Busca de Matrizes MDS de baixo custo com algoritmo genético

Tópicos em Otimização Combinatória (Equipe 8)

Giovana Kerche Bonás (RA:216832)
Henrique Finger Zimerman (RA:217771)

Matrizes MDS

- Uso em algoritmos criptográficos;
- O que são matrizes MDS?
- Desafio de complexidade;
- Como esse problema é abordado hoje?

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} a & c \\ g & i \end{bmatrix} \begin{bmatrix} b & c \\ h & i \end{bmatrix} \begin{bmatrix} d & e \\ g & h \end{bmatrix} \begin{bmatrix} d & f \\ g & i \end{bmatrix} \begin{bmatrix} e & f \\ h & i \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ g & h \end{bmatrix} \begin{bmatrix} b & c \\ e & f \end{bmatrix} \begin{bmatrix} a & c \\ d & f \end{bmatrix} \begin{bmatrix} a & b \\ d & e \end{bmatrix}$$

$$a, b, c, d, e, f, g, h, i$$

Variáveis de decisão

- Próprios elementos da matriz;

Minimizar c e d

- c é o custo da matriz
- d é a distância da matriz para uma MDS

Funções objetivos

1

$$f = \frac{k}{c \cdot (d+1)}$$

2

$$f = \begin{cases} k_1/(1+c+k_3 \cdot d) & d > 0 \\ k_2/(1+c) & d = 0 \end{cases}$$

Metodologia

- Função-objetivo
  - 1) Custo computacional $c = 3 \cdot \mathrm{XTIME} + 1 \cdot \mathrm{XOR}$
  - 2) Quantificação do quão distante uma matriz é de ser MDS d
  - 3) Função-objetivo

$$\text{fitness} = \begin{cases} k_1 / (1 + c + k_3 \cdot d \cdot c) & d > 0 \\ k_2 / (1 + c) & d = 0 \end{cases}$$

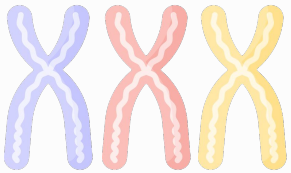
Metodologia

- Matrizes circulantes
  - Definidas pela primeira linha.
  - Cada linha subsequente é uma rotação em uma casa da linha anterior.
  - Diminui o espaço de busca e converge mais rápido.

$$\begin{bmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{bmatrix}$$

Metodologia

- População inicial;



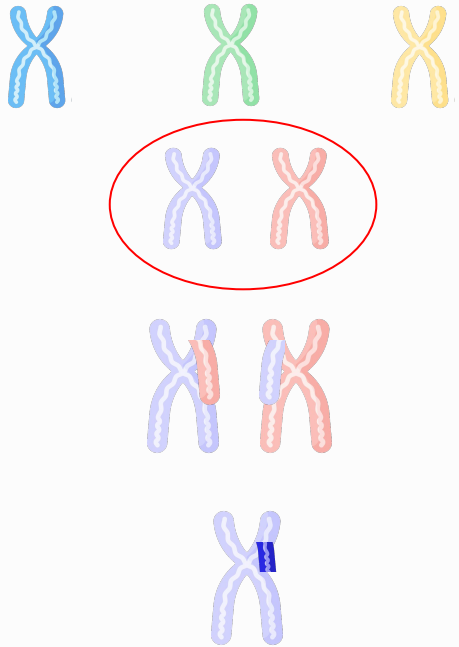
$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

- Representação dos cromossomos;

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \cdots \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix} \quad a \quad b \quad c$$

Metodologia

- Seleção (torneio);
- Crossover (2 pontos);
- Mutação
  - 1) substituição aleatória
  - 2) método de relaxação



Metodologia

- Manutenção da variedade
  - Medida de homogeneidade da população:

$$h = \frac{f - n}{p \cdot n - n}$$

  - Mantém a população ***diversificada*** pois introduz ***mutações*** aleatórias nos genes, especialmente quando a população se torna muito ***homogênea (h mais próximo de 1)***.

$$p_{mut} = p_{min} + (p_{max} - p_{min}) \cdot h^2$$

Estratégias híbridas

- Método padrão;
- Método com mutação guiada na solução incumbente;
- Método de busca local na solução incumbente;
- Método de mini busca local nos filhos;
- Método de busca exaustiva na população inicial;
- Método de busca local puro.

Avaliação dos resultados

Baseline - matrizes mais baratas da literatura

Dim	#xtime	#xor	Combined Cost
2	2	2	8
3	3	6	15
4	8	16	40
5	30	30	120
6	59	59	236
7	96	96	384
8	72	80	296
16	1248	800	4544
32	5440	3712	20032

Resultados de Serpa, 2023

Dim	#xor	#xtime	Baseline Diff	FF
2	3	2	1	$GF(2^4)$
3	24	34	21	$GF(2^8)$
4	26	32	24	$GF(2^4)$
5	89	126	96	$GF(2^8)$
6	84	120	210	$GF(2^4)$
6	54	60	0	$GF(2^4)$
7	96	104	24	$GF(2^4)$
7	112	214	370	$GF(2^8)$

Avaliação dos resultados

Configuração 1

Dim	Custo	Baseline	Tempo computacional (s)
2	5	8	153
3	15	15	415
4	49	40	1993
5	116	120	38164
6	388	236	37222

Avaliação dos resultados

Configuração 2 - Algoritmo Genético

Dim	Matriz	#xtime	#xor	Custo	Custo Baseline
4x4	(1)	8	16	40	40
5x5	(5)	15	25	70	120
6x6	(17)	30	48	138	236
7x7	(39)	42	56	182	384
8x8	(47)	88	96	360	296

Avaliação dos resultados

Configuração 2 - Busca Local

Dim	Matriz	#xtime	#xor	Custo	Custo Baseline
6x6	(22)	30	48	138	236
7x7	(33)	42	56	182	384
8x8	(42)	88	88	352	296

Principais conclusões

- Busca local melhor que algoritmo genético
- Nova função objetivo do algoritmo genético teve resultados promissores em relação aos de Serpa 2023
- Matrizes circulantes ajudaram muito
- Custos que superam o estado da arte para dimensoes 5x5, 6x6, 7x7
- Estado da arte não superado para 4x4 e 8x8
- *Possível trabalho futuro:* teste eficiente de propriedade MDS em matrizes circulantes, Malakhov, 2021

#Obrigado!