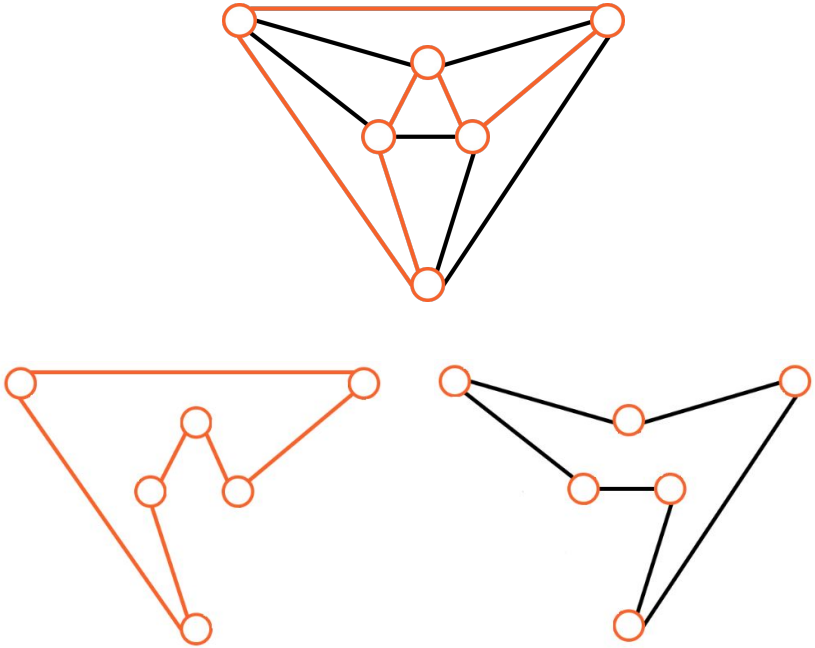
Ciclos Hamiltonianos

Demonstração de teoremas e avanço da aplicação

João Vitor Gonçalves
Paulo David

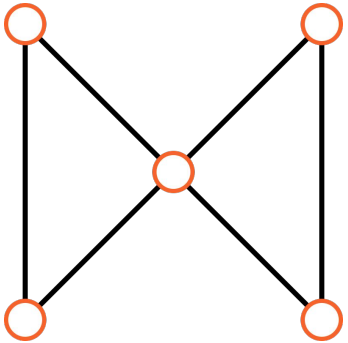
Sumário

Ciclo Hamiltoniano



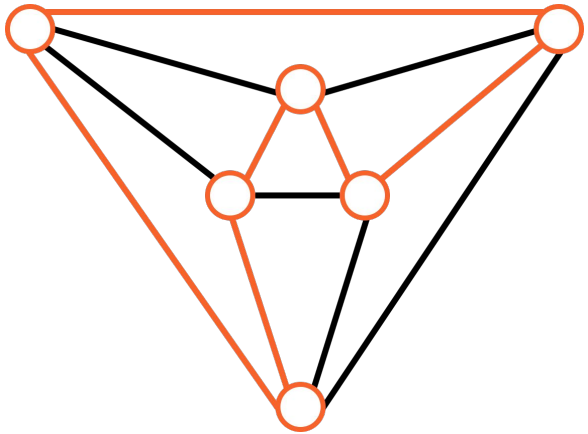
Um dos problemas em Teoria dos Grafos é definir se um grafo G possui ou não um ciclo hamiltoniano. Ou seja, um caminho que, saindo de um vértice x, passa por todos os outros e retorna para o vértice x.

Determinando se um grafo é Hamiltoniano



Conseguir afirmar que um grafo possui um ciclo hamiltoniano é um problema NP-completo, ou seja é um problema de resolução difícil e no momento ainda não se tem uma condição **necessária** e **suficiente** para apontar se um grafo é Hamiltoniano.

