição de κ^{+} em κ . Como κ^{+} é regular, para cada μ escolha (AC) uma cor $g(\mu)$ tal que:

$$A_{\mu,g(\mu)} = \left\{\alpha < \kappa^{+} : F(\mu,\alpha) = g(\mu)\right\}$$

tenha cardinalidade κ^{+} . Variando $\mu < \kappa^{++}$, a função $g : \kappa^{++} \to \kappa$ estabelace uma partição de κ^{++} em κ partes . Logo, existem uma cor δ e um conjunto A em κ^{++} de tamanho κ^{++} tais que : $|A_{\mu,\delta}| = \kappa^{+}$ para todo $\mu \in A$.

Dado n natural ; para cada $\mu \in A$, $(A_{\mu,\delta})^{n} = \{Y \subset A_{\mu,\delta} : |Y| = n\}$ tem cardinalidade κ^{+} , pois

$$\kappa^{+} = |A_{\mu,\delta}| \leq |(A_{\mu,\delta})^{n}| = |\kappa^{+}|^{n} = \kappa^{+}$$

pela lei de absorção dos cardinais infinitos.

Variando $\mu \in A$, escolha um n-subconjunto de $(A_{\mu,\delta})^{n}$. Como $|A| = \kappa^{++}$, há um n-subconjunto destes escolhidos , digamos H_2 , que aparece κ^{++} vezes em $H_1 = \{\mu : H_2 \subset A_{\mu,\delta}\}$. Logo, $H_1 \times H_2$ é homogêneo para F .□

Como consequência imediata , temos

Corolário 13.13 : Para cada κ infinito,

$$\binom{\kappa^{++}}{\kappa^{+}} \to \binom{2}{2}_{\kappa}$$

Exemplo 13.14 : De (13.11) , obtemos $\omega^{+} \not\rightrightarrows (\omega)^{2}_{\omega}$. Por outro lado, pelo corolário acima, $\omega^{++} \rightrightarrows (\omega)^{2}_{\omega}$. Com isto, ω^{++} é o menor cardinal que satisfaz a relação $\kappa \rightrightarrows (\omega)^{2}_{\omega}$.

14 Partições em Domínios de Dimensão Infinita

Esta seção versa sobre relações do tipo $\kappa \rightrightarrows (\lambda)^{\eta}_{\delta}$ onde o expoente η assume valores infinitos. Abordamos principalmente um caso particular destas partições, conhecida como "Princípio de Ariadne " .

Assim como na seção anterior, optamos pela apresentação dos principais resultados de [CP1] e [CP2] dando ênfase nas comparações entre ZFC, Teoria de Ramsey Infinita e o Princípio de Ariadne.

Princípio de Ariadne

O nome Princípio de Ariadne é devido a uma interpretação baseada numa estória da mitologia grega.

Pedimos certa liberdade para adaptar a conhecida versão envolvendo Ariadne, Teseu e o labirinto e possibilidade de acrescentar um fato na história da matemática - esta ilustração trata de ficção científica: portanto, tudo é permitido, inclusive alterar a ordem cronológica e utilizar como personagem de nossa versão um contemporâneo mestre na arte de inventar personagens, criaturas e objetos fantásticos [Bo].

Imaginemos a situação seguinte. Ariadne, a bela filha do rei Minos, e seu amado Teseu estão presos num labirinto projetado por Dédalo e auxiliado por um perverso grupo de matemáticos. Estes já assumiam a validade de um princípio, segundo o qual, dois números sempre podem ser comparados em qualquer sistema aritmético.

Estamos numa época em que se acreditava na existência de uma única matemática. Toda verdade era passível de demonstração. Não menos verdadeiro era o princípio mencionado.

O labirinto é constituído de infinitos níveis, cada um deles possuindo infinitas portas (pontos) : $0, 1, 2, \ldots$.

Para um prisioneiro que está no nível i passar ao próximo, ele obrigatoriamente deve abrir uma porta do nível $i + 1$. A fuga se realiza quando for possível percorrer um caminho , passando em todos os $\aleph_0$ níveis do labirinto, perfazendo uma sequência de pontos $c_1, c_2, \ldots, c_n, \ldots \; n \in \omega$.