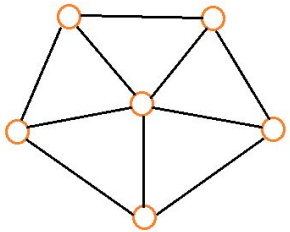
Condições Suficientes e Necessárias

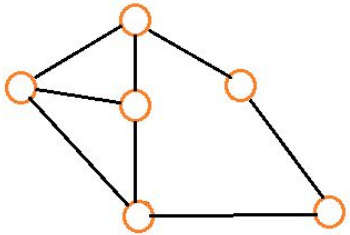


As condições Suficientes são as que caso sejam verdadeiras, provam que um grafo é Hamiltoniano, como exemplo temos os Teoremas de ***Dirac*** e ***Ore.*** Mas caso essas não sejam aplicáveis no grafo ***não podemos afirmar algo.***

Condições Suficientes

Teorema de Dirac





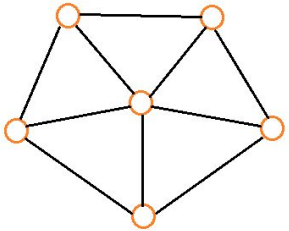
O teorema de Dirac afirma que:

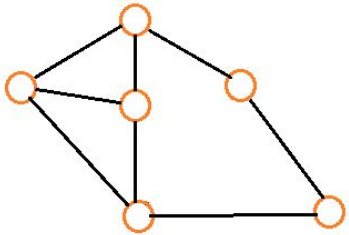
Se G é um grafo de ordem $n \geq 3$

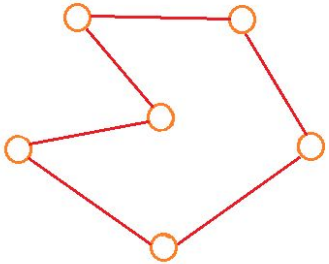
$g(v) \geq n/2$ para todo $v \in V(G)$

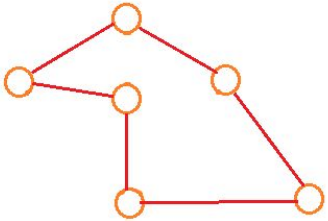
Em outras palavras, em um grafo com pelo menos 3 vértices, cada um desses vértices tem que possuir um número de arestas(grau do vértice) maior ou igual à metade da quantidade total de vértices no grafo

Teorema de Dirac





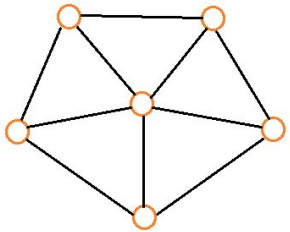


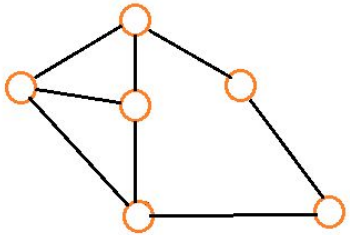


Para um grafo ser Hamiltoniano todos os vértices precisam ter uma quantidade de arestas maior ou igual a metade de sua ordem.

Condição suficiente, mas não necessária.

Teorema de Ore





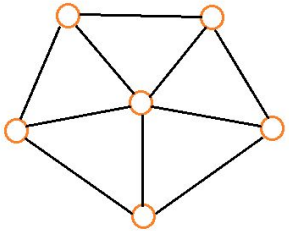
O teorema de Ore afirma que:

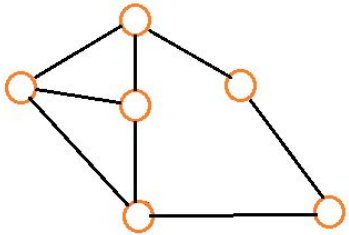
G sendo um grafo de ordem n > 3

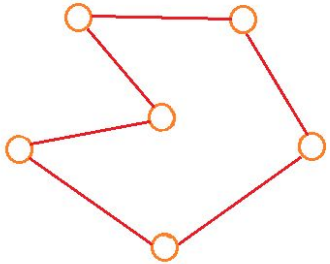
g(u) + g(v) ≥ n para todo par u, v de vértices não-adjacentes

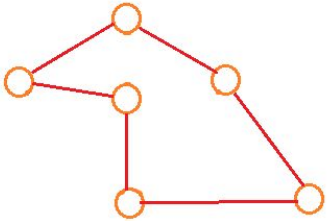
Em outras palavras, em um grafo com mais de 3 vértices (ordem > 3), se a soma do número de arestas de todos os pares de vértices não adjacentes sempre forem maior ou igual à ordem do grafo, este por sua vez é Hamiltoniano.