Cada um dos $2^{\aleph_0}$ caminhos está pintado de uma das cores, branco ou cinza. O labirinto foi projetado tomando-se certos cuidados:

(a) o prisioneiro não pode voltar a um nível anterior, pois as portas se fecham automaticamente

(b) dois prisioneiros não podem passar na mesma porta de um determinado nível ; logo, eles percorrem caminhos $a_1, a_2, a_3, \ldots$ e $t_1, t_2, t_3, \ldots$ totalmente disjuntos, $a_i \neq t_i$ para todo i em ω .

(c) feita inicialmente a escolha da cor, os fugitivos só podem caminhar em trilhas desta cor , pois os caminhos da outra cor são impedidos.

Além disto, o labirinto possui um sistema de bloqueio ao acesso de portas controlado por Bergos, o único auxiliar de Dédalo disposto a dedicar toda sua vida numa tarefa potencialmente sem fim. Embora cético à filosofia matemática da época, ele não esboçava qualquer oposição perante à comunidade.

Enquanto Teseu e Ariadne tentam escapar , acessos à determinadas portas vão sendo fechados da seguinte forma. Para cada nível i , se Teseu e Ariadne ocupam as portas t_i e a_i , Bergos pode impedir o acesso a uma porta do nível $i+1$, digamos a_i a a_{i+1} , de tal modo que todas os caminhos iniciados por $a_1, a_2, \ldots, a_i, a_{i+1}$ ficam bloqueados.

Dado uma coloração dos caminhos, Bergos vence se ele possui um estratégia eficaz que impeça a fuga de pelo menos um dos prisioneiros. Por outro lado, Teseu e Ariadne vencem se possuem uma estratégia que garanta a fuga dos dois , por mais que Bergos tente impedi-los através do sistema mencionado.

O *Princípio de Ariadne (PAr)* postula que

"Em todo labirinto, sempre há estratégia de fuga para Teseu e Ariadne"

Esperamos que os dois próximos resultados esclareçam a nossa versão.

Resultados

Proposição 14.1: PAr equivale a relação $\omega \rightrightarrows (2)^{\omega}_{2}$.

Prova De $\omega \rightrightarrows (2)^{\omega}_{2}$, existem conjuntos $H_1, H_2, \ldots, H_n, \ldots, |H_n| = 2$, $n \in w$ tais que $H_1 \times H_2 \times \ldots \times H_n \times \ldots$ é monocromático . Logo, se Teseu e Ariadne percorrem caminhos , digamos $t_1, t_2, \ldots, t_n$ e $a_1, a_2, \ldots, a_n$ em $H_1 \times H_2 \times \ldots \times H_n$, há pelo menos duas possibilidades no próximo nível, desde que $H_{n+1} = \{c_{n+1}, b_{n+1}\}$.

Sem perda de generalidade, suponha que Bergos bloqueie o acesso de t_n a b_{n+1} , então Ariadne pode ocupar a porta b_{n+1} e Teseu , a porta c_{n+1} . Portanto, Teseu e Ariadne possuem estratégia vencedora.

Reciprocamente, assumindo PAr, devemos mostrar a existência de $H_1 \times H_2 \times \ldots \times H_n \times \ldots$ homogêneo . Isto será feito por indução . Para $n = 1$, tome $H_1 = \{a_1, t_1\}$ as posições ocupadas pelo casal no nível 1 .

Por hipótese indutiva, existe $H_1 \times H_2 \times \ldots \times H_n$ homogêneo . Desse modo, há duas portas no nível $n + 1$, digamos b_{n+1} e c_{n+1} , tais que ambos têm acesso a elas; caso contrário, se um deles só tem acesso a uma destas portas, então Bergos poderia bloqueá-la através do mecanismo de defesa. Mas isto contraria a hipótese inicial. Definindo $H_{n+1} = \{b_{n+1}, c_{n+1}\}$, a prova segue indutivamente.□

Em seguida, apresentamos o principal resultado deste capítulo, surpreendendo os auxiliares de Dédalo e talvez o leitor também ; pois o princípio de Ariadne afirma a existência de um certo tipo de ordem (regularidade) no universo do labirinto, isto é, a destruição total da possibilidade de fuga de Teseu e Ariadne é impossível. No entanto, este tipo de ordem contradiz o axioma da escolha, o qual intuitivamente representa a essência da noção de ordem (boa ordem) em matemática.

Teorema 14.2 [CP1] O princípio de Ariadne contradiz o axioma da escolha :

$$ZF \vdash AC \Rightarrow \neg PAr$$

Prova: Defina a relação de equivalência $\sim$ em ω^{ω}:

$$p \sim q \Leftrightarrow (\exists n \in \omega)\,((\forall m \geq n)\;\; p(m) = q(m))$$

Pelo AC, tome um representante de cada classe de equivalência. Dado p em ω^ω, denote por $\overline{p}$ o representante da classe a qual p pertence e seja n_p o menor natural tal que : $(\forall m \geq n_p)\ \ p(m) = \overline{p}(m)$.

Finalmente, defina a coloração $F : \omega^\omega \longrightarrow 2$ por:

$$F(p) = \begin{cases} 0 & se \quad n_p \text{ é par} \\ 1 & se \quad n_p \text{ é ímpar} \end{cases}$$

Seja $\{H_i : i \in \omega\}$ uma coleção de subconjuntos de ω com $|H_i| = 2$ para $i \in \omega$. Vamos mostrar que $\prod_{i\in\omega} H_i$ não é monocromático para F . De fato, dado p em $\prod_{i\in\omega} H_i$, p e $\overline{p}$ satisfazem $(\forall m \geq n_p)\ (p(m) = \overline{p}(m))$.

Uma vez que $\left|H_{n_p}\right| = 2$, defina q em $\prod_{i\in\omega} H_i$ como $q(m) = p(m)$ para $m \neq n_p$ e $q(\ n_p) \neq p(\ n_p)$. Por definição, $\overline{q} = \overline{p}$ pois $p \sim q$ $(\ \forall m \geq n_p + 1\ q(m) = p(m)\ )$. Assim $n_q \leq n_p + 1$. Por outro lado, $p(\ n_p) = \overline{p}(\ n_p) \neq q(\ n_p)$. Logo $F(q) \neq F(p)$ pois $n_q = n_p + 1$. □

Corolário 14.3 : Em ZF, não existe uma sequência de naturais $a_1, a_2, \ldots, a_n, \ldots$ satisfazendo

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} 2 \\ 2 \\ \vdots \end{pmatrix}_2$$

Prova : De fato, se tal sequência de naturais exitisse, então $\omega \rightrightarrows (2)^\omega_2$ pela regra de monotonicidade. Mas pelo teorema 14.2 , teríamos a demonstração da negação do axioma da escolha , levando-nos a uma contradição , pois AC é independente de ZF.□

Pelo teorema 12.7 e o resultado acima, ambas as relações PAr e $\omega \longrightarrow (\omega)^\omega_2$ implicam a negação do axioma da escolha, sugerindo a pergunta:

Problema : São PAr e $\omega \longrightarrow (\omega)^\omega_2$ equivalentes ?

Até agora, sabe-se a resposta parcial , descrita abaixo.

Lema 14.4 [CP1] : Se $\omega \rightarrow (\omega)^{\omega}_{2}$ então para todo sequência de naturais $a_1, a_2, \ldots, a_n, \ldots, n \in \omega$ vale:

$$\begin{pmatrix} \omega \\ \omega \\ \vdots \end{pmatrix} \rightarrow \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix}_2$$

Prova : Identifique $\omega^{(\omega)}$ como o conjunto das sequências estritamente crescentes em ω^{ω} . Dado $F : \omega^{\omega} \rightarrow 2$, defina G como $F \mid \omega^{(\omega)}$. Por hipótese, existe um conjunto monocromático infinito $H \subset \omega$ para G . Tome H_1 os primeiros a_1 elementos de H , H_2 os primeiros a_2 elementos de $H - H_1$,e assim sucessivamente. Logo, $\prod_{i \in \omega} H_i$ forma conjunto homogêneo para F .□

Como consequência imediata:

Teorema 14.5 [CP1] A relação $\omega \rightarrow (\omega)^{\omega}_{2}$ implica PAr .