Teorema de Ore



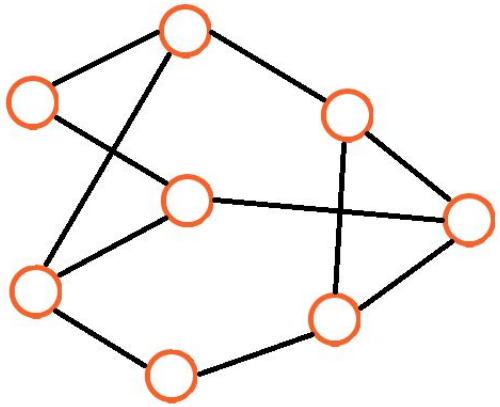






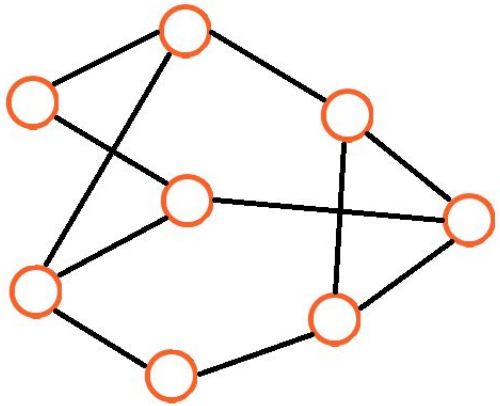
Para um grafo ser Hamiltoniano a soma do número de arestas que pertencem a dois vértices que não são conectados diretamente deve ser maior ou igual à sua ordem.

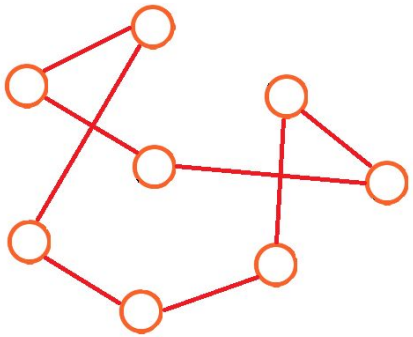
Condição suficiente mas não necessária.

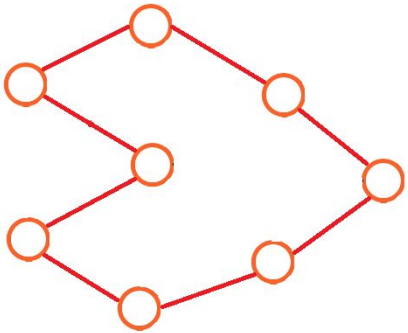


Relembrando teorema de Dirac: Se G é um grafo de ordem $n \geq 3$; $g(v) \geq n/2$ para todo $v \in V(G)$

Relembrando teorema de Ore: G sendo um grafo de ordem $n > 3$; $g(u) + g(v) \geq n$ para todo par u, v de vértices não-adjacentes

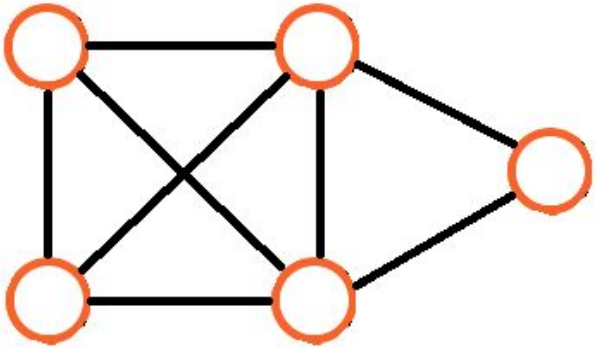






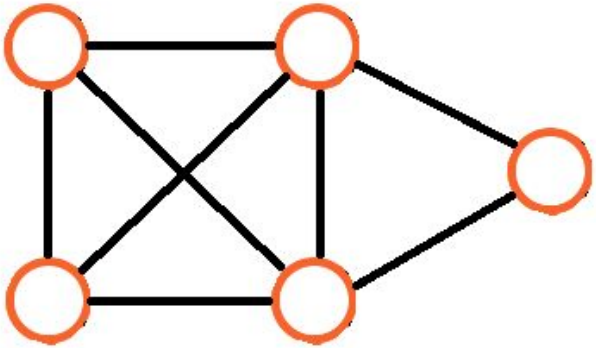
Relembrando teorema de Dirac: Se G é um grafo de ordem $n \geq 3$; $g(v) \geq n/2$ para todo $v \in V(G)$

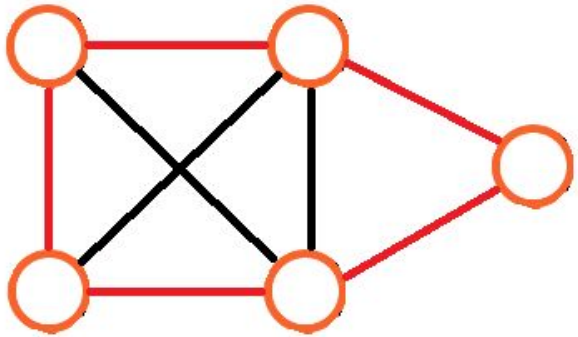
Relembrando teorema de Ore: G sendo um grafo de ordem $n > 3$; $g(u) + g(v) \geq n$ para todo par u, v de vértices não-adjacentes



Relembrando teorema de Dirac: Se G é um grafo de ordem $n \geq 3$; $g(v) \geq n/2$ para todo $v \in V(G)$

Relembrando teorema de Ore: G sendo um grafo de ordem $n > 3$; $g(u) + g(v) \geq n$ para todo par u, v de vértices não-adjacentes

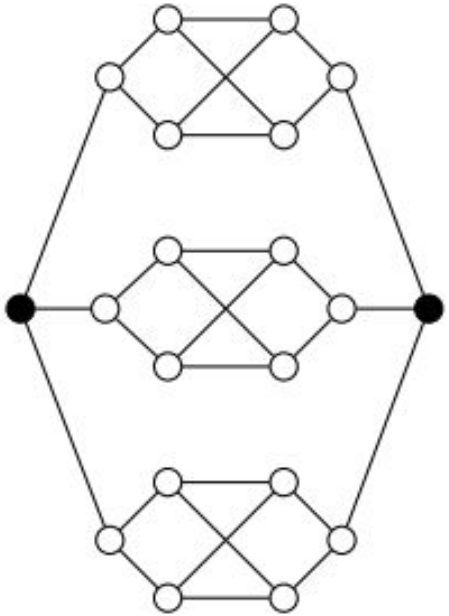




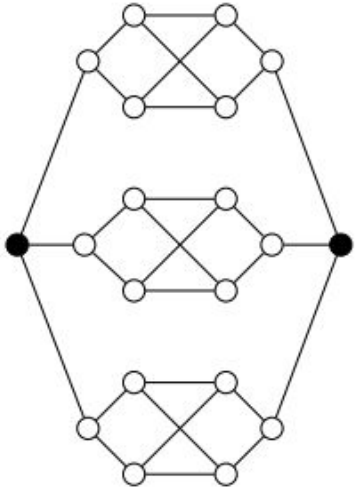
Relembrando teorema de Dirac: Se G é um grafo de ordem $n \geq 3$; $g(v) \geq n/2$ para todo $v \in V(G)$

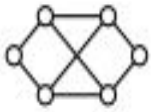
Relembrando teorema de Ore: G sendo um grafo de ordem $n > 3$; $g(u) + g(v) \geq n$ para todo par u, v de vértices não-adjacentes

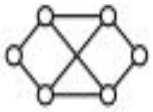
Condições Necessárias

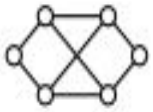


Condição necessária de West: Se G = (V,E) tem um ciclo hamiltoniano, então, para cada conjunto não vazio S ⊆ V, o grafo G − S tem no máximo|S| componentes









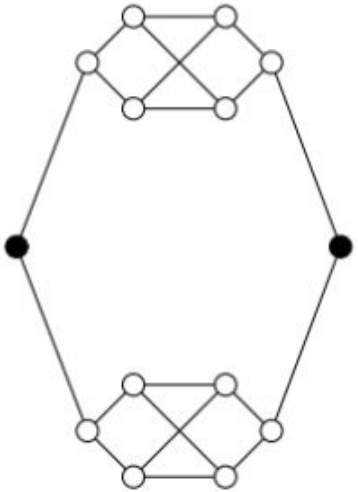
Como exemplo, se tomarmos o conjunto S como os vértices em preto, |S| = 2.

Agora subtraímos esses dois vértices do grafo e podemos analisar que agora o grafo tem 3 componentes.