Observação: Por outro lado, provar a recíproca (ou refutá-la através de um contra-exemplo) continua em aberto.

Observação 14.6 : Vimos que $\omega \rightarrow (\omega)^{\omega}_{2} \Rightarrow$PAr e que PAr $\Rightarrow \neg AC$. Destes fatos, encontramos uma prova alternativa de uma parte do teorema 12.7, a saber: $\omega \rightarrow (\omega)^{\omega}_{2} \Rightarrow \neg AC$.

Problema Um problema que continua em aberto é investigar as relações entre PAr e o axioma da determinação.

Problemas

Elencamos aqui alguns problemas que não só nos parecem relevantes, mas sobre os quais esta dissertação oferece algumas informações e referências básicas. Alguns são aparentemente difíceis (marcados com $\star$) e os que apresentam um grau maior de dificuldade são marcados com $\star\star$.

1. Da existência de classes de planejamentos com parâmetros $(v, k, 1)$ derivam-se limites próximos dos otimais, conforme teoremas 3.1 e 3.5. Como estender este resultado (ou seja, encontrar limites inferiores para ρ) partindo da construção de planejamentos com parâmetros (v, k, λ), $\lambda > 1$?

2. Em termos computacionais, um desafio estimulante seria obter cotas inferiores para ρ e K (pelo menos para parâmetros pequenos do domínio) via programas baseados em construções de colorações desprovidas de conjunto monocromático .

3. É possível estender os resultados 4.5 e 5.4 para dimensões d superiores a 2 ? Isto possivelmente determinaria " boas " cotas superiores para ρ e para a função de Zarankiewicz generalizada.

4. $\star$ Como havíamos comentado, o estudo da função polarizada encontra-se em fase embrionária, contrastando com a clássica função de Ramsey. Devido à similaridade entre elas, traduzir métodos empregados na teoria clássica para a função ρ , em especial, aprofundar o método probabilístico de Erdös (ver [GRS]).

5. As relacões da partições polarizadas também podem ser reformuladas em termos de hipergrafos , permitindo talvez a tradução de delimitações através de resultados previamente conhecidos desta teoria .

6. $\star$ Qual o comportamento assintótico de $\rho(t, r, n)$?

7. $\star$ Este problema foi proposto pelo prof. Cid C. Souza, IMECC: Pode-se interpretar a cobertura por hipertorres como uma classe de problemas da programação linear inteira e neste contexto, utilizar o método de "relaxação linear ". A etapa de tranferência de soluções reais para

soluções inteiras exigiria um estudo aprofundado dos grafos associados às coberturas, tendo em vista a determinação de novas condições restritivas ao problema.

8. $\star$ Nas hipóteses do lema 9.13 e do corolário 9.21 aparecem R-coberturas cujos múltiplos escalares das palavras-código geram todo o espaço. Códigos satisfazendo tais condições relacionam-se com o problema seguinte. Encarando V_k^n como $(\mathbb{Z}_k)^n$, qual a mínima cardinalidade de $W \subset V_k^n$ cujas combinações lineares de tamanho até R cobrem todo o espaço ? Por exemplo, $W = \{(0,1),(1,0),(1,1),(2,1),(3,1),(4,1)\}$ é um código cujos múltiplos cobrem $(\mathbb{Z}_5)^2$.

9. Limites encontrados nas seções 8 e 9 foram obtidos graças à existência de certas classes de códigos latinos. A referência [Os] apresenta boas cotas superiores para γ , cujas demonstrações fazem uso de códigos normais e subnormais. Sabe-se que a existência de determinados códigos propiciaria novos limites superiores ; contudo, este problema existencial continua em aberto.