Como a quantidade de componentes restante é maior que a cardinalidade de S então o grafo NÃO é hamiltoninano

G - S > |S|

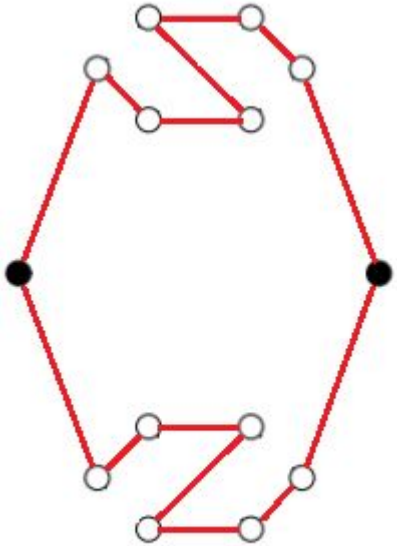
Contra-exemplo

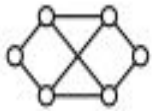


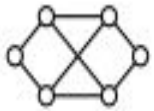
Se tiver o conjunto S pelos vértices em preto, e os retirarmos do grafo, temos 2 componentes restantes, logo o número de componentes restantes é igual a cardinalidade de S, logo não conseguimos afirmar que esse grafo NÃO é hamiltoniano

G - S <= |S|

Contra-exemplo







Se tiver o conjunto S pelos vértices em preto, e os retirarmos do grafo, temos 2 componentes restantes, logo o número de componentes restantes é igual a cardinalidade de S, logo não conseguimos afirmar que esse grafo NÃO é hamiltoniano

G - S <= |S|

Desenvolvimento da aplicação

Implementação

Foi escolhido o C pela familariedade com tal linguagem de programação e a biblioteca GSL (GNU Scientific Library) que nos permite utilizar as funções BLAS (Basic Linear Algebra Subprograms) facilmente.

GSL é uma biblioteca númerica que fornece grande variedade de rotinas matemáticas para C e C++ (álgebra linear, geração de números aleatórios, transformadas rápidas de Fourier, vetores e matrizes).

BLAS coleção de rotinas de baixo nível para operações aritméticas de matriz e vetor.

Criptografia

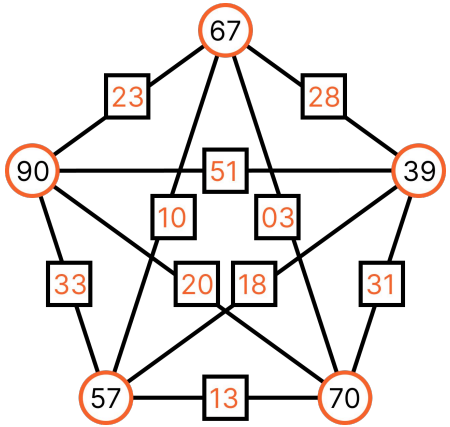
Passo 1

Transforme o texto a ser codificado em números usando a tabela abaixo.

	0	1	2	3	4	5	6
7	A	B	C	D	E	F	G
8	H	I	J	K	L	M	N
9	O	P	Q	R	S	T	U
10	V	W	X	Y	Z	space	dot

Passo 2

Construir a matriz A (grafo completo) cada vértice representa os valores calculados no Passo 1 e as arestas são o valor absoluto da diferença dos vértices .



Passo 3

Construir a matriz B copiando as arestas externas de A, e sua diagonal principal seguindo os valores da tabela abaixo.

A	B	C	...	...	X	Y	Z
1	2	3	...	...	24	25	26

DOT	scalar product, $x^T y$
AXPY	vector sum, $\alpha x + y$
MV	matrix-vector product, Ax
SV	matrix-vector solve, $inv(A)x$
MM	matrix-matrix product, AB
SM	matrix-matrix solve, $inv(A)B$

The types of matrices are,

GE	general
GB	general band
SY	symmetric
SB	symmetric band
SP	symmetric packed
HE	hermitian
HB	hermitian band
HP	hermitian packed
TR	triangular
TB	triangular band
TP	triangular packed

Each operation is defined for four precisions,

S	single real
D	double real
C	single complex
Z	double complex

Passo 4

Calcular a matriz N multiplicando as matrizes A e B, sendo A e B matrizes simêtricas podemos utilizar uma versão otimizada das multiplcação entre matrizes do BLAS.

Passo 5

Proceda com a multiplicação da matriz N pela matriz triangular superior K, de forma a obter a primeira cifra C1.

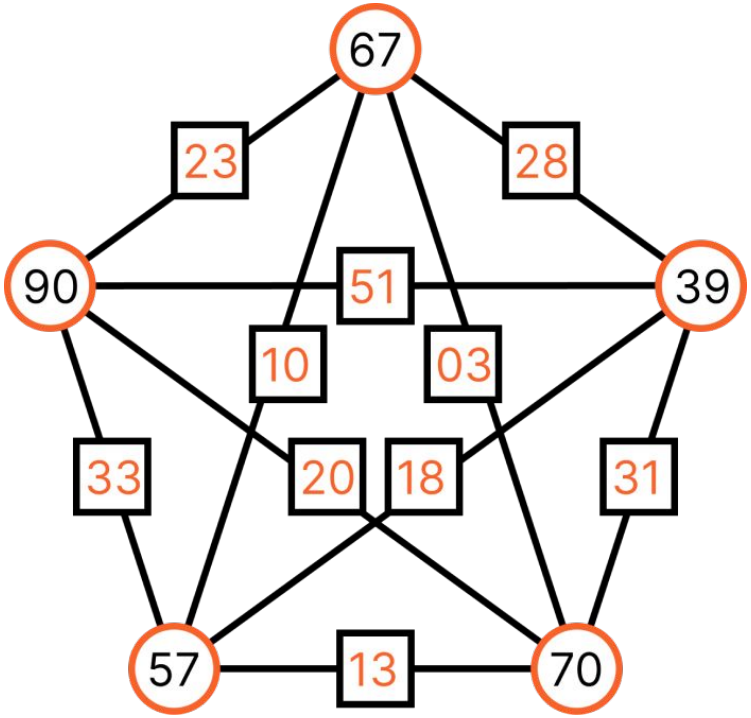
K =

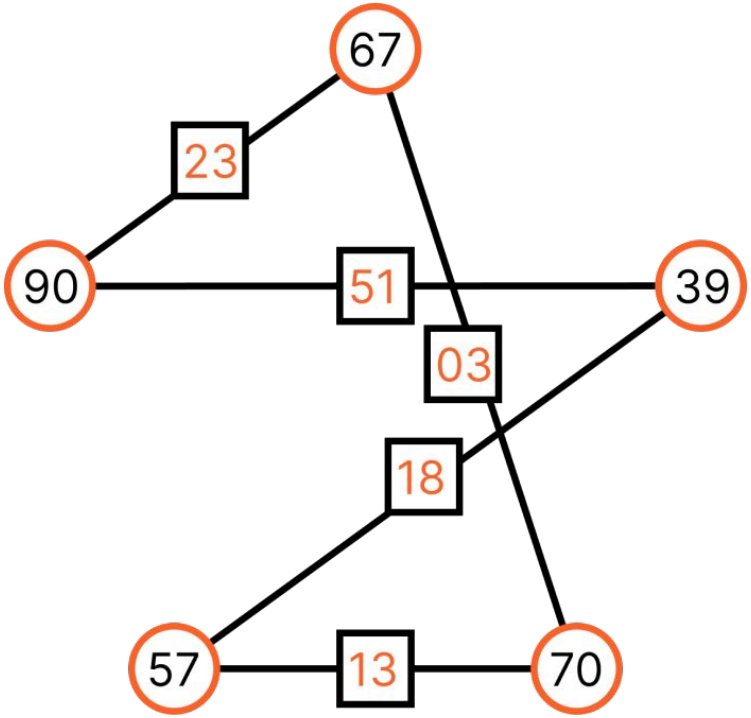
1	2	3	4	5
0	1	2	3	4
0	0	1	2	3
0	0	0	1	2
0	0	0	0	1

Passo 6

Utilizar o algoritmo de *Nearest-Neighbor* para encontrar um ciclo hamiltoniano (somar as arestas do ciclo para computar o valor de S). E os passos para tal algoritmo são:

1. Selecione o vértice inicial.
2. Busque o vértice adjacente de menor peso.
3. Caso haja vértices com pesos iguais, deve-se realizar a escolha de forma aleatória.
4. Repita 2 e 3 até que o ciclo hamiltoniano esteja completo.


67
23
28
90
51
39
10
03
33
20
18
31
57
13
70


67
23
90
51
39
03
18
57
13
70

Passo 7

Dividir cada item da matriz C1 por S, o resto será a cifra final C2 e a matriz Q os quocientes da operação.