10. $\star\star$ Sabe-se que $\alpha(n,k) \geq \frac{k^{n-1}}{(n-1)}$ e que $\gamma(n,k,2) \geq \frac{k^2}{(n-1)}$. É verdadeira a conjectura: $\gamma(n,k,s) \geq \frac{k^s}{(n-1)}$ para todo s ?

11. Encontrado o valor de $\gamma(n,k,n-R)$, uma questão ainda pouco estudada refere-se à determinação da quantidade de R-coberturas minimais de V_k^n não isomorfas.

12. $\star$ Quais são as relacões entre $(\forall\kappa)\ 2^\kappa \not\rightrightarrows (\kappa^+)_2$ e a hipótese do contínuo generalizada ?

13. Vale o similar do teorema 12.5 , ou melhor: para κ infinito e r natural, $\kappa \rightrightarrows (\kappa)_2 \Rightarrow \kappa \rightrightarrows (\kappa)_r$?

14. O Princípio de Ariadne e $\omega \rightrightarrows (\omega)^\omega_2$ são equivalentes ?

15. $\star\star$ Tanto o axioma da determinação como o princípio de Ariadne contrariam o axioma da escolha, sugerindo a questão: quais as relações (se existirem) entre AD e PAr ?

Lista de Notações	
$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Z}_q$	anel dos inteiros módulo q
$GF_{(q)}$	corpo de Galois com q elementos
I_q	matriz identidade de ordem q
0_q	matriz nula de ordem q
A^T	transposta de A
$A * B$	concatenação das matrizes A e B
$(A;B)$	justaposição de B em A
$C \bullet C'$	soma direta dos codigos C e C'
$\|X\|$	cardinalidade do conjunto X
X^n	produto cartesiano de X n vezes
$X^{(n)}$	$\{Y : Y \subset X,\ \|Y\| = n\}$
$a \rightarrow (t)^n_r$	relação de partição Ramsey
$a \not\rightarrow (t)^n_r$	negação de $a \rightarrow (t)^n_r$
$a \Rightarrow (t)^n_r$	relação de partição polarizada
$a \not\Rightarrow (t)^n_r$	negação de $a \Rightarrow (t)^n_r$
$R(t,r,n)$	função de Ramsey
$\rho(t,r,n)$	função polarizada
$K_t(n)$	função de Zarankiewicz
$\gamma(n,k,n-R)$	função associada á cobertura das hiper-torres
$\sigma(n,k)$	função $\gamma(n,k,n-1)$
$d(x,y)$	distância de Hamming entre os pontos x e y
$\lfloor x \rfloor$	maior inteiro não superior a x
$\rceil x \lceil$	menor inteiro não inferior a x
$\binom{m}{t}$	função binomial , sujeita à convenção $\binom{m}{t} = 0$ se $m < t$
$\|x\|_t$	$\sum_{i=1}^{n} \binom{x_i}{t}$ para $x = (x_1, x_2, \ldots, x_n)$
$F \mid A$	função F restrita ao domínio A
$F"A$	imagem de $F \mid A$
ω	conjunto dos números naturais
$cof(\alpha)$	cofinalidade do ordinal α
α^+	cardinal sucessor de α
$\Gamma \vdash A$	A é teorema na teoria Γ
$\neg A$	negação da fórmula A
$\aleph_\alpha$	α-ésimo cardinal infinito

Bibliografia

[AK] E.H.L. Aarts e J. Korst - *Simulated Annealing an Boltzmann Machines: A Stochastic Approach to Combinatorial Optimization and Neural Computing* -Wiley, Chichester (1989).

[AvL] E.H.L. Aarts e P.J.M. van Laarhoven - *Local Search in Coding Theory* - Discrete Math . **106/107** (1992) 11-18.

[BJL] T. Beth , D. Jungnickel e H. Lenz - *Design Theory* - Bibliographisches Insttitut (1985).

[BL] A. Blokluis e C.H.M. Lam - *More Coverings by Rook Domains* - Journal of Combinatorial Theory (A) **36** (1984) 240-244.