Descriptografia

Passo 1

Para decodificar a mensagem é necessário as matrizes C2, Q, K e A e o valor S. O primeiro passo é obter C1 (se temos o divisor, quociente e resto é possível calcularmos o dividendo).

$$[Q]ij \times S + [C2]ij = C1$$

Passo 2

Calcular o inverso da matriz K.

$K =$

1	2	3	4	5
0	1	2	3	4
0	0	1	2	3
0	0	0	1	2
0	0	0	0	1

$K^{-1} =$

1	-2	1	0	0
0	1	-2	1	0
0	0	1	-2	1
0	0	0	1	-2
0	0	0	0	1

Passo 3

Calcular a matriz N multiplicando C1 e K^{-1}.

1313	3223	6134	9903	14347
1369	4483	7862	13435	21011
1349	3340	6461	10320	14977
1333	3673	6584	10753	15647
1589	5360	11161	17420	25297

X

1	-2	1	0	0
0	1	-2	1	0
0	0	1	-2	1
0	0	0	1	-2
0	0	0	0	1

=

1313	597	1001	858	675
1369	1745	265	2194	2003
1349	642	1130	738	798
1333	1007	571	1258	725
1589	2182	2030	458	1618

Passo 4

Calcular o inverso da matriz A.

$A =$

0	28	3	10	23
28	0	31	18	51
3	31	0	13	20
10	18	13	0	33
23	51	20	33	0

$A^{-1} =$

-2.17E-01	-9.11E-18	1.67E-01	5.00E-02	3.97E-18
-6.53E-18	-1.80E-02	1.31E-17	2.78E-02	9.80E-03
1.67E-01	8.22E-18	-1.92E-01	-2.30E-17	2.50E-02
5.00E-02	2.78E-02	-2.07E-17	-7.78E-02	3.96E-18
7.40E-18	9.80E-03	2.50E-02	-1.02E-33	-1.52E-02

Passo 5

Calcular a matriz B multiplicando N e A^{-1}.

1313	597	1001	858	675
1369	1745	265	2194	2003
1349	642	1130	738	798
1333	1007	571	1258	725
1589	2182	2030	458	1618

X

-2.17E-01	-9.11E-18	1.67E-01	5.00E-02	3.97E-18
-6.53E-18	-1.80E-02	1.31E-17	2.78E-02	9.80E-03
1.67E-01	8.22E-18	-1.92E-01	-2.30E-17	2.50E-02
5.00E-02	2.78E-02	-2.07E-17	-7.78E-02	3.96E-18
7.40E-18	9.80E-03	2.50E-02	-1.02E-33	-1.52E-02

=

7	28	0	0	23
28	18	31	0	0
0	31	1	13	0
0	0	13	6	33
23	0	0	33	15

Passo 6

A mensagem original é a diagonal principal da matriz B.

7	28	0	0	23
28	18	31	0	0
0	31	1	13	0
0	0	13	6	33
23	0	0	33	15

Computação quântica e ciclos hamiltonianos

Solucionado *HC* com teoria de Gauge

Na publicação *Solving Hamiltonian Cycle Problem using Quantum Z2 Lattice Gauge Theory* de Xiaopeng Cui1 and Yu Shi foi apresentado um algoritmo com complexidade temporal de $O(\frac{1}{g_c^2}\sqrt{\frac{1}{\varepsilon}N_e^{3/2}(N_v^3+\frac{N_e}{g_c})})$, sendo Nv, Ne e Gc, respectivamente, número de vértices e número de arestas, valor crítico do parâmetro de acoplamento g.

O valor médio da depêndencia de Gc (√Nhc , raiz quadrada do número de *HC*), e o valor médio de 1/Gc são lineares, sugerindo que para alguns grafos é possível solucionar o problema do ciclo hamiltoniano em tempo polinomial, mais eficiente que o algoritmo com programação dinâmica $O(N_v{}^2 2^{N_v})$ e o algoritmo de Monte Carlo $O(1.657^{N_v})$

Referências

- Ciclos Hamiltonianos em Grafos. Marcelo de Souza Santos
- http://www.math.nagoya-u.ac.jp
- https://en.wikipedia.org/wiki/Hamiltonian_path_problem
- Existência de Ciclos Hamiltonianos via técnicas espectrais. Guilherme Brandão Pereira
- https://www.gnu.org/software/gsl/doc/html/blas
- https://arxiv.org/abs/2202.08817