[BM] I.F. Blake e R.C.Mullin - *The Mathematical Theory of Coding* - Academic Press, NewYork (1975)

[Bo] J.L. Borges - *O Aleph* - Editora Globo (1985)

[Ca1] W.A.Carnielli - *On Covering and Coloring Problems for Rook Domains* - Discrete Math. **57** (1985) 9-16.

[Ca2] W.A.Carnielli - *Hyper-rook Domain Inequalities* - Studies in Apllied Mathematics **82** (1990) 50-69.

[Ca3] W.A.Carnielli - *Ramsey-Type Theorems for Cubes* - Relatório Interno IMECC-UNICAMP (1986) .

[Ca4] W.A.Carnielli - *Notes on Ramsey's Cubic Numbers* - manuscrito.

[CP1] W.A.Carnielli e C.A. Di Prisco - *Some Results on Polarized Partition Relations of Higher Dimension* - Math. Log. Quart. **39** (1993) 461-474.

[CP2] W.A.Carnielli e C.A. Di Prisco - *The Principle of Ariadne and other Problems in Infinite Combinatorics* - manuscrito.

[DP] C.A. Di Prisco - *Particiones y Axiomas de la Teoria de Conjuntos* - VII Encontro Brasileiro de Lógica (1986)

[Dr] F.R.Drake - *Set Theory* - Nort-Holland Publ. Comp. Amesterdan-Oxford-New York (1974).

[Fe] P. Feofiloff - *Sobre os Números de Ramsey* - dissertação de mestrado IME-USP (1974).

[GL1] F. Glover - *Tabu Search Part I* - ORSA Journal on Computing **1** (1989) 190-206.

[Gl2] F. Glover - *Tabu Search Part II* - ORSA Journal on Computing **2** (1990) 4-32.

[GRS] R.Graham, B.Rothschild e J.Spencer - *Ramsey Theory* - Jonh Whilley & Sons . New York (1980)

[GZ] R.K.Guy e S.Znám - *A Problem of Zarankiewicz* - W.T.Tutte (editor) - "Recent Progress in Combinatorics" - Academic Press, New York (1969) 237-243.

[Je] T.Jech - *Set Theory* - Academic Press. New York (1978).

[Ko] K. Koschnick - *A New Upper Bound for the Football Pool Problem for Nine Matches* - Journal of Combinatorial Theory (A) **62** (1993) 162-167.

[KvL] H.J.L.Kamps e H. van Lint - *the Football Pool Problem for 5 Matches* - Journal of Combinatorial Theory (A) **3** (1967) 315-325.

[LAL] P.J.M. van Laarhoven , E.H.L. Aarts , J.H. van Lint e L.T.Wille - *New Upper Bounds for the Football Pool Problem for 6, 7 and 8 Matches* -Journal of Combinatorial Theory (A) **52** (1989) 304-312.

[NR] J. Nešetřil e V. Rödl (Editores)- *Mathematics of Ramsey Theory* -Springer-Verlag (1990)

[Os] P.R.J. Östegard - *Construction Methods for Covering Codes* - Doctor thesis Helsink University of Technology , Finland (1993).

[PS] C.H. Papadimitrion e K. Steiglitz - *Combinatorial Optimization: Algorithms and Complexity* - Prentice-Hall , New York (1982).

[Si] I.Simon - *Configurações Combinatórias* - $13^{\underline{0}}$ Colóquio Brasileiro de Matemática , IMPA (1981).

[Sn] R.C. Singleton - *Maximum Distance Q-Nary Codes* - IEEE Inf. Theory **10** (1964) 116-118.

[St] R.G. Stanton - *Covering Theorems in Groups (or: How to Win at Football Pools)* - W.T.Tutte (editor) - "Recent Progress in Combinatorics"- Academic Press, New York (1969) 21-36.

[Wo] S.Wolfran - *Mathematica* - Addison-Wesley Publ.Comp. (1991)

[Za] S.K. Zaremba - *Covering Problems Concerning Abelian Groups* - J. London Math. Soc. *27* (1952) 242-246.

[Zn] S. Znám - *Two Improvements of a Result Concerning a Problem of Zarankiewicz* - Colloquium Math. **13** (1965) 255-258